

Regeringens proposition till riksdagen med förslag till lagstiftning som kompletterar EU:s förordning som gäller gränsöverskridande elektronisk identifiering, betrodda tjänster och europeisk digital identitet

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att det stiftas en ny lag om vissa tjänster som möjliggör gränsöverskridande e-tjänster och en ny lag om e-legitimation samt ändringar i lagen om stark autentisering och betrodda elektroniska tjänster. Vidare föreslås ändringar i 27 andra lagar, i huvudsak laghänvisningar och andra tekniska ändringar.

Propositionens huvudsakliga syfte är att genomföra ändringarna i EU:s så kallade eIDAS-förordning, som gäller elektronisk identifiering, betrodda elektroniska tjänster och europeisk digital identitet. En central ändring gäller gemensam lagstiftning om den europeiska digitala identitetsplånboken. Det är fråga om en applikation som i regel fungerar i en mobil enhet och med hjälp av vilken användaren på ett tillförlitligt sätt kan styrka sin identitet elektroniskt på motsvarande sätt som för närvarande med identifieringsverktyg för stark autentisering. Med hjälp av plånboken ska det dessutom vara möjligt att hantera andra personuppgifter om sig själv med hjälp av elektroniska attributsintyg, som i praktiken är bestyrkta uppgifter i elektronisk form. Plånboken gör det också möjligt att skapa en kvalificerad elektronisk underskrift eller i fråga om juridiska personer en kvalificerad elektronisk stämpel. Det ska vara frivilligt för användarna att ta i bruk plånboken.

Myndigheten för digitalisering och befolkningsdata ska ha i uppgift att tillhandahålla plånboken i Finland. Detta begränsar dock inte möjligheterna för aktörer inom den privata sektorn att tillhandahålla en plånbok. Dessutom ska Myndigheten för digitalisering och befolkningsdata utifrån befolkningsdatasystemet bevilja fysiska personer identifieringsuppgifter som gör det möjligt att styrka sin identitet i plånboken. Patent- och registerstyrelsen ska ha rätt att bevilja identifieringsuppgifter för juridiska personer på basis av handelsregistret. Enligt propositionen ska Transport- och kommunikationsverket ha i uppgift att övervaka dem som tillhandahåller plånböcker samt de plånböcker som tillhandahållarna erbjuder. Därtill ska verket föra ett register över plånböckers förlitande parter. Transport- och kommunikationsverket föreslås också vara behörig myndighet att påföra tillhandahållare av betrodda tjänster administrativa påföljdsavgifter.

Genom förslaget skapas en rättslig grund för en e-legitimation som gör det möjligt att påvisa personuppgifter på ett tillförlitligt sätt. Polisen eller någon annan myndighet som beviljar pass- och identitetskort beviljar rätten till en e-legitimation och Myndigheten för digitalisering och befolkningsdata tillhandahåller den som ett kvalificerat elektroniskt attributsintyg som är kompatibelt med plånboken.

Vidare föreslås sådana ändringar i lagen om stark autentisering och betrodda elektroniska tjänster som beror på nationella behov och som ökar säkerheten vid användning av elektroniska tjänster och stark autentisering samt ändringar som behövs för att modernisera lagstiftningen.

De föreslagna lagarna avses träda i kraft så snart som möjligt hösten 2026.

INNEHÅLL

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL	1
MOTIVERING.....	8
1 Bakgrund och beredning.....	8
1.1 Bakgrund.....	8
1.2 Beredning.....	8
1.2.1 Beredningen av EU-rättsakten.....	8
1.2.2 Beredningen av propositionen.....	10
2 EU-rättsaktens målsättning och huvudsakliga innehåll.....	12
2.1 Målsättning	12
2.2 Det huvudsakliga innehållet i den reviderade eIDAS-förordningen	12
2.2.1 Europeisk digital identitet.....	12
2.2.2 Gränsöverskridande identitetsmatchning.....	16
2.2.3 Certifiering av system för elektronisk identifiering.....	16
2.2.4 Betrodda tjänster	17
2.2.5 Styrningsramverk.....	18
2.2.6 Rapporteringskrav.....	19
3 Nuläge och bedömning av nuläget	20
3.1 Genomförande av den reviderade eIDAS-förordningen.....	20
3.1.1 Nuläget i fråga om stark autentisering.....	20
3.1.2 Nuläget ifråga om betrodda tjänster	21
3.1.3 Nuläget i fråga om plånbokslösningar	23
3.1.4 Genomförandet av den ursprungliga eIDAS-förordningen	24
3.1.5 Bedömning.....	25
3.2 E-legitimation	26
3.3 Nationella behov av ändringar som främjar säkerheten i stark autentisering.....	28
3.3.1 Identifieringsverktygens tillförlitlighet.....	28
3.3.2 Skyldigheten att kontrollera passets och identitetskortets giltighet.....	28
3.3.3 Sammankopplad inledande identifiering och förmedling av uppgifter om den	28
3.3.4 Återaktivering av identifieringsverktyg.....	29
4 Förslagen och deras konsekvenser	30
4.1 De viktigaste förslagen	30
4.1.1 Genomförande av den reviderade eIDAS-förordningen.....	30
4.1.2 E-legitimation	33
4.1.3 Nationella behov av ändringar som främjar säkerheten vid stark autentisering.....	34
4.2 De huvudsakliga konsekvenserna.....	34
4.2.1 Inledning.....	34
4.2.2 Ekonomiska konsekvenser.....	35
4.2.2.1 Konsekvenserna för förtroendenätet för elektronisk identifiering.....	35
4.2.2.2 Konkurrensrättsliga konsekvenser avseende Myndigheten för digitalisering och befolkningsdatas uppgift som tillhandahållare av en europeisk digital identitetsplånbok	36
4.2.2.3 Regleringsbördan och övriga kostnader för e-tjänster.....	38
4.2.2.4 Administrativa påföljdsavgifter för tillhandahållare av betrodda tjänster	39

4.2.2.5 Avgifter för tillhandahållare av en europeisk digital identitetsplånbok, leverantörer av identifieringstjänster och tillhandahållare av betrodda tjänster samt organ för bedömning av överensstämmelse och certifierare	41
4.2.2.6 Nationella ändringar som främjar säkerheten vid användning av stark autentisering.....	42
4.2.2.7 Uppkomsten och spridningen av innovationer på marknaden.....	43
4.2.2.8 Konsekvenser för statsbudgeten	44
4.2.3 Övriga konsekvenser för människor och samhällsliga konsekvenser	45
4.2.3.1 Allmänna konsekvenser.....	45
4.2.3.2 Barn och unga	48
4.2.3.3 Utlandsfinländare.....	48
4.2.3.4 Personer med funktionsnedsättning	49
4.2.3.5 Konsekvenser för myndigheterna	50
4.2.3.6 Konsekvenser för informationshanteringen.....	55
4.2.3.7 Säkerheten i elektronisk kommunikation	57
4.2.3.8 Informationssamhället	58
4.2.3.9 Dataskydd	59
4.2.4 Gränsöverskridande konsekvenser	60
4.2.4.1 Förordningen om ett interoperabelt Europa och interoperabilitetsbedömning	60
4.2.4.2 EU-förordningen om en gemensam digital ingång.....	61
4.2.4.3 Gränsöverskridande konsekvenser för konsumenterna	61
4.2.4.4 Gränsöverskridande konsekvenser för företagen.....	62
5 Alternativa handlingsvägar.....	62
5.1 Handlingsalternativen och deras konsekvenser	62
5.1.1 Tillhandahållande av den europeiska digitala identitetsplånboken i Finland.....	62
5.1.2 Alternativ att lagstiftning som kompletterar den reviderade eIDAS-förordningen ingår i autentiseringslagen	63
5.1.3 Utnyttjande av det nationella handlingsutrymmet.....	64
5.1.4 Den nationella regleringen av plånböcker som enbart används i Finland	65
5.2 Handlingsmodeller som används eller planeras i andra medlemsstater	65
5.2.1 Sverige	66
5.2.2 Estland	67
5.2.3 Tyskland	67
5.2.4 Nederländerna.....	68
5.2.5 Danmark	69
6 Remissvar	69
6.1 Remissvar om genomförandet av den reviderade eIDAS-förordningen	69
6.2 Remissvar om e-legitimation	75
6.3 Remissvar om de ändringar som förbättrar säkerheten i den nationella starka autentiseringen.....	80
6.4 Utlåtande av rådet för bedömning av lagstiftningen.....	80
7 Specialmotivering.....	81
7.1 Lag om vissa tjänster som möjliggör gränsöverskridande e-tjänster.....	81
7.2 Lagen om stark autentisering och betrodda elektroniska tjänster.....	128
7.3 Lagen om e-legitimation.....	137

7.4 Lagen om tillhandahållande av digitala tjänster	149
7.5 Lagen om förvaltningens gemensamma stödtjänster för e-tjänster	149
7.6 Lagen om verkställighet av böter	150
7.7 Lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata	150
7.8 Lagen om behandling av kunduppgifter inom social- och hälsovården	151
7.9 Lagen om förhindrande av penningtvätt och av finansiering av terrorism	151
7.10 Jordabalken	152
7.11 Lagen om medborgarinitiativ	152
7.12 Lagen om förfarandet vid rådgivande folkomröstningar i välfärdsområden och kommuner	152
7.13 Lagen om fonderna inom området för inrikes frågor under programperioden 2021–2027	152
7.14 Lagen om identitetskort	152
7.15 Partilagen	153
7.16 Lagen om finansiering av projekt inom regionutveckling och Europeiska unionens regional- och strukturpolitik	153
7.17 Passlagen	153
7.18 Lagen om stödjande av landsbygdens utveckling under finansieringsperioden 2023–2027	153
7.19 Lagen om verkställighet av vissa av Europeiska unionens jordbruksstöd och vissa nationella jordbruksstöd	153
7.20 Lagen om det nationella genomförandet av Europeiska unionens gemensamma fiskeripolitik	154
7.21 Lagen om behandling av personuppgifter i polisens verksamhet	154
7.22 Lagen om behandling av personuppgifter inom Tullen	154
7.23 Lagen om strukturstöd till jordbruket	154
7.24 Lagen om behandling av personuppgifter vid Gränsbevakningsväsendet	154
7.25 Lagen om en marknadsordning för jordbruksprodukter	154
7.26 Konsumentskyddslagen	154
7.27 Lagen om strukturstöd för renhushållning och naturnäringar	155
7.28 Skjutvapenlagen	155
7.29 Fordonslagen	155
7.30 Konkurrenslagen	156
8 Bestämmelser på lägre nivå än lag	156
9 Ikraftträdande	158
10 Verkställighet och uppföljning	159
11 Förhållande till andra propositioner	160
12 Förhållande till grundlagen samt lagstiftningsordning	161
12.1 Inledning	161
12.2 Jämlikhet	161
12.3 Skydd av personuppgifter	164
12.3.1 Nationellt handlingsutrymme	164
12.3.2 E-legitimation, personuppgifter som ska behandlas och skyddet av dem	166
12.3.3 Rätt att få information	167

12.4 Rättsskydd.....	168
12.5 Påföljdsbestämmelser	170
12.5.1 Nationellt handlingsutrymme	170
12.5.2 Villkor som gäller administrativa påföljder.....	170
12.5.3 Påföljder som gäller myndigheter.....	174
12.6 Överföring av förvaltningsuppgifter på andra än myndigheter	175
12.7 Statliga skatter och avgifter	177
12.8 Bemyndiganden att utfärda föreskrifter.....	180
LAGFÖRSLAG.....	183
Lag om vissa tjänster som möjliggör gränsöverskridande e-tjänster.....	183
Lag om ändring av lagen om stark autentisering och betrodda elektroniska tjänster.....	202
Lag om e-legitimation.....	209
Lag om ändring av 3 och 6 § i lagen om tillhandahållande av digitala tjänster	214
Lag om ändring av 3 § i lagen om förvaltningens gemensamma stödtjänster för e-tjänster	215
Lag om ändring av 1 § i lagen om verkställighet av böter	216
Lag om ändring av lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata.....	217
Lag om ändring av 8 och 65 § i lagen om behandling av kunduppgifter inom social- och hälsovården	220
Lag om ändring av 3 kap. 11 § i lagen om förhindrande av penningtvätt och av finansiering av terrorism.....	221
Lag om ändring av 9 a kap. 1 § i jordabalken	222
Lag om ändring av 7 § i lagen om medborgarinitiativ	223
Lag om ändring av 4 § i lagen om förfarandet vid rådgivande folkomröstningar i välfärdsområden och kommuner	224
Lag om ändring av 15 och 26 § i lagen om fonderna inom området för inrikes frågor under programperioden 2021–2027.....	225
Lag om ändring av lagen om identitetskort	226
Lag om ändring av 3 § i partilagen.....	227
Lag om ändring av 52 § i lagen om finansiering av projekt inom regionutveckling och Europeiska unionens regional- och strukturpolitik.....	228
Lag om ändring av passlagen	229
Lag om ändring av 31 § i lagen om stödjande av landsbygdens utveckling under finansieringsperioden 2023–2027.....	230
Lag om ändring av 12 § i lagen om verkställighet av vissa av Europeiska unionens jordbruksstöd och vissa nationella jordbruksstöd.....	231
Lag om ändring av 32 § i lagen om det nationella genomförandet av Europeiska unionens gemensamma fiskeripolitik	232
Lag om ändring av 41 § i lagen om behandling av personuppgifter i polisens verksamhet	233
Lag om ändring av 35 § i lagen om behandling av personuppgifter inom Tullen.....	234
Lag om ändring av 29 § i lagen om strukturstöd till jordbruket.....	235
Lag om ändring av 50 § i lagen om behandling av personuppgifter vid Gränsbevakningsväsendet.....	236

Lag om ändring av 70 a § i lagen om en marknadsordning för jordbruksprodukter	237
Lag om ändring av konsumentskyddslagen.....	238
Lag om ändring av 48 § i lagen om strukturstöd för renhushållning och naturnäringar	240
Lag om ändring av 119 a § i skjutvapenlagen	241
Lag om ändring av 84 § i fordonslagen	242
Lag om ändring av 39 § i konkurrenslagen	243
BILAGA.....	244
PARALLELLTEXTER.....	244
Lag om ändring av lagen om stark autentisering och betrodda elektroniska tjänster.....	244
Lag om ändring av 3 och 6 § i lagen om tillhandahållande av digitala tjänster	261
Lag om ändring av 3 § i lagen om förvaltningens gemensamma stödtjänster för e-tjänster	263
Lag om ändring av 1 § i lagen om verkställighet av böter	265
Lag om ändring av lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata.....	266
Lag om ändring av 8 och 65 § i lagen om behandling av kunduppgifter inom social- och hälsovården	271
Lag om ändring av 3 kap. 11 § i lagen om förhindrande av penningtvätt och av finansiering av terrorism.....	273
Lag om ändring av 9 a kap. 1 § i jordabalken	274
Lag om ändring av 7 § i lagen om medborgarinitiativ	276
Lag om ändring av 4 § i lagen om förfarandet vid rådgivande folkomröstningar i välfärdsområden och kommuner	277
Lag om ändring av 15 och 26 § i lagen om fonderna inom området för inrikes frågor under programperioden 2021–2027.....	278
Lag om ändring av lagen om identitetskort	279
Lag om ändring av 3 § i partilagen.....	280
Lag om ändring av 52 § i lagen om finansiering av projekt inom regionutveckling och Europeiska unionens regional- och strukturpolitik.....	281
Lag om ändring av passlagen	282
Lag om ändring av 31 § i lagen om stödjande av landsbygdens utveckling under finansieringsperioden 2023–2027.....	283
Lag om ändring av 12 § i lagen om verkställighet av vissa av Europeiska unionens jordbruksstöd och vissa nationella jordbruksstöd.....	284
Lag om ändring av 32 § i lagen om det nationella genomförandet av Europeiska unionens gemensamma fiskeripolitik	285
Lag om ändring av 41 § i lagen om behandling av personuppgifter i polisens verksamhet	286
Lag om ändring av 35 § i lagen om behandling av personuppgifter inom Tullen.....	287
Lag om ändring av 29 § i lagen om strukturstöd till jordbruket.....	288
Lag om ändring av 50 § i lagen om behandling av personuppgifter vid Gränsbevakningsväsendet.....	289
Lag om ändring av 70 a § i lagen om en marknadsordning för jordbruksprodukter	290
Lag om ändring av konsumentskyddslagen.....	291
Lag om ändring av 48 § i lagen om strukturstöd för renhushållning och naturnäringar	294

Lag om ändring av 119 a § i skjutvapenlagen	295
Lag om ändring av 84 § i fordonslagen	296
Lag om ändring av 39 § i konkurrenslagen	297

MOTIVERING

1 Bakgrund och beredning

1.1 Bakgrund

Med stark autentisering avses att identiteten styrks elektroniskt. Med autentisering kan en person på ett tillförlitligt och tryggt sätt styrka vem han eller hon är vid uträttandet av elektroniska ärenden, och e-tjänsterna kan identifiera vem som uträttar ärenden hos dem och erbjuda dem sina tjänster. I praktiken sker autentisering med ett identifieringsverktyg för stark autentisering. De identifieringsverktyg för stark autentisering som för närvarande används i Finland är t.ex. bankkoder som bankerna tillhandahåller och teleföretagens mobilcertifikat. Med betrodda tjänster avses i sin tur tjänster som möjliggör förtroende för elektroniska handlingar och elektroniska processer. De betrodda tjänsterna kan inte alltid ses av användaren utan är osynliga i tjänsternas strukturer. Betrodda tjänster är t.ex. tjänster i anslutning till skapandet av elektroniska underskrifter och vissa andra certifikat.

I Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, dvs. i den s.k. *eIDAS-förordningen*, inrättades ett elektroniskt interoperabilitetsramverk för identifiering vars syfte var att med elektroniska identifieringsverktyg som beviljats i en medlemsstat möjliggöra identifiering i en annan medlemsstats offentliga e-tjänster. En annan avsikt med förordningen var att harmonisera bestämmelserna om betrodda tjänster inom EU.

Europaparlamentet och rådet antog den 11 april 2024 förordningen (EU) 2024/1183 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet. Genom den förordningen ändrades den ursprungliga eIDAS-förordningen så att vissa av dess ursprungliga artiklar förblev i kraft som sådana medan vissa ändrades och vissa upphävdes. Den viktigaste ändringen var emellertid att nya artiklar om den europeiska digitala identiteten tillfogades. *Den reviderade eIDAS-förordningen* är som sådan tillämplig rätt i medlemsstaterna, men den ger medlemsstaterna nationellt handlingsutrymme i vissa frågor. Den reviderade eIDAS-förordningen innehåller dessutom vissa skyldigheter för medlemsstaterna, bl.a. när det gäller att tillhandahålla europeiska digitala identitetsplånböcker samt att utse ett nationellt tillsynsorgan och en nationell kontaktpunkt, vilket förutsätter kompletterande nationell lagstiftning. Den här regeringspropositionen innehåller förslag till bestämmelser om de ovannämnda frågorna för att den reviderade eIDAS-förordningen ska kunna tillämpas effektivt i Finland.

1.2 Beredning

1.2.1 Beredningen av EU-rättsakten

Europeiska kommissionen ordnade ett offentligt samråd om översynen av eIDAS-förordningen mellan den 23 juli 2020 och den 3 september 2020. Till följd av det offentliga samrådet lämnade statsrådet riksdagen en utredning ([E 109/2020 rd](#)) om Finlands föregripande inflytande vid översynen av eIDAS-förordningen. Kommissionen lade den 3 juni 2021 fram ett förslag till ändring av förordningen (EU) nr 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet ([COM/2021/281 final](#)) samt en hithörande konsekvensbedömning på EU-nivå ([SWD/2021/124 final](#)). Behandlingen av kommissionens lagstiftningsförslag inleddes i Europeiska unionens råds arbetsgrupp för telekommunikation och informationssamhället i juni 2021. Europaparlamentet antog ändringarna till eIDAS-förordningen den 29 februari 2024 och

Europeiska unionens råd för sin del den 26 mars 2024. Ändringarna till eIDAS-förordningen publicerades i Europeiska unionens officiella tidning den 30 april 2024 och förordningen trädde i kraft den 20 maj 2024.

Statsrådets skrivelse ([U 41/2021 rd](#)) om kommissionens förslag överlämnades till riksdagen i september 2021. Förvaltningsutskottets utlåtande ([FvUU 34/2021 rd](#)) till stora utskottet färdigställdes i december 2021. Likaså godkände stora utskottet i december 2021 ståndpunkten i förvaltningsutskottets utlåtande. Dessutom tillsatte finansministeriet en nationell samordningsgrupp för beredningen av en europeisk digital identitet ([Projekt VM025:00/2022](#)). Samordningsgruppen hade som mål att i rätt tid påverka beredningen av den europeiska digitala identiteten i EU:s institutioner och i samarbete med de övriga medlemsstaterna så att slutresultatet överensstämmer med Finlands mål. Som ordförande för samordningsgruppen verkade en företrädare för finansministeriet och dessutom var kommunikationsministeriet, justitieministeriet, undervisnings- och kulturministeriet, inrikesministeriet, social- och hälsovårdsministeriet, arbets- och näringsministeriet, statsrådets kansli, Myndigheten för digitalisering och befolkningsdata samt Transport- och kommunikationsverket företrädare i gruppen.

Finland ansåg att kommissionens förslag till ändring av eIDAS-förordningen var allmänt viktigt och stödde strävan att ytterligare förbättra de gränsöverskridande e-tjänsterna och e-handeln mellan medlemsstaterna. Finland ansåg det vara viktigt att den föreslagna regleringen sammanjämkas med den övriga EU-lagstiftningen. För Finland var det väsentligt att regleringen utgör en samlad helhet där medlemsstaterna och marknadsaktörerna t.ex. inte åläggs överlappande eller motstridiga skyldigheter. Finland förhöll sig i princip positivt till den lagstiftningsram som föreslogs för den europeiska digitala identitetsplånboken. Lagstiftningsramen för plånboken ska komplettera de nationella identitetshanteringsmetoderna, dvs. den ska basera sig på en nationellt registrerad identitet. Finland ansåg dessutom att det är viktigt att en persons identitet i de plånböcker som medlemsstaterna tillhandahåller verifieras i enlighet med de krav som gäller för tillitsnivån hög.

Finland ansåg att det är väsentligt att lagstiftningen också tar hänsyn till tryggheten av verksamhetsförutsättningarna för leverantörer av identifieringstjänster inom den privata sektorn samt att den möjliggör innovationer. För Finland var det viktigt att lagstiftningen gör det möjligt att anmäla de identifieringssystem och plånböcker som den privata sektorn tillhandahåller till kommissionen och därigenom användningen av dem vid gränsöverskridande identifiering. Dessutom ansåg Finland att det är viktigt att främja säkerheten i e-tjänster och e-handel såväl i den offentliga som i den privata sektorns tjänster.

Finland ansåg att det behöver skapas ett nytt alternativt förfarande, dvs. certifiering, för anmälan av system för elektronisk identifiering. Certifiering och hithörande standardisering kan förbättra enhetligheten och förutsägbarheten i kraven, göra själva anmälan snabbare och minska den administrativa börda anmälan utgör. Finland understödde förslaget om att elektroniska attributsintyg och andra nya betrodda tjänster läggs till i förordningens tillämpningsområde. Kraven och kriterierna för elektroniska betrodda tjänster behöver harmoniseras för att det i praktiken ska vara möjligt att tillhandahålla tjänsterna på den inre marknaden.

I den reviderade eIDAS-förordningen ges kommissionen befogenhet att anta genomförandeförordningar som kompletterar förordningen, i synnerhet vad gäller den europeiska digitala identitetsplånboken och standarderna för betrodda tjänster. Kommissionens genomförandeförordningar har behandlats av eIDAS-kommittén, som bistår kommissionen i dess arbete och där även medlemsstaterna är företrädare. För Finlands del har experter från Transport- och kommunikationsverket och Myndigheten för digitalisering och befolkningsdata

utsetts till medlemmar i kommittén. Statsrådet har lämnat en utredning ([E 62/2024 rd](#)) om beredningen av genomförandeförordningarna. Sett till genomförandeförordningarna och en noggrannare definition av de tekniska kraven ansåg Finland det vara mycket viktigt, och med tanke på en mer allmän användning av plånböcker avgörande, att det blir så enkelt som möjligt att använda plånböcker och att de är så tillgängliga som möjligt. Vid beredningen av genomförandeförordningarna bör man eftersträva en ändamålsenlig balans mellan hög säkerhet och användbarhet som samtidigt främjar användningen. Dessutom är det viktigt att förordningarna innehåller alla bestämmelser som behövs för att genomföra plånböckerna eftersom medlemsstaternas tidsfrist för att genomföra dem börjar när genomförandeförordningarna träder i kraft.

Förutom att delta i beredningen av EU-rättsakterna deltog Finland aktivt tillsammans med övriga medlemsstater och organisationer i ett gränsöverskridande pilotförsök med europeiska digitala identitetsplånböcker. Pilotförsöken inleddes 2023 och de syftade till att främja plånböckernas gränsöverskridande interoperabilitet. Finland medverkade i tre olika samarbetsprojekt (nedan *konsortier*) där Finlands centrala mål var att pilottesta ett mobilt körkort och elektroniska myndighetstjänster, utveckla digital identitet för företag och företagsplånböcker samt pilottesta utnyttjandet av högskolesektorns examensbetyg och studerandeuppgifter. Pilotförsöken var ett centralt led i beredningen av ändringarna i eIDAS-förordningen och erbjöd konkret information om plånböckerna även för beredningen av genomförandeförordningarna och arbetet med standarderna.

Finland deltog dessutom i ett samarbete mellan kommissionen och medlemsstaterna där man beredde tekniska bestämmelser vad gäller de europeiska digitala identitetsplånböckerna i den s.k. *Toolbox*-processen som inleddes utifrån kommissionens rekommendation ([EU 2021/946](#)). Som resultat av processen producerade medlemsstaterna och kommissionen en arkitekturell referensram för plånböckerna för att främja interoperabiliteten mellan plånböckerna och anknyttande tjänster. Den arkitekturella referensramen är inte förpliktande för medlemsstaterna. Däremot förpliktar de standarder som det hänvisas till i genomförandeförordningarna medlemsstaterna. Standarder bereds av såväl europeiska (t.ex. ETSI och CEN/CENELEC) som internationella standardiseringsorganisationer (t.ex. ISO/IEC) samt av olika sammanslutningar som tillhandahåller protokoll för digitala identiteter (t.ex. OpenID Foundation, W3C och IETF). Standardiseringsorganisationernas och sammanslutningarnas arbete har till vissa delar ännu inte slutförts. De genomförandeförordningar om plånböcker som hittills antagits kommer att kompletteras med nya hänvisningar när standarderna har blivit klara.

1.2.2 Beredningen av propositionen

Finansministeriet tillsatte den 26 april 2024 ett projekt i syfte att stödja det nationella genomförandet av den reviderade eIDAS-förordningen. Det primära målet med projektet är att säkerställa att skyldigheterna enligt den reviderade eIDAS-förordningen fullgörs inom den tidsfrist som EU fastställt. För projektet tillsattes en styrgrupp, en lagstiftningsarbetsgrupp och en operativ arbetsgrupp. Lagstiftningsarbetsgruppens mandatperiod varade från den 26 april 2024 till den 30 juni 2025 och dess primära uppgift var att bedöma vilka ändringar som behövs i lagstiftningen och att i form av regeringsproposition utarbeta ett förslag till lagstiftning som är nödvändig för att genomföra skyldigheterna i den reviderade eIDAS-förordningen nationellt. I lagstiftningsarbetsgruppen ingick företrädare för kommunikationsministeriet, inrikesministeriet, arbets- och näringsministeriet, Myndigheten för digitalisering och befolkningsdata, Transport- och kommunikationsverket och Polisstyrelsen. Förutom de ovan nämnda är undervisnings- och kulturministeriet samt social- och hälsovårdsministeriet företrädare i styrgruppen och Patent- och registerstyrelsen i den operativa arbetsgruppen.

Beredningsunderlaget till regeringens proposition finns i den offentliga tjänsten på <https://vm.fi/hanke?tunnus=VM059:00/2024>.

Som ett led i den nationella beredningen av genomförandet av den reviderade eIDAS-förordningen lät finansministeriet göra en marknadsundersökning för att kartlägga vilka aktörer inom den offentliga och den privata sektorn som kunde tänkas ha kapaciteter och beredskap att i Finland tillhandahålla fysiska personer en europeisk digital identitetsplånbok i enlighet med den reviderade eIDAS-förordningen för mobila terminaler inom den tidsfrist som EU har satt. Marknadsundersökningen genomfördes som en enkät riktad till centrala tillhandahållare av betrodda tjänster och leverantörer av identifieringstjänster samt i form av fördjupande intervjuer. Utifrån iakttagelserna i marknadsundersökningen beslutade finansministeriet i samband med att projektet tillsattes att beredningen utgår från att Myndigheten för digitalisering och befolkningsdata producerar en plånbok i Finland som motsvarar de krav som ställs i den reviderade eIDAS-förordningen. Enligt uppgifterna från marknadsundersökningen föreföll det som att den privata sektorns aktörer vid tidpunkten för undersökningen inte hade förutsättningar att producera en plånbok inom den tidsfrist som förordningen förutsätter.

Under beredningen hörde man sig vid rundabordsdiskussioner för om hur centrala intressentgrupper som ämbetsverk, intresseorganisationer och medlemmar i förtroendenätet såg på det nationella genomförandet. Det ordnades två diskussioner varvid man frågade efter intressentgruppernas åsikter om i synnerhet det nationella handlingsutrymmet och frågor som gällde en plånbok för juridiska personer. Dessutom ordnade finansministeriet för allmänheten öppna intressentgruppsmöten om det nationella genomförandet av den reviderade eIDAS-förordningen.

Utkastet till regeringsproposition var ute på remiss mellan den 12 juni och den 29 augusti 2025. Utkastet till propositionen publicerades i tjänsten Utlåtande.fi där vem som helst hade möjlighet att lämna sin åsikt om det. Begäran om yttrande skickades bl.a. till olika ministerier, ämbetsverk, andra offentligt-rättsliga organisationer, kommuner och städer, företag, intresseorganisationer, föreningar, Ålands landskapsregering och Ålandsdelegationen. Det inkom sammanlagt 115 yttranden, där 13 av instanserna meddelade att de inte hade något att yttra i frågan och två att de inte lämnar något yttrande. Remissvaren refereras i avsnitt 6. Över yttrandena har det dessutom upprättats ett sammandrag som finns tillgängligt i den ovan nämnda offentliga tjänsten.

Rådet för bedömning av lagstiftningen lämnade ett utlåtande om propositionen den 13 januari 2026. Utlåtandet och de kompletteringar som gjordes utifrån det behandlas närmare i avsnitt 6.4.

Samtidigt som revideringen av den ursprungliga eIDAS-förordningen bereddes i EU, pågick vid finansministeriet ett projekt för att utveckla en e-legitimation. Syftet med projektet var att via Myndigheten för digitalisering och befolkningsdata tillhandahålla en e-legitimation som en applikation för mobila enheter. Handlingarna som gäller beredningen är tillgängliga i den offentliga tjänsten på <https://vm.fi/sv/projekt?tunnus=VM092:00/2021>. Den ursprungliga tanken då e-legitimationen började beredas var att den i ett senare skede ska kunna utvidgas till att motsvara de krav som ställs på den europeiska digitala identitetsplånboken. När det preliminära förhandlingsresultatet om ändringarna i eIDAS-förordningen kom i november 2023, fattades beslutet att med grund i finansministeriets bedömning flytta fokus från e-legitimationen till genomförandet av den europeiska digitala identitetsplånboken i stället för att ha en överlappande beredning. I stället för att arbeta med en separat applikation och ett separat projekt går arbetet med e-legitimationen nu vidare som ett led i utvecklandet av plånboken. Myndigheten för digitalisering och befolkningsdatas och Polisstyrelsens tidigare arbete med att

utveckla e-legitimationen kan utnyttjas när e-legitimationen tas fram. De befintliga tekniska lösningarna har skapat en grund även för den nationella beredningen av plånboken.

2 EU-rättsaktens målsättning och huvudsakliga innehåll

2.1 Målsättning

Målet med den ursprungliga eIDAS-förordningen var att bygga upp förtroendet för e-tjänster och e-handel på den inre marknaden och säkerställa att det för skötseln av gränsöverskridande ärenden finns trygga medel för elektronisk identifiering. Ett annat mål med förordningen var att skapa en allmän rättslig ram för användningen av betrodda tjänster. Fokus på marknaden har emellertid förskjutits från utnyttjandet av digital identitet mot tillhandahållande och användning av olika uppgifter i anslutning till identitet. Sådana lösningar skulle också behövas i synnerhet för e-tjänsterna inom den privata sektorn, som den ursprungliga eIDAS-förordningen inte är tillämplig på. Med den ursprungliga eIDAS-förordningen kunde man således inte längre svara mot marknadens nya behov.

Syftet med den reviderade eIDAS-förordningen är att säkerställa att unionsmedborgarna och invånare i unionen har rätt till en digital identitet som helt står under deras egen kontroll. Avsikten är att säkerställa att det finns mycket säkra och tillförlitliga elektroniska identitetslösningar för skötsel av olika ärenden över medlemsstaternas gränser, både med tanke på användarna och med tanke på tjänsterna. Målet är också att minska riskerna och kostnaderna genom att anta ett mer enhetligt förhållningssätt i fråga om elektronisk identifiering. När det gäller betrodda tjänster är målet att säkerställa lika villkor för tillhandahållande och kvalificering av betrodda tjänster i medlemsstaterna.

2.2 Det huvudsakliga innehållet i den reviderade eIDAS-förordningen

2.2.1 Europeisk digital identitet

Den väsentliga ändringen i den reviderade eIDAS-förordningen jämfört med den ursprungliga eIDAS-förordningen är ett förstärkt regelverk för europeisk digital identitet. Till centrala delar genomfördes detta genom att det till förordningens kapitel II om elektronisk identifiering fogades avsnitt 1 Europeisk digital identitetsplånbok (nedan även *plånbok*). Plånboken är i princip en applikation som fungerar i mobila enheter och med hjälp av vilken användaren på ett tillförlitligt sätt kan styrka sin identitet elektroniskt på motsvarande sätt som för närvarande med ett identifieringsverktyg för stark autentisering. De identifieringsverktyg för stark autentisering som för närvarande används i Finland är bankkoder som bankerna tillhandahåller, teleföretagens mobilcertifikat, av Myndigheten för digitalisering och befolkningsdata beviljade medborgarcertifikat som finns på identitetskort och av Myndigheten för digitalisering och befolkningsdata beviljade organisationscertifikat som finns på organisationskort. Förutom att identifiera sig ska det med hjälp av plånboken dessutom vara möjligt att administrera andra personuppgifter som gäller en själv. Det sker med hjälp av elektroniska attributsintyg som är en ny betrodd tjänst som har lagts till i tillämpningsområdet. I praktiken är ett elektroniskt attributsintyg bestyrkta uppgifter i elektronisk form som beskriver egenskaper, beskaffenhet, rätt eller tillstånd vad gäller användaren. Ett elektroniskt attributsintyg kan t.ex. vara elektroniska uppgifter om giltig körkort eller avlagd examen. Plånboken gör det också möjligt att skapa en kvalificerad elektronisk underskrift eller i fråga om juridiska personer en kvalificerad stämpel.

Till centrala delar föreskrivs det om plånboken i artiklarna 5a–5f i den reviderade eIDAS-förordningen. Enligt artikel 5a.1 i förordningen ska varje medlemsstat tillhandahålla åtminstone

en europeisk digital identitetsplånbok. Detta är den viktigaste skyldighet som åläggs medlemsstaterna i den reviderade eIDAS-förordningen. Plånböckerna ska tillhandahållas inom 24 månader från det att kommissionens genomförandeförordningar om dem har trätt i kraft. Kommissionen har antagit genomförandeförordningarna i fråga och de trädde i kraft den 24 december 2024. Medlemsstaterna ska således tillhandahålla plånböcker senast den 24 december 2026. Enligt artikel 5a.2 i den reviderade eIDAS-förordningen kan den europeiska digitala identitetsplånboken tillhandahållas direkt av en medlemsstat, på uppdrag av en medlemsstat eller oberoende av en medlemsstat men med den medlemsstatens erkännande. Förordningen anger inte hur erkännandet av plånboken ska ske i medlemsstaten, utan det får medlemsstaterna själva besluta om.

Till centrala delar finns bestämmelserna om kraven på den europeiska digitala identitetsplånboken i artikel 5a. De plånböcker som medlemsstaterna tillhandahåller ska uppfylla de krav som det föreskrivs om i artikeln och i dem ingår egentligen inget nationellt handlingsutrymme. Medlemsstaterna får emellertid nationellt besluta om vilken aktör som ansvarar för uppfyllandet av vilken skyldighet i fråga om plånboken. Artikel 5a innehåller dock nationellt handlingsutrymme i fråga om öppenheten i plånbokens källkod samt kostnadsfriheten för elektronisk underskrift med plånboken. Artikel 5a.3 sätter som utgångspunkt att källkoden för programvarukomponenterna i applikationen ska vara licensierad med öppen källkod. Genom kravet på öppen källkod främjas transparensen i plånbokens funktion och ges möjlighet att förstå hur källkoden fungerar och att revidera och granska den. Medlemsstaterna får föreskriva att källkoden för andra specifika komponenter än de som installeras på användarenheter inte ska lämnas ut om det föreligger vederbörligen motiverade skäl. Medlemsstaterna kan alltså avgränsa olika bakomliggande system från kravet på öppen källkod, som t.ex. bibliotek, kommunikationskanaler eller andra sådana element som inte finns på användarens enhet. Ett vederbörligt motiverat skäl enligt skäl 33 kan vara ett skäl särskilt med hänsyn till den allmänna säkerheten.

I artikel 5a.5 g i förordningen förutsätts att plånboken ska ge alla fysiska personer möjlighet att använda kostnadsfria elektroniska underskrifter. Däremot kan avgift förutsättas av juridiska personer om de använder plånboken för elektronisk stämpling. Medlemsstaterna har emellertid nationellt handlingsutrymme också i fråga om avgifter för elektroniska underskrifter som tas ut av fysiska personer. Enligt artikel 5a.5 andra stycket får medlemsstaterna föreskriva proportionella åtgärder för att säkerställa att fysiska personers kostnadsfria användning av elektroniska underskrifter är begränsad till icke-yrkesmässiga ändamål. Medlemsstaterna kan alltså föreskriva åtgärder med vilka det går att ta ut en avgift även för underskrifter som görs med en fysisk persons plånbok om underskriften görs för yrkesmässiga ändamål. Åtgärderna ska emellertid stå i proportion till identifierade risker och vara motiverade.

Förutom i artikel 5a i den reviderade eIDAS-förordningen föreskrivs det om närmare tekniska krav på den europeiska digitala identitetsplånboken i genomförandeförordningar av kommissionen som kommissionen ges befogenhet att anta med stöd av artikel 5a.23. Kommissionen har antagit genomförandeförordningen (EU) 2024/2977 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller personidentifieringsuppgifter och elektroniska attributsintyg som utfärdats för EU:s digitala identitetsplånböcker, genomförandeförordningen (EU) 2024/2979 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller integritet och centrala funktioner i EU:s digitala identitetsplånböcker, genomförandeförordningen (EU) 2024/2982 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller protokoll och gränssnitt som ska stödjas av det europeiska ramverket för digital identitet samt genomförandeförordningen (EU) 2024/2980 om tillämpningsföreskrifter för

Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller anmälningar till kommissionen avseende ekosystemet för EU:s digitala identitetsplånböcker. Kommissionen har emellertid uppgett att det kommer att göras ändringar i antagna genomförandeförordningar innan medlemsstaternas tidsfrist för att tillhandahålla plånböcker går ut.

I artikel 5b i den reviderade eIDAS-förordningen föreskrivs det om förlitande parter avseende den europeiska digitala identitetsplånboken. Med förlitande parter avses i praktiken olika e-tjänster som möjliggör att ärenden sköts med plånboken i deras tjänster. Med förlitande parter kan också avses tjänsteleverantörer av annat slag som utnyttjar plånboken i sina tjänster och det är också möjligt att det bakom en juridisk person som verkar som förlitande part verkar flera olika e-tjänster. Förlitande parter förlitar sig således på de uppgifter de får från plånböckerna och tillhandahåller personer tjänster utifrån dem.

Artikel 5b ålägger förlitande parter att registrera sig i den medlemsstat där de är etablerade. Dessutom anger artikeln vilka uppgifter som den förlitande parten åtminstone ska tillhandahålla i samband med registreringen. Sådana uppgifter är bl.a. att ange vilka uppgifter den förlitande parten begär av användarna. Enligt artikeln får förlitande parter inte begära att användare tillhandahåller några andra uppgifter än dem som angavs i samband med registreringen. Dessutom har kommissionen med stöd av artikel 5b.11 antagit kommissionens genomförandeförordning (EU) 2025/848 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller registrering av förlitande parter. Artikeln och genomförandeförordningen lämnar medlemsstaterna ett visst handlingsutrymme i fråga om hur registret över förlitande parter och registreringsprocessen anges. Enligt artikel 5b.2 ska registreringsprocessen dock vara kostnadseffektiv och stå i proportion till riskerna. Medlemsstaterna kan besluta t.ex. om huruvida medlemsstaten för ett eller flera register över förlitande parter samt om huruvida medlemsstaten förutom det obligatoriska förlitandepartcertifikatet utfärdar även ett förlitandepartregistreringscertifikat på frivillig väg.

Bestämmelser om certifieringen av europeiska digitala identitetsplånböcker finns i artikel 5c i den reviderade eIDAS-förordningen. På plånböckerna tillämpas således inte det förfarande för anmälan av system för elektronisk identifiering som det föreskrivs om i eIDAS-förordningen. Förfarandet har tidigare tillämpats för att stärka det gränsöverskridande förtroendet för elektroniska identifieringsverktyg. Däremot ska plånboken certifieras för att styrka att plånboken följer kraven i förordningen. Utgångsläget är att organ för bedömning av överensstämmelse som utsetts av medlemsstaterna certifierar att plånböckerna uppfyller kraven i förordningen. Dessutom ska medlemsstaterna skapa nationella certifieringsordningar. Certifieringen är i kraft i fem år förutsatt att det görs en sårbarhetsbedömning vartannat år. Det nationella handlingsutrymme medlemsstaterna har anknyter närmast till hur medlemsstaten utser de organ för bedömning av överensstämmelse som avses i eIDAS-förordningen och vilken aktör som upprättar nationella certifieringsordningar.

Kommissionen har dessutom med stöd av artikel 5c.6 antagit genomförandeförordningen (EU) 2024/2981 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller certifiering av EU:s digitala identitetsplånböcker (nedan *förordning om certifiering av plånböcker*). Enligt artikel 3.1 i den genomförandeförordningen ska medlemsstaterna utse en systemägare för varje nationell certifieringsordning. Dessutom ställer genomförandeförordningen flera krav på innehållet i den nationella certifieringsordningen. I praktiken innebär upprättandet av en nationell certifieringsordning att man på nationell nivå anger de tekniska kraven mer exakt eller gör vissa val beträffande det tekniska utförandet inom de gränser som genomförandeförordningen tillåter i fråga om kraven på plånboken. Då plånboken uppfyller kraven i den nationella certifieringsordningen uppfyller den även kraven i den reviderade eIDAS-förordningen. I genomförandeförordningen föreskrivs det också mer

ingående om kraven på certifieringsorgan samt om livscykeln för den certifiering som de beviljar.

Enligt artikel 5c i den reviderade eIDAS-förordningen ska krav som är relevanta för cybersäkerheten certifieras i enlighet med europeiska cybersäkerhetscertifieringsordningar. Sådana certifieringssystem har dock ännu inte skapats. Av den anledningen ska nationella certifieringsordningar skapas också med avseende på cybersäkerhetskraven och tillämpas tills europeiska ordningar för cybersäkerhetscertifiering har införts. För plånboken kan man också skaffa certifiering för behandling av personuppgifter i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (*allmän dataskyddsförordning*).

I artikel 5d i den reviderade eIDAS-förordningen föreskrivs det om offentliggörande av en förteckning över certifierade europeiska digitala identitetsplånböcker. I artikel 5d.1 och 5d.2 föreskrivs det om medlemsstaternas skyldighet att informera kommissionen och den samarbetsgrupp som inrättats i enlighet med artikel 46e.1 om europeiska digitala identitetsplånböcker som medlemsstaterna tillhandahåller samt om de uppgifter som ska anmälas. Kommissionen offentliggör utifrån dessa uppgifter en förteckning över certifierade europeiska digitala identitetsplånböcker. Den offentliggörs i Europeiska unionens officiella tidning. Med stöd av artikel 5d.7 har kommissionen antagit genomförandeförordningen (EU) 2025/849 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller inlämning av information till kommissionen och till samarbetsgruppen för förteckningen över certifierade europeiska digitala identitetsplånböcker. I genomförandeförordningen föreskrivs det närmare om hur uppgifterna ska tillhandahållas samt om vilka uppgifter som ska meddelas. Medlemsstaterna kan besluta vilken aktör som i praktiken tillhandahåller kommissionen och samarbetsgruppen uppgifterna.

I anslutning till medlemsstaternas skyldigheter föreskrivs det i artikel 5e i den reviderade eIDAS-förordningen om säkerhetsincidenter som rör europeiska digitala identitetsplånböcker. Enligt artikel 5e.1 ska en medlemsstat i samband med en säkerhetsincident utan onödigt dröjsmål tillfälligt upphäva tillhandahållandet och användningen av europeiska digitala identitetsplånböcker eller när det är motiverat mot bakgrund av allvaret i säkerhetsincidenten återkalla europeiska digitala identitetsplånböcker som blivit utsatta för säkerhetsincidenten utan onödigt dröjsmål. Enligt artikel 5e.2 ska medlemsstaterna återkalla plånböckerna även i det fall att säkerhetsincidenten eller äventyrandet inte har åtgärdats inom tre månader från att plånböckerna tillfälligt upphävdes. Medlemsstaten ska dessutom informera de berörda användarna, de gemensamma kontaktpunkter som utsetts i enlighet med den reviderade eIDAS-förordningen, de förlitande parterna och kommissionen om en situation i enlighet med samtliga punkter i artikeln. Dessutom har kommissionen med stöd av artikel 5e.5 antagit genomförandeförordningen (EU) 2025/847 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller åtgärder mot säkerhetsincidenter som rör europeiska digitala identitetsplånböcker. I genomförandeförordningen föreskrivs det t.ex. om kriterierna för bedömning av en säkerhetsincident eller ett äventyrande samt om tillfälligt upphävande av tillhandahållandet och användningen av plånböcker samt om andra åtgärder. Medlemsstaterna kan själva ange vilken aktör i medlemsstaten som ansvarar för fullgörandet av de skyldigheter som åläggs medlemsstaterna i artikeln och genomförandeförordningen. Till övriga delar ingår det inget nationellt handlingsutrymme i fråga om säkerhetsincidenter och anmälan av dem.

I artikel 5f i den reviderade eIDAS-förordningen föreskrivs det om e-tjänsternas skyldighet att godta europeiska digitala identitetsplånböcker i sina tjänster. I artikeln föreskrivs det separat om

skyldigheten i fråga om den offentliga och den privata sektorn. Plånboken ska godtas i e-tjänster inom den offentliga sektorn när det i medlemsstaten för användning av tjänsten förutsätts elektronisk identifiering och autentisering. För den privata sektorns del förutsätts det att plånboken godtas när unionslagstiftningen eller den nationella lagstiftningen eller avtalsförpliktelser som gäller en privat förlitande part förutsätter stark autentisering av användaren. Den privata sektorns skyldighet att godta plånboken gäller emellertid inte mikroföretag och små företag. Dessa definieras i artikel 2 i bilagan till kommissionens rekommendation 2003/362/EG. I artikel 5f.3 i den reviderade eIDAS-förordningen konstateras det separat i fråga om de mycket stora onlineplattformar som avses i artikel 33 i Europaparlamentets och rådets förordning (EU) 2022/2065 att dessa måste godta användningen av plånböcker för åtkomst till sina tjänster om tjänsterna kräver användarautentisering. Artikeln innehåller inget nationellt handlingsutrymme för medlemsstaterna.

2.2.2 Gränsöverskridande identitetsmatchning

I artikel 11a i den reviderade eIDAS-förordningen föreskrivs det om gränsöverskridande identitetsmatchning. Enligt artikeln ska medlemsstaterna säkerställa otvetydig identitetsmatchning för fysiska personer när medlemsstaterna agerar som förlitande parter för gränsöverskridande tjänster. Med identitetsmatchning avses enligt artikel 3.55 i den reviderade eIDAS-förordningen en process där uppgifter för personidentifiering eller medel för elektronisk identifiering matchas mot eller kopplas till ett befintligt konto som tillhör samma person. I praktiken handlar identitetsmatchning om att säkerställa att en persons identitet i samband med elektronisk identifiering tillförlitligt alltid kan kopplas till en och samma person. Det handlar ändå inte om att ge en ny registeridentitet, dvs. medlemsstaterna är inte skyldiga att registrera nya identiteter på grundval av artikel 11a. Identitetsmatchning ska göras om en fysisk person använder en metod för elektronisk identifiering eller en europeisk digital identitetsplånbok som har anmälts i enlighet med eIDAS-förordningen.

Skyldigheten gäller endast situationer där en medlemsstat agerar som förlitande part för gränsöverskridande tjänster. Med andra ord gäller skyldigheten till identitetsmatchning endast den offentliga sektorns tjänster. Enligt artikeln ska medlemsstaterna genom tekniska och organisatoriska åtgärder säkerställa en hög skyddsnivå för personuppgifter som används för identitetsmatchning och förhindra profilering av användare. Dessutom har kommissionen med stöd av artikel 11a.3 antagit kommissionens genomförandeförordning (EU) 2025/846 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller gränsöverskridande identitetsmatchning av fysiska personer. Medlemsstaterna får själva ange om de genomför identitetsmatchningen som en centraliserad lösning eller om samtliga e-tjänster inom den offentliga sektorn genomför matchningen själva. Medlemsstaterna kan om de så vill genomföra identitetsmatchningen även i fråga om den privata sektorns e-tjänster, men det är inte obligatoriskt.

2.2.3 Certifiering av system för elektronisk identifiering

Enligt artikel 12a i den reviderade eIDAS-förordningen kan medlemsstaterna genom certifiering styrka att det elektroniska system för identifiering som ska anmälas överensstämmer med kraven. Då tillämpas inte den sakkunnigbedömning som avses i förordningens artikel 12.5, som för närvarande har varit det sätt på vilket det har styrkts att det system för elektronisk identifiering som ska anmälas har överensstämt med kraven. Certifieringen kan göras av organ för bedömning av överensstämmelse som utsetts av medlemsstaterna. Enligt artikel 3.18 i den reviderade eIDAS-förordningen avses med organ för bedömning av överensstämmelse ett organ för bedömning av överensstämmelse enligt definitionen i artikel 2.13 i förordning (EG) nr 765/2008 som i enlighet med den förordningen är ackrediterat som behörigt att certifiera bl.a.

metoder för elektronisk identifiering. I den reviderade eIDAS-förordningen föreskrivs det inte om närmare krav på organ för bedömning av överensstämmelse eller hur de utses, varvid dessa anges av medlemsstaterna. Certifieringen ska utföras inom ramen för en relevant ordning för cybersäkerhetscertifiering enligt förordning (EU) 2019/881 eller delar därav i den mån cybersäkerhetssystemet eller dess delar omfattar dessa cybersäkerhetskrav. Certifieringen är i kraft i fem år förutsatt att det görs en sårbarhetsbedömning vartannat år.

2.2.4 Betrodda tjänster

I kapitel III i eIDAS-förordningen föreskrivs om betrodda tjänster. Kapitlet innehåller flera avsnitt som omfattar artiklarna 13–45 i. I artikel 16 i den reviderade eIDAS-förordningen föreskrivs det om sanktioner för tillhandahållare av betrodda tjänster. Enligt artikel 16.1 i den förordningen ska medlemsstaterna fastställa bestämmelser om sanktioner som ska gälla vid överträdelser av förordningen. Sanktionerna ska vara effektiva, proportionella och avskräckande. Enligt artikel 16.2 ska medlemsstaterna säkerställa att överträdelser av den förordningen som begås av tillhandahållare av betrodda tjänster medför administrativ sanktionsavgift. Dessutom ställer artikeln ett minimikrav för de maximala administrativa sanktionsavgifter som påförs nationellt. Om en tillhandahållare av betrodda tjänster är en fysisk person ska den maximala administrativa sanktionsavgiften vara minst 5 000 000 euro. Om tillhandahållaren av betrodda tjänster är en juridisk person, får den administrativa sanktionsavgift som påförs tillhandahållaren vara högst 5 000 000 euro eller en procent av den globala årsomsättningen för det företag till vilket tillhandahållaren av betrodda tjänster hörde under det räkenskapsår som föregick överträdelseåret, beroende på vilket som är störst.

Artikel 16 i den reviderade eIDAS-förordningen ger således medlemsstaterna nationellt handlingsutrymme när det gäller hur påföljderna i medlemsstaterna genomförs. Medlemsstaterna kan således i princip själva besluta om sanktionerna genomförs som administrativa påföljdsavgifter eller straffrättsliga straff. Det nationella handlingsutrymmet begränsas emellertid av artikel 16.2 som förpliktar medlemsstaterna att säkerställa att påföljden för överträdelser av förordningen som begås av kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster är administrativ påföljdsavgift. I förordningen specificeras inte vilken typ av överträdelse av skyldigheterna som kan leda till påföljdsavgift, men utgångspunkten i förordningen är att varje överträdelse av skyldigheterna i förordningen ska förenas med en påföljdsavgift. Förordningen kan dock anses lämna medlemsstaterna nationellt handlingsutrymme genom att de ska fastställa vilka av skyldigheterna enligt förordningen som förenas med myndighetens behörighet att påföra en påföljdsavgift.

I artikel 19a i förordningen föreskrivs det om krav som gäller icke-kvalificerade tillhandahållare av betrodda tjänster. I artikel 19a.1 a föreskrivs det om de verksamhetsprinciper som en icke-kvalificerad tillhandahållare åtminstone ska följa. Sådana är t.ex. registrerings- och anslutningsförfaranden för en betrodd tjänst. I artikel 19a.1 b föreskrivs det om den skyldighet en icke-kvalificerad tillhandahållare av betrodda tjänster har att anmäla säkerhetsincidenter till tillsynsorganet, de identifierbara berörda personerna och allmänheten om det är av allmänt intresse och, om tillämpligt, andra behöriga myndigheter. Kommissionen ska upprätta en förteckning över referensstandarder och fastställa standarder genom att anta genomförandeförordningar i anslutning till 1 a punkten i artikeln.

I artikel 45 i den reviderade eIDAS-förordningen föreskrivs det om krav på kvalificerade certifikat för autentisering av webbplatser. Enligt den nya artikeln 45.1 a ska kvalificerade certifikat för autentisering av webbplatser som utfärdats i enlighet med punkt 1 erkännas av tillhandahållare av webbläsare. Enligt den nya artikeln 45.1 b ska kvalificerade certifikat för autentisering av webbplatser inte omfattas av några obligatoriska krav utöver de krav som

fastställs i punkt 1. I den nya artikeln 45a föreskrivs det emellertid om säkerhetsåtgärder för cybersäkerhet, med vilka tillhandahållare av webbläsare kan vidta säkerhetsåtgärder om tillhandahållaren har väl underbyggda farhågor om säkerhetsincidenter eller integritetsförlust hos ett identifierat certifikat eller en identifierad uppsättning certifikat.

Artiklarna 45b–45h i den reviderade eIDAS-förordningen har bestämmelser om elektroniska attributsintyg. Det handlar om en ny betrodd elektronisk tjänst som har inkluderats i förordningens tillämpningsområde. I artiklarna föreskrivs det om elektroniska attributsintygs rättsliga verkan, användning av elektroniska attributsintyg i offentliga tjänster, krav på kvalificerade elektroniska attributsintyg, kontroll av attribut mot autentiska källor, krav på elektroniska attributsintyg utfärdade av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa, utfärdande av elektroniska attributsintyg till europeiska digitala identitetsplånböcker samt om ytterligare regler för tillhandahållande av tjänster för elektroniska attributsintyg. Kommissionen har dessutom med stöd av artikel 45e.2 antagit genomförandeförordningen (EU) 2025/1569 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller kvalificerade elektroniska attributsintyg och elektroniska attributsintyg som tillhandahålls av eller på uppdrag av ett offentligt organ som ansvarar för en autentisk källa.

Sett i perspektiv av det nationella genomförandet är i synnerhet artikel 45e om kontroll av attribut mot autentiska källor central. Enligt den ska medlemsstaterna, åtminstone för vissa attribut som förtecknas i bilaga VI, när dessa attribut baseras på autentiska källor, inom offentliga sektorn vidta åtgärder som gör det möjligt för kvalificerade tillhandahållare av betrodda tjänster för elektroniska attributsintyg att på användarens begäran på elektronisk väg kontrollera dessa attribut. Med autentisk källa avses enligt artikel 3.47 en samlingsplats eller system, som innehas under ansvar av ett offentligt organ eller en privat enhet, som innehåller och tillhandahåller attribut om en fysisk eller juridisk person eller ett föremål och som anses vara en primärkälla för den informationen eller erkänns som autentisk i enlighet med unionsrätten eller nationell rätt, inbegripet administrativa förfaranden. De uppgifter som förtecknas i bilaga VI till förordningen är adress, ålder, kön, civilstånd, nationalitet eller medborgarskap och offentliga tillstånd och licenser. Medlemsstaterna kan i stor utsträckning själva erkänna vad som är en autentisk källa för en viss uppgift.

I artiklarna 45i och 45j i den reviderade eIDAS-förordningen föreskrivs det om elektroniska arkiveringstjänster och i artiklarna 45k och 45l om elektroniska liggare. Det handlar om nya betrodda tjänster som har inkluderats i förordningens tillämpningsområde. I artiklarna föreskrivs det om dessa betrodda tjänsters rättsliga verkan samt om krav som ska följas när dessa betrodda tjänster tillhandahålls som kvalificerade betrodda tjänster.

2.2.5 Styrningsramverk

I den reviderade eIDAS-förordningen finns bestämmelser om tillsynen och den gemensamma kontaktpunkten samt den nya samarbetsgruppen samlade i kapitel IV a i slutet av förordningen. Bestämmelser om tillsynen över ramverket för den europeiska digitala identitetsplånboken finns i artikel 46a. Enligt den ska medlemsstaterna utse ett tillsynsorgan som är etablerat på deras territorium och det ska ges nödvändiga befogenheter och adekvata resurser för att kunna utföra sina uppgifter på ett ändamålsenligt, effektivt och oberoende sätt. Tillsynsorganet ska bl.a. utöva tillsyn över tillhandahållare av europeiska digitala identitetsplånböcker etablerade i den medlemsstat där det har utsetts och, genom tillsynsverksamhet på förhand och i efterhand, säkerställa att dessa tillhandahållare och de europeiska digitala identitetsplånböcker som de tillhandahåller uppfyller kraven i förordningen. I tillsynsorganets uppgifter ingår i synnerhet att begära information som är nödvändig för att övervaka efterlevnaden av förordningen, utföra

inspektioner på plats och utöva tillsyn på distans, kräva åtgärdande av brister vid underlåtenhet att uppfylla kraven samt tillfälligt eller permanent upphäva registreringen av förlitande parter. Tillsynsorganet kan också i vissa fall ålägga tillhandahållaren att tillfälligt eller permanent upphöra med tillhandahållandet av plånboken. Medlemsstaterna ska således utse ett tillsynsorgan och säkerställa nationellt att det har tillräckliga befogenheter för att utföra de tillsynsuppgifter som föreskrivs i förordningen.

Redan före revideringen förutsatte eIDAS-förordningen att medlemsstaterna utser ett tillsynsorgan för betrodda tjänster och om detta föreskrevs det tidigare i artikel 17. Artikel 17 har emellertid upphävts i den reviderade eIDAS-förordningen och framöver föreskrivs det om tillsynen över betrodda tjänster och tillhandahållarna av dem i den nya artikeln 46b. Innehållet i den motsvarar till stor del den tidigare artikeln 17.

I artikel 46c i förordningen föreskrivs det om gemensamma kontaktpunkter. Medlemsstaterna ska utse en gemensam kontaktpunkt för betrodda tjänster, europeiska digitala identitetsplånböcker och anmälda system för elektronisk identifiering. Den gemensamma kontaktpunkten ska utöva en sambandsfunktion för att underlätta gränsöverskridande samarbete mellan tillsynsorganen samt andra behöriga myndigheter i sin medlemsstat, kommissionen och Europeiska unionens cybersäkerhetsbyrå.

I artikel 46e i den reviderade eIDAS-förordningen föreskrivs det om den europeiska samarbetsgruppen för digital identitet (nedan *samarbetsgrupp*). Gruppens syfte är att stödja och underlätta medlemsstaternas gränsöverskridande samarbete och informationsutbyte om betrodda tjänster, europeiska digitala identitetsplånböcker och anmälda system för elektronisk identifiering. Samarbetsgruppen ska bl.a. samarbeta med kommissionen om nya politiska initiativ på området digitala identitetsplånböcker, medel för elektronisk identifiering och betrodda tjänster samt vid behov ge kommissionen råd vid utarbetandet av utkast till genomförandeakter och delegerade akter som ska antas enligt eIDAS-förordningen. Dessutom ska samarbetsgruppen stödja tillsynsorganen bl.a. genom att utbyta bästa praxis och information om genomförandet av bestämmelserna i förordningen samt bedöma den relevanta utvecklingen inom sektorerna för digitala identitetsplånböcker, elektronisk identifiering och betrodda tjänster. Kommissionen bad redan vid tiden för beredningen av propositionen medlemsstaterna utse medlemmar till samarbetsgruppen och samarbetsgruppen har inlett sitt arbete. Myndigheten för digitalisering och befolkningsdata företräder Finland i samarbetsgruppen.

2.2.6 Rapporteringskrav

I artikel 48a i den reviderade eIDAS-förordningen föreskrivs om de rapporteringskrav som ställs på medlemsstaterna. Medlemsstaterna ska säkerställa att det samlas in statistik om hur de plånböcker och kvalificerade betrodda tjänster som tillhandahålls på deras territorium används. Den statistik som samlas in ska omfatta bl.a. antalet fysiska och juridiska personer som har en giltig plånbok, antalet tjänster som godtar användning av plånböcker samt en sammanfattning av betydande säkerhetsincidenter, dataöverträdelser och berörda användare av plånböcker eller kvalificerade betrodda tjänster. Kommissionen ska tillställas en rapport om statistiken årligen. Medlemsstaten ska bedöma hur uppgifterna samlas in och offentliggörs samt vilken aktör som lämnar uppgifterna till kommissionen.

3 Nuläge och bedömning av nuläget

3.1 Genomförande av den reviderade eIDAS-förordningen

3.1.1 Nuläget i fråga om stark autentisering

I fråga om stark autentisering föreskrivs det i eIDAS-förordningen om ett gränsöverskridande system för interoperabilitet i elektronisk identifiering. Förordningen gör det möjligt för medlemsstaterna att anmäla det nationella systemet för elektronisk identifiering till kommissionen, dvs. notifiera kommissionen. Det är möjligt att använda ett anmält system för elektronisk identifiering för att uträtta ärenden inom den offentliga förvaltningen i andra medlemsländer. I eIDAS-förordningen och genomförandeförordningar som antagits av kommissionen med stöd av den anges tre tillitsnivåer för identifieringssystemen: låg, väsentlig och hög. Medlemsstaterna ska i sin tur godkänna att sådana identifieringssystem som en annan medlemsstat har anmält och vilkas tillitsnivå motsvarar den som gäller nationellt i landet i fråga används för uträttande av ärenden i deras offentliga förvaltning.

Det föreskrivs om identifieringsverktyg som används nationellt för stark autentisering i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009, nedan *autentiseringslagen*). Syftet med lagen är att genom reglering främja en marknadsbaserad utveckling av stark autentisering i Finland. Ett annat centralt mål med lagen är att främja säkerheten hos e-tjänster och vid anlitaandet av tjänster genom att utöka användningen av stark autentisering. Autentiseringslagen inkluderar en definition av stark autentisering samt mer ingående krav på elektroniska identifieringsverktyg. Det krävs minst samma tillförlitlighet och informationssäkerhet av identifieringsverktygen som eIDAS-förordningen kräver av gränsöverskridande system för elektronisk identifiering på tillitsnivån väsentlig.

I autentiseringslagen föreskrivs det dessutom om ett förtroendenät för leverantörer av identifieringstjänster. Leverantörer av identifieringstjänster ska innan verksamheten inleds göra en skriftlig anmälan till Transport- och kommunikationsverket och de leverantörer av identifieringstjänster som gjort anmälan bildar direkt med stöd av lagen ett förtroendenät för elektronisk identifiering. Det finns två slags leverantörer av identifieringstjänster: leverantörer av identifieringsverktyg och leverantörer av tjänster för identifieringsförmedling. Med leverantörer av identifieringsverktyg avses aktörer som tillhandahåller identifieringsverktyg för stark identifiering till användarna, dvs. fysiska personer och juridiska personer. Med leverantörer av tjänster för identifieringsförmedling avses i sin tur de aktörer som förmedlar identifieringstransaktioner till e-tjänster. Leverantörer av tjänster för identifieringsförmedling ingår avtal med leverantörer av identifieringsverktyg om att de får förmedla identifieringstransaktioner som görs med identifieringsverktyg till e-tjänster. Samma tjänsteleverantör kan vara leverantör av både verktyg och förmedlingstjänst. I autentiseringslagen föreskrivs det om de skyldigheter som hänför sig till identifieringstjänsteleverantörernas verksamhet i förtroendenätet, såsom leverantörernas skyldigheter att tillhandahålla tjänster och samarbeta sinsemellan, maximipriserna för identifieringstransaktioner samt skyldigheten att bedöma att ett identifieringsverktyg överensstämmer med kraven. Transport- och kommunikationsverket utövar tillsyn över efterlevnaden av den lagen.

Med hjälp av stark autentisering kan konsumenterna tryggt styrka sin identitet i olika e-tjänster och dessutom kan leverantörer av e-tjänster identifiera sina kunder. Förtroendenätet bildar i praktiken en marknad för stark autentisering för e-tjänster, som e-handel och e-tjänster inom den offentliga förvaltningen. I stället för att en e-tjänst ingår avtal med samtliga leverantörer av identifieringstjänster kan den centralt hos förtroendenätet skaffa sig stark autentisering. För

närvarande är Myndigheten för digitalisering och befolkningsdata en betydande enskild köpare av identifieringstjänster som centralt förmedlar identifieringstjänster för den offentliga förvaltningen via identifieringstjänsten Suomi.fi. Aktörer inom den offentliga förvaltningen är ofta genom lagstiftning förpliktade att använda stark autentisering i sina e-tjänster där personuppgifter eller annars sekretessbelagd information behandlas.

De identifieringsverktyg för stark autentisering som för närvarande används i Finland är bankkoder som bankerna tillhandahåller, teleföretagens mobilcertifikat och Megical Oy:s Hightrust.id. Starka identifieringsverktyg är dessutom det medborgarcertifikat som beviljas av Myndigheten för digitalisering och befolkningsdata och som finns på det identitetskort som polisen beviljar och det organisationscertifikat som finns på organisationskort som Myndigheten för digitalisering och befolkningsdata beviljar. Finland inledde processen för att anmäla medborgarcertifikatet i enlighet med eIDAS-förordningen för gränsöverskridande identifiering i december 2023. Sakkunnigbedömningen av medborgarcertifikatet har avslutats och den resulterade i att certifikatet godkändes för gränsöverskridande elektronisk identifiering på tillitsnivån hög. Den officiella notifikationen har gjorts och meddelandet om det ingick i EU:s officiella tidning den 25 april 2025. Inga andra nationella identifieringsverktyg har anmälts för gränsöverskridande elektronisk identifiering.

Trots att autentiseringslagen gör det möjligt att tillhandahålla identifieringsverktyg till både fysiska och juridiska personer, finns det inte i det register över leverantörer av identifieringstjänster som Transport- och kommunikationsverket förvaltar en enda leverantör av identifieringstjänster som skulle tillhandahålla juridiska personer identifieringsverktyg för stark autentisering. Den motsvarighet som kommer närmast stark autentisering av juridiska personer torde vara servercertifikat som i tiotals år har använts vid etablering av anslutningar på WWW- och VPN-servrar. När anslutningen till servern etableras säkerställer WWW-servern att servern använder ett giltigt certifikat för DNS-namnet i fråga (t.ex. www.vero.fi). När servercertifikatet beviljas kontrollerar certifikatutfärdaren åtminstone att den som ansöker om certifikatet har rätt till DNS-namnet (domain validated certificate) och kontrollerar inom ramen för sin praxis eventuellt också uppgifter om den (juridiska) person som äger DNS-namnet.

I stället för stark autentisering av juridiska personer har det etablerats en praxis där en e-tjänst identifierar en fysisk person som loggar in för ett företags del med sitt eget personliga identifieringsverktyg varefter e-tjänsten separat verifierar personens rätt att agera för företagets del. Till detta anknyter fullmaktstjänsten Suomi.fi som tillhandahålls av Myndigheten för digitalisering och befolkningsdata. Både offentliga och privata organisationer kan utnyttja Suomi.fi-fullmakter. E-tjänster som utnyttjar Suomi.fi-fullmakter ska i princip identifiera användarna med hjälp av stark autentisering. E-tjänsten (t.ex. MinSkatt) kontrollerar via gränssnittet i Suomi.fi-fullmakterna om den fysiska personen har rätt att företräda företaget.

3.1.2 Nuläget ifråga om betrodda tjänster

I eIDAS-förordningen föreskrivs det även om betrodda elektroniska tjänster. Med betrodda tjänster möjliggörs förtroende för elektroniska handlingar och elektroniska processer. De kan nödvändigtvis inte alltid ses av användaren, utan är dolda i tjänsternas struktur. Med hjälp av dem kan man t.ex. försäkra sig om att en viss elektronisk åtgärd har vidtagits vid en viss tidpunkt eller att leverantören av e-tjänsten är den vederbörande utger sig för att vara. Betrodda elektroniska tjänster är t.ex. elektronisk underskrift samt elektronisk stämpel och olika certifikat.

Den som tillhandahåller en betrodd tjänst och den tillhandahållna betrodda tjänsten kan enligt eIDAS-förordningen vara antingen kvalificerad eller icke-kvalificerad. Förordningen ställer

särskilt på kvalificerade tillhandahållare av betrodda tjänster och på kvalificerade betrodda tjänster krav vilkas syfte är att öka deras tillförlitlighet. Tillhandahållare av kvalificerade betrodda tjänster ska t.ex. informera det nationella tillsynsorganet om sin avsikt att börja tillhandahålla en kvalificerad betrodd tjänst samt regelbundet skaffa en bedömning av ett organ för bedömning av överensstämmelse om huruvida den tjänst de tillhandahåller uppfyller kraven i eIDAS-förordningen. Dessutom förutsätter eIDAS-förordningen att kvalificerade tillhandahållare av betrodda tjänster och de tjänster de tillhandahåller övervakas genom åtgärder som vidtas både på förhand innan tjänsterna börjar tillhandahållas och i efterhand. Dessutom fastställer och offentliggör de nationella tillsynsmyndigheterna de kvalificerade betrodda tjänster som tillhandahålls i enlighet med förordningens krav i en betrodd förteckning.

Den för närvarande enda kvalificerade tillhandahållaren av betrodda tjänster i Finland är Myndigheten för digitalisering och befolkningsdata. De kvalificerade betrodda tjänster den tillhandahåller är kvalificerade certifikat för elektroniska underskrifter samt kvalificerade certifikat för autentisering av webbplatser, dvs. så kallade servercertifikat. Bestämmelser om Myndigheten för digitalisering och befolkningsdatas certifikattjänster finns i lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata (661/2009, nedan *lagen om befolkningsdatasystemet*). I 6 kap. i lagen om befolkningsdatasystemet föreskrivs det om certifierad elektronisk kommunikation som Myndigheten för digitalisering och befolkningsdata ansvarar för och i kapitlets 61 § föreskrivs om tjänster som tillhandahålls vid certifierad elektronisk kommunikation. Enligt 61.1 § ska Myndigheten för digitalisering och befolkningsdata producera, tillhandahålla och administrera medborgarcertifikat som är avsedda att användas vid certifierad elektronisk kommunikation samt certifikatregistrertjänster och spärllisttjänster som direkt hänför sig till användningen av medborgarcertifikat.

Med medborgarcertifikat avses ett certifikat som utfärdats av Myndigheten för digitalisering och befolkningsdata för en fysisk person och som ingår i ett i lagen om identitetskort (663/2016) avsett identitetskort eller i en annan myndighetshandling eller ett tekniskt underlag och som används för verifiering av personen, för elektroniska underskrifter och för kryptering av handlingar och meddelanden. Med medborgarcertifikat avses också ett av Myndigheten för digitalisering och befolkningsdata utfärdat certifikat som ingår i en annan myndighetshandling eller ett tekniskt underlag och som används i ovannämnda syfte och som uppfyller kraven i eIDAS-förordningen. I praktiken kan medborgarcertifikatet således användas för flera ändamål, dvs. stark autentisering, som det beskrivs i avsnitt 3.1.1 ovan, eller som betrodd tjänst för elektronisk underskrift eller kryptering av handlingar och meddelanden.

Ikke-kvalificerade tillhandahållare av betrodda tjänster har inte ålagts samma skyldigheter som kvalificerade tillhandahållare av betrodda tjänster. De har inte samma skyldighet att informera om att de börjar tillhandahålla tjänster och det förutsätts inte heller bedömning av överensstämmelse för de betrodda tjänster de tillhandahåller. Det förs inte heller en betrodd förteckning över ikke-kvalificerade tillhandahållare av betrodda tjänster på motsvarande sätt. Dessutom kan det i fråga om dem endast utövas efterhandstillsyn. Av dessa anledningar har det funnits relativt begränsat med information om ikke-kvalificerade tillhandahållare av betrodda tjänster och de tjänster de tillhandahåller. Tillhandahållare av betrodda tjänster omfattas dock av tillämpningsområdet för cybersäkerhetslagen (124/2025) oavsett om de är kvalificerade eller ikke-kvalificerade tillhandahållare av betrodda tjänster. I 41 § i cybersäkerhetslagen sägs det att tillsynsmyndigheten i fråga om sitt tillsynsområde för en förteckning över aktörerna. Förteckningen över aktörerna grundar sig på uppgifter aktörerna lämnat om sin verksamhet. Också ikke-kvalificerade tillhandahållare av betrodda tjänster ska anmäla sin verksamhet och lämna anmälan till Transport- och kommunikationsverket. Hittills har 17 tillhandahållare av betrodda tjänster lämnat en anmälan, men vid beredningen av propositionen blev bedömningen

att det dock finns avsevärt fler nationella icke-kvalificerade tillhandahållare av betrodda tjänster, uppskattningsvis totalt cirka 50.

Utifrån anmälningarna och sakkunnigbedömningarna kan det konstateras att det tillhandahålls flera olika betrodda tjänster i Finland. Det tillhandahålls t.ex. flera betrodda tjänster för elektronisk underskrift och elektronisk stämpel och eventuellt även elektroniska tjänster för rekommenderade leveranser samt elektroniska arkiveringstjänster. Storleken på tillhandahållarna av betrodda tjänster varierar från medelstora till små aktörer. Det är möjligt att alla aktörer inte själva uppmärksammat att det i deras tjänst handlar om tillhandahållandet av en betrodd tjänst.

Bestämmelser om den nationella tillsynsmyndigheten över betrodda tjänster, bedömningen av tjänsternas överensstämmelse med kraven samt vissa andra omständigheter i samband med betrodda tjänster finns i autentiseringslagen. Enligt den lagen är Transport- och kommunikationsverket nationell tillsynsmyndighet. I bestämmelserna i autentiseringslagen om betrodda tjänster handlar det om nationella bestämmelser som kompletterar den ursprungliga eIDAS-förordningen och som behövs för att genomföra skyldigheterna i förordningen. Genomförandet av den ursprungliga eIDAS-förordningen beskrivs närmare i avsnitt 3.1.4.

3.1.3 Nuläget i fråga om plånbokslösningar

Som det beskrivs ovan i avsnitt 2.2.1 föreskrivs det i den reviderade eIDAS-förordningen om en europeisk digital identitetsplånbok som kombinerar elektronisk identifiering och betrodda tjänster. Med plånboken blir det möjligt att omfattande identifiera sig i e-tjänster på samma sätt som med de nuvarande identifieringsverktygen för stark autentisering. Dessutom ska det vara möjligt att göra kvalificerade elektroniska underskrifter. Det ska också vara möjligt att med plånboken använda de nya betrodda tjänsterna enligt den reviderade eIDAS-förordningen, dvs. elektroniska attributsintyg. Elektroniska attributsintyg kan innehålla en mycket bred uppsättning av olika uppgifter om användaren, som uppgifter om giltig körkort, jaktlicens eller gymmedlemskap.

Finland har ingen nationell lagstiftning för plånbokslösningar motsvarande plånböckerna i eIDAS-förordningen. I autentiseringslagen föreskrivs det på det sätt som beskrivs i avsnitten 3.1.1 och 3.1.2 om stark autentisering och betrodda tjänster. Plånböckerna handlar emellertid om ett större koncept, och plånboken kan inte reduceras endast till ett verktyg för stark autentisering eller en betrodd tjänst. Transport- och kommunikationsverkets gällande anvisning om bedömning av elektroniska identifieringstjänster (211/2023 O) använder termen plånbok om sådana elektroniska identifieringsverktyg som vid sidan av elektronisk identifiering även kan innehålla kapaciteter som kännetecknar plånböcker som elektronisk underskrift eller behandling av bevis. Dessa är ändå inte europeiska digitala identitetsplånböcker enligt eIDAS-förordningen och det finns således ingen nationell lagstiftning för plånböckerna. I plånböcker enligt den reviderade eIDAS-förordningen handlar det således om en ny helhet sett ur den nationella lagstiftningens perspektiv.

Det tillhandahålls dock plånbokslösningar som bygger på liknande grundläggande principer som plånböckerna enligt eIDAS-förordningen. Det gemensamma för dem är vanligtvis administration och delning av olika digitala bevis och uppgifter. För närvarande möjliggör de vanligtvis inte stark autentisering eller elektronisk underskrift. Det handlar dock om en verksamhet som utvecklas och det är möjligt att det framöver kan uppkomma andra plånbokslösningar parallellt med plånböckerna i enlighet med eIDAS-förordningen. Det är ändå inte sannolikt att de kan användas i gränsöverskridande e-tjänster på samma sätt som plånböckerna enligt eIDAS-förordningen, men samtidigt är de inte heller bundna till kraven

enligt eIDAS-förordningen. Det är således möjligt att andra plånbokslösningar avviker avsevärt från plånböckerna enligt eIDAS-förordningen både till egenskaper och användning.

3.1.4 Genomförandet av den ursprungliga eIDAS-förordningen

Den kompletterande nationella lagstiftning som behövs för att tillämpa eIDAS-förordningen och fullfölja skyldigheterna finns för närvarande i autentiseringslagen. Enligt 1 § 2 mom. i autentiseringslagen föreskrivs det i lagen om tillsynen över efterlevnaden av eIDAS-förordningens bestämmelser samt utfärdas i den bestämmelser som kompletterar den förordningen. Dessutom innehåller lagen bestämmelser om bedömning av överensstämmelsen med kraven när det gäller identifieringstjänster och betrodda tjänster. De ändringar i den nationella lagstiftningen som den ursprungliga eIDAS-förordningen förutsätter trädde i kraft den 1 juli 2016.

I fråga om stark autentisering handlade ändringarna särskilt om harmonisering av kraven på de nationella identifieringsverktygen för stark autentisering med kraven i eIDAS-förordningen. Det här var ett nationellt legislativt val eftersom eIDAS-förordningen gäller endast gränsöverskridande elektronisk identifiering och inte förutsätter att identifieringsverktyg som endast används i nationella tjänster uppfyller kraven i förordningen. Till följd av ändringarna gäller minst samma krav på tillförlitlighet och informationssäkerhet hos de system för stark autentisering som tillhandahålls i Finland som eIDAS-förordningen och genomförandeförordningarna kräver av gränsöverskridande system för elektronisk identifiering med tillitsnivån väsentlig. Harmoniseringen av kraven hade som mål att underlätta för aktörerna inom stark autentisering i Finland att söka s.k. status som gränsöverskridande identifieringsverktyg för sina verktyg (RP 74/2016 rd, s. 12). Som ett nytt krav på leverantörer av identifieringstjänster i Finland föreskrevs dessutom om skyldigheten till en bedömning av identifieringstjänsternas överensstämmelse med kraven.

Beträffande stark autentisering fick Transport- och kommunikationsverket (då Kommunikationsverket) nya uppdrag i anslutning till det interoperabilitetssystem för elektronisk identifiering mellan medlemsstaterna som det föreskrivs om i eIDAS-förordningen. Transport- och kommunikationsverket ska bl.a. delta i samarbetet mellan EU:s medlemsstater och anmäla system för elektronisk identifiering till Europeiska kommissionen i enlighet med eIDAS-förordningen. Myndigheten för digitalisering och befolkningsdata (då Befolkningsregistercentralen) fick i uppgift att i Finland bygga och upprätthålla en nationell s.k. nod som bildar ett gränssnitt för de andra EU-staternas identifieringsverktyg när de används i finländska e-tjänster för ärendehantering.

För de betrodda tjänsternas del innehöll autentiseringslagen tidigare bestämmelser om elektronisk underskrift som grundade sig på Europaparlamentets och rådets direktiv 1999/93/EG om ett gemenskapsramverk för elektroniska signaturer. Direktivet upphävdes med den ursprungliga eIDAS-förordningen varvid autentiseringslagen ändrades till denna del. I fråga om betrodda tjänster föreskrevs det dessutom att Transport- och kommunikationsverket övervakar att de nationella tillhandahållarna av betrodda tjänster följer bestämmelserna i eIDAS-förordningen. Dessutom föreskrevs för verket uppgiften att föra och publicera förteckningar över kvalificerade tillhandahållare av betrodda tjänster i Finland och de kvalificerade betrodda tjänster som de tillhandahåller. Dessutom infördes kompletterande bestämmelser om bedömningen av överensstämmelse avseende tillhandahållare av betrodda tjänster som ingår i 4 kap. i lagen, samt om återkallande av certifikat (39 §), ansvar för obehörig användning av framställningsdata för en underteckning eller elektronisk stämpel (40 §) samt det ansvar som vilar på tillhandahållare av betrodda tjänster (41 §). Motsvarande ansvarsbestämmelser ingick inte i eIDAS-förordningen.

3.1.5 Bedömning

På grund av den reviderade eIDAS-förordningen behöver det inte göras ändringar i de krav som gäller nationell stark autentisering. Också den reviderade eIDAS-förordningen gäller i fråga om elektronisk identifiering endast ömsesidigt erkännande av systemen för elektronisk identifiering vid gränsöverskridande tjänster. De nationella kompletterande bestämmelserna i dessa frågor utfärdades redan i samband med att den ursprungliga eIDAS-förordningen genomfördes. Den reviderade eIDAS-förordningen har inte påverkat kraven på systemen för elektronisk identifiering på olika tillitsnivåer och om dem föreskrivs fortfarande i kommissionens genomförandeförordning (EU) 2015/1502 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (nedan *förordningen om tillitsnivåer vid elektronisk identifiering*). De nationella kraven på stark autentisering behöver således inte heller ur detta perspektiv ses över på nytt.

Bestämmelserna om den europeiska digitala identitetsplånboken i den reviderade eIDAS-förordningen bedöms inte medföra några egentliga ändringar i den nationella regleringen om stark elektronisk autentisering. Det har föreskrivits uttömmande om plånboken och kraven på tillhandahållandet av den i den reviderade eIDAS-förordningen och det är inte möjligt att ställa ytterligare nationella krav. Sålunda omfattas de europeiska digitala identitetsplånböckerna och tillhandahållarna av dem inte av de nationella bestämmelserna om stark autentisering och den nationella lagstiftningen (inkl. bestämmelserna om förtroendenätet) förblir oförändrad. I praktiken innebär detta att de europeiska digitala identitetsplånböckerna bildar ett parallellt system till förtroendenätet för nationell stark autentisering och kraven i det härrör från den reviderade eIDAS-förordningen och de genomförandeförordningar som kommissionen antagit med stöd av den.

Artikel 5f i den reviderade eIDAS-förordningen förutsätter att både den offentliga sektorn och den privata sektorn i vissa fall godtar identifiering med den europeiska digitala identitetsplånboken (se närmare avsnitt 2.2.1). Det är motiverat att e-tjänster ska kunna utnyttja redan befintliga nationella gränssnitt för stark autentisering i stället för att utveckla nya gränssnitt. Eftersom de europeiska digitala identitetsplånböckerna inte omfattas av det nationella förtroendenätet för stark autentisering behöver det föreskrivas separat om möjligheten för de nuvarande leverantörerna av tjänster för identifieringsförmedling att förmedla identifiering baserad på dessa plånböcker. På samma sätt ska det föreskrivas att man i identifieringstjänsten Suomi.fi som förvaltas av Myndigheten för digitalisering och befolkningsdata, dvs. identifieringstjänsten för fysiska personer, (nedan även *Suomi.fi-identifiering*) med vilken stark autentisering förmedlas till den offentliga sektorns e-tjänster, kan förmedla även identifiering som baserar sig på en plånbok. I vilket fall som helst ska e-tjänster alltid ha möjlighet att bygga ett direkt gränssnitt för utnyttjande av identifiering utifrån plånböcker, även om det är möjligt att använda de nuvarande gränssnitten för stark autentisering.

I fråga om betrodda tjänster behövs det egentligen inga ändringar i den giltiga nationella lagstiftning som kompletterar eIDAS-förordningen. Kraven på de betrodda tjänsterna som reglerades redan i den ursprungliga eIDAS-förordningen ändrades inte och således behövs kompletterande nationell lagstiftning om dem fortfarande. I fråga om betrodda tjänster och tillhandahållarna av dem är Transport- och kommunikationsverket tillsynsmyndighet. Bestämmelserna om tillsynen över de betrodda tjänsterna och tillhandahållarna av dem i den reviderade eIDAS-förordningen motsvarar till innehållet till stora delar de ursprungliga

bestämmelserna om tillsyn. Sålunda behöver den nationella lagstiftningen om betrodda tjänster och tillhandahållarna av dem inte ändras.

Till följd av den reviderade eIDAS-förordningen behöver det dock till vissa delar utfärdas helt ny kompletterande nationell reglering i fråga om vissa delar. Det har tidigare inte varit möjligt att påföra tillhandahållare av betrodda tjänster administrativa påföljdsavgifter för överträdelser av skyldigheterna i förordningen och framöver ska det föreskrivas om dem i nationell lagstiftning. Dessutom behöver det utfärdas nationella bestämmelser om vilken aktör som vidtar de åtgärder som avses i artikel 45e i eIDAS-förordningen. Genom dessa åtgärder kan kvalificerade tillhandahållare av betrodda tjänster för elektroniska attributsintyg kontrollera vissa uppgifter direkt mot det register som förvaltas av den offentliga sektorn, dvs. mot en autentisk källa. Åtgärder behöver vidtas i fråga om sådana uppgifter som förtecknas i bilaga VI till förordningen och de är t.ex. ålder, adress, nationalitet och examen samt offentliga tillstånd och licenser.

Europeiska digitala identitetsplånböcker enligt den reviderade eIDAS-förordningen handlar ur ett nationellt lagstiftningsperspektiv om ett nytt koncept och det har inte tidigare föreskrivits nationellt om plånböcker. Tillhandahållandet av plånböcker och relaterade system och tjänster är förknippat med ett flertal skyldigheter för medlemsstaterna. Nationellt behöver det utfärdas preciserande bestämmelser om vilken aktör som ansvarar för genomförandet av vilken i förordningen föreskriven skyldighet i Finland. Det behöver föreskrivas nationellt om t.ex. tillhandahållare av europeiska digitala identitetsplånböcker och om hur man säkerställer skyldigheten enligt den reviderade eIDAS-förordningen att tillhandahålla plånböcker i Finland. Dessutom behövs det bestämmelser om vem som beviljar identifieringsuppgifter för personer, den personuppgiftsansvarige för förlitande parter i fråga om plånböcker samt tillsynsmyndigheten för ramverket för plånboken och myndighetens befogenheter. Som ovan beskrivet innehåller den reviderade eIDAS-förordningen nationellt handlingsutrymme i fråga om öppenheten i plånbokens källkod samt avgifter för elektronisk underskrift. Kompletterande nationella bestämmelser om hur handlingsutrymmet får användas behöver utfärdas. Den reviderade eIDAS-förordningen förutsätter dessutom att identitetsmatchning genomförs. Det handlar om en ny tjänst av sådant slag som inte tidigare har tillhandahållits i Finland. I den nationella lagstiftningen behöver det preciseras vilken aktör som ansvarar för att skyldigheten fullföljs i Finland samt föreskrivas om de övriga eventuella ändringar som regleringen om identitetsmatchning kräver.

Bestämmelser som kompletterar den ursprungliga eIDAS-förordningen har ingått i autentiseringslagen på ovan beskrivet sätt. Vid beredningen av propositionen bedömdes det emellertid att det ur lagtillämparens synvinkel blir tydligast att de nationella kraven på stark autentisering och den reglering som kompletterar eIDAS-förordningen framöver finns i egna lagar. Saken bedöms närmare i avsnitt 5.1.2. Framöver kan tjänsteleverantörer och andra tillämpare av lagen enkelt välja vilken lag som tillämpas utgående från om avsikten är att som leverantör av identifieringstjänster agera endast på nationell nivå eller att leverera tjänster mer omfattande inom EU:s medlemsstaters territorier.

3.2 E-legitimation

Medborgarna och andra som sköter ärenden i Finland behöver styrka sin identitet i olika situationer med traditionella handlingar som pass eller identitetskort. Identifiering av en person kan grunda sig på ett praktiskt behov eller etablerat handlingsätt, men det kan förutsättas även utifrån lagstiftning eller avtal. I t.ex. konsumentskyddslagen (38/1978) föreskrivs det om skyldigheten att kontrollera identiteten omsorgsfullt i konsumentkreditavtal.

Den gällande lagstiftningen har emellertid inga allmänna bestämmelser om med vilka handlingar personuppgifterna kan styrkas eller vilka handlingar som kan godtas för att styrka uppgifter, och i lagstiftningen ingår inte heller begreppet officiell legitimation. Rutinerna grundar sig dels på regleringen om handlingar i likhet med pass och identitetskort som myndigheterna beviljar, dels på myndighets- eller branschspecifik identifieringsreglering, i synnerhet när ärenden sköts vid personliga möten.

Finska pass och identitetskort är handlingar som polisen beviljar och de används allmänt för att styrka personuppgifter. De är även resedokument med vissa undantag som gäller identitetskort. I passlagen (671/2006) och lagen om identitetskort föreskrivs det bl.a. om förutsättningarna för beviljande av handlingarna och identifiering av en person i samband med ansökan. Enligt 3 § i passlagen är pass i första hand resedokument och pass beviljas finska medborgare på ansökan för att styrka rätten att resa. Enligt 1 § i lagen om identitetskort beviljas identitetskort för styrkande av identiteten, men ingendera lagen förpliktar myndigheterna eller andra aktörer att godkänna handlingarna i identifieringssyfte.

Ansökan om både pass och identitetskort kan göras elektroniskt, men den sökande ska personligen infinna sig hos myndigheten för identifiering och komplettering av handlingen. Undantag är situationer där den sökande under de senaste sex åren har beviljats pass eller identitetskort varvid denne personligen infunnit sig hos myndigheten och lämnat de biometriska kännetecken som behövs. Minderåriga kan beviljas handlingarna med vårdnadshavarnas samtycke och i särskilda fall även utan det.

I både identitetskortet och passet antecknas de grundläggande uppgifterna om en person som namn, kön, födelseid, personbeteckning, nationalitet, utfärdandedag och giltighetstid. I båda handlingarna finns också innehavarens ansiktsbild och namnteckning. I passet kan det läggas till uppgift om födelsehemkommun eller anteckningen "utlandet" när hemkommunen inte kan utredas på tillförlitligt sätt.

Båda handlingarna har en teknisk del (chip) där de biometriska kännetecknen som ansiktsbilden och fingeravtrycken lagras. Identitetskort för minderåriga och temporära identitetskort saknar teknisk del i chipet. De biometriska uppgifterna är permanenta och individuella och i behandlingen av dem betonas informationssäkerheten. I Europeiska unionens råds förordning (EU) 2025/1208 om säkrare identitetskort för unionsmedborgare och uppehållshandlingar som utfärdas till unionsmedborgare och deras familjemedlemmar när de utövar rätten till fri rörlighet anges kraven på innehållet i chipet och informationssäkerheten. Kortinnehavaren har rätt att kontrollera och be att korrigeringar görs i de uppgifter som lagrats i den tekniska delen. För skyddet av uppgifter svarar i Finland Myndigheten för digitalisering och befolkningsdata och utrikesministeriet (i fråga om diplomat- och tjänstepass). Uppgifterna i chipet skyddas effektivt mot otillåten användning och missbruk i enlighet med EU-lagstiftningen.

För närvarande baserar sig styrkandet av personuppgifter vid besök i huvudsak på uppvisandet av fysiska handlingar. Utveckling har dock skett, och också vid fysiska besök är det tekniskt möjligt att utnyttja nya lösningar, som e-legitimation som beviljas av en myndighet, som kan användas för att styrka identiteten t.ex. på en mobil enhet utan någon traditionell handling. Den gällande lagstiftningen möjliggör inte e-legitimation beviljad av myndigheter.

3.3 Nationella behov av ändringar som främjar säkerheten i stark autentisering

3.3.1 Identifieringsverktygens tillförlitlighet

Tjänsterna inom stark autentisering är grundläggande tjänster i informationssamhället och det är av kritisk betydelse för samhället att de fungerar tillförlitligt. Med hjälp av dessa tjänster styrker medborgarna tryggt sin identitet när de använder e-tjänster. Dessutom kan e-tjänsterna identifiera sina kunder på ett tillförlitligt sätt med dem.

I och med att allt fler ärenden sköts på nätet har också riskerna för missbruk av verktyg för stark autentisering ökat. Identifieringsverktyg kan t.ex. hamna i fel händer vilket möjliggör identitetsstöld och användning av e-tjänster med en annan persons identitet. Dessutom är det värt att beakta att alltid när en medborgares identifieringsverktyg för stark autentisering äventyras finns risken att nya olagliga identifieringsverktyg beviljas. Med hjälp av identifieringsverktyg för stark autentisering är det möjligt att ta i bruk nya identifieringsverktyg och på detta sätt kan t.ex. kriminella fortsätta använda en annan persons identitet länge. Det förekommer också allt mer bedrägerier på nätet där kriminella försöker fiska fram personuppgifter av sina offer genom att ge sig ut för att vara t.ex. myndigheter eller banker. Enligt de anmälningar som gjorts till polisen har finländarna förlorat upp till över 70 procent mer i pengar 2024 än 2023 i internetbedrägerier.

Riksdagens kommunikationsutskott har ansett det vara viktigt att risken för missbruk i samband med att identifieringsverktyg för stark autentisering förnyas och beviljas ska försöka förhindras med alla till buds stående medel. Dessutom har kommunikationsutskottet förutsatt att de behov av lagstiftning som föranleds av missbruk följs och att eventuella korrigeringar åtgärder vidtas (KoUB 6/2021 rd).

3.3.2 Skyldigheten att kontrollera passets och identitetskortets giltighet

I 24 § i autentiseringslagen föreskrivs det om att leverantörer av identifieringstjänster trots sekretessbestämmelserna har rätt att via ett gränssnitt eller annars i elektronisk form få information ur polisens informationssystem om giltigheten hos pass eller identitetskort som används vid inledande identifiering. Det har funnits möjlighet att kontrollera giltighetstiden för ett pass eller identitetskort som används vid den inledande identifieringen i polisens informationssystem redan sedan 2017, men leverantörerna av identifieringsverktyg har utnyttjat den endast sällan.

Med stöd av den nuvarande lagstiftningen har leverantörerna av identifieringsverktyg ingen skyldighet att kontrollera passets eller identitetskortets giltighet i polisens elektroniska informationssystem, utan kontrollen bygger på frivillighet hos leverantören av identifieringsverktyget. Det här gör det möjligt för tredje personer att med ett stulet pass eller identitetskort komma i besittning av ett identifieringsverktyg i offrets namn. Det gör det möjligt att t.ex. i situationer där en leverantör av identifieringsverktyg identifierar den som ansöker om ett identifieringsverktyg på distans utifrån ett pass eller identitetskort, t.ex. genom att med en separat applikation fjärravläsa uppgifterna i handlingens maskinläsbara rad eller på chipet.

3.3.3 Sammankopplad inledande identifiering och förmedling av uppgifter om den

Bestämmelser om inledande identifiering, dvs. identifiering av en fysisk person i samband med ansökan om identifieringsverktyg finns i 17 § i autentiseringslagen. Vid inledande identifiering ska identifieringen av en fysisk person göras personligen eller elektroniskt på ett sådant sätt att de krav uppfylls som gäller för tillitsnivån väsentlig eller hög i förordningen om tillitsnivåer.

Kontrollen av en persons identitet kan grunda sig på en identitetshandling som utfärdats av en myndighet eller ett sådant identifieringsverktyg för stark autentisering som avses i autentiseringslagen. Kontrollen av identiteten kan dessutom grunda sig på ett förfarande som en offentlig eller privat aktör tidigare och i annat syfte än för beviljande av ett identifieringsverktyg för stark autentisering har använt sig av och som Transport- och kommunikationsverket godkänner med stöd av det förfarande som avses i 17 § i autentiseringslagen eller utifrån en bekräftelse av ett organ för bedömning av överensstämmelse.

När den inledande identifieringen grundar sig på ett befintligt identifieringsverktyg för stark autentisering handlar det om sammankoppling av inledande identifiering. Det handlar om sammankopplad inledande identifiering t.ex. när man med giltiga nätbankskoder tar i bruk ett mobilcertifikat. Sammankopplad inledande identifiering gör det lättare att skaffa nya identifieringsverktyg i synnerhet ur konsumentens synvinkel, när det går att skaffa sig ett nytt identifieringsverktyg helt på elektronisk väg utan att fysiskt besöka leverantören av identifieringsverktyget på verksamhetsstället. Sammankopplad inledande identifiering underlättar även tillhandahållandet av nya identifieringsverktyg. Samtidigt möjliggör den att kriminella aktörer med ett identitetsverktyg vars säkerhet har äventyrats kan skaffa nya identifieringsverktyg i den personens namn.

Nuvarande lagstiftning förpliktar inte leverantörer av identifieringsverktyg att förmedla uppgifter om sammankopplad inledande identifiering. Sålunda har en leverantör av identifieringsverktyg, som vid den inledande identifieringen av en fysisk person använder ett identifieringsverktyg för stark identifiering som beviljats av en annan leverantör, ingen uttrycklig skyldighet att när denne begär identifiering uppge att det handlar om att använda informationen för inledande identifiering av användaren. I Transport- och kommunikationsverkets rekommendation 213/2023 S, som har utarbetats i samarbete med leverantörer av identifieringstjänster, rekommenderas emellertid förmedling av information om den sammankopplade inledande identifieringen.

Av avsaknaden av juridiskt förpliktande informationsskyldighet följer att leverantören av ett identifieringsverktyg inte nödvändigtvis får veta om den starka autentisering som denne har tillhandahållit har använts för sammankoppling av inledande identifiering. Vid utredningen av vissa störningssituationer har man lagt märke till att bristfällig information om sammankopplingen av inledande identifiering även gör det svårare att utreda situationer med missbruk. Om ett identifieringsverktyg för stark identifiering t.ex. har hamnat i en annans besittning kan det i efterhand vara svårt att ta reda på om det med identifieringsverktyget i fråga har tagits i bruk nya elektroniska identifieringsverktyg om det inte finns tillgänglig information om användningen av identifieringsverktyget för inledande identifiering.

Information om den inledande identifieringen har betydelse även för faktureringen av den ersättning som ska erläggas för användningen av identifieringstjänsten och för ansvarsfördelningen i felsituationer. Bestämmelser om maximipriset för inledande identifiering har tidigare utfärdats genom en temporär lagändring som upphörde att gälla den 31 mars 2023. Därefter har det inte längre föreskrivits om maximipriset varför leverantörer av identifieringsverktyg kan ta ut en högre ersättning för inledande identifiering än för förmedling av andra identifieringstransaktioner. Information om användningen av identifieringsverktyg för inledande identifiering behövs alltså för att rätt ersättning ska kunna tas ut.

3.3.4 Återaktivering av identifieringsverktyg

Kraven på identifieringsverktygens säkerhet har i autentiseringslagen till många delar harmoniserats med regleringen i eIDAS-förordningen. Förordningen om tillitsnivåer vid

elektronisk identifiering innehåller kraven på identifieringssystem på olika tillitsnivåer. Autentiseringslagen innehåller hänvisningar till förordningen om tillitsnivåer vid elektronisk identifiering varvid vissa krav i den ska tillämpas även på sådana leverantörer av tjänster som inte ingår i tillämpningsområdet för eIDAS-förordningen.

Autentiseringslagen innehåller genom hänvisningsbestämmelserna en skyldighet att uppfylla de övriga krav i avsnitt 2.2 Hantering av medel för elektronisk identifiering i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering än de krav som anges i avsnitt 2.2.3. T.ex. enligt 22 § i autentiseringslagen ska när identifieringsverktyg förnyas de krav uppfyllas som gäller för tillitsnivån väsentlig enligt avsnitt 2.2.4 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering.

Avsnitt 2.2.3 gäller upphävande, återkallelse och återaktivering av giltighetstiden. Av dessa har i synnerhet den uttryckliga avsaknaden av krav gällande återaktivering orsakat oklarhet i den nationella lagstiftningen. Som återaktivering kan man i praktiken se t.ex. situationer där ny PIN-kod anges i stället för en glömd och låsta koder öppnas. Leverantörer av identifieringstjänster har olika metoder för att låsa upp låsta koder. Eftersom det inte finns nationella bestämmelser om återaktivering tillämpas inga särskilda säkerhetskrav på detta.

4 Förslagen och deras konsekvenser

4.1 De viktigaste förslagen

4.1.1 Genomförande av den reviderade eIDAS-förordningen

Propositionens huvudsakliga syfte är att genomföra den reviderade eIDAS-förordningen. I denna proposition föreslås det att det stiftas en ny lag om vissa tjänster som möjliggör gränsöverskridande e-tjänster (nedan *eIDAS-lagen*) samt att autentiseringslagen ändras. Det föreslås att all nationell kompletterande reglering som gäller eIDAS-förordningen framöver tas in i eIDAS-lagen. Lagen innehåller sålunda ny reglering som behövs för genomförande av den reviderade eIDAS-förordningen och dessutom flyttas den redan befintliga reglering med vilken den ursprungliga eIDAS-förordningen genomfördes från autentiseringslagen till den här lagen. Ur lagtillämparens synvinkel blir det tydligast att de nationella kraven på stark autentisering och den reglering som kompletterar eIDAS-förordningen framöver finns i egna lagar. Framöver kan tjänsteleverantörer och andra tillämpare av lagen enkelt välja vilken lag som tillämpas utgående från om avsikten är att som leverantör av identifieringstjänster agera endast på nationell nivå eller att leverera tjänster mer omfattande inom EU:s medlemsstaters territorier.

Det centrala innehållet i den reviderade eIDAS-förordningen är gemensam lagstiftning om en europeisk digital identitetsplånbok. Plånboken och dess egenskaper beskrivs närmare i avsnitt 2.2.1. I propositionen föreslås det att Myndigheten för digitalisering och befolkningsdata ska ha till uppgift att tillhandahålla en europeisk digital identitetsplånbok i Finland. Detta begränsar dock inte möjligheterna för aktörer inom den privata sektorn att tillhandahålla en plånbok parallellt med den plånbok Myndigheten för digitalisering och befolkningsdata tillhandahåller. Dessutom föreslås det att Myndigheten för digitalisering och befolkningsdata utifrån befolkningsdatasystemet ska bevilja fysiska personer identifieringsuppgifter som gör det möjligt att styrka sin identitet i plånboken. I fråga om juridiska personer föreslås det att Patent- och registerstyrelsen ska ha rätt att bevilja identifieringsuppgifter för plånböcker på basis av handelsregistret. Dessutom föreslås det i propositionen att personer som vistas utomlands ska kunna ta i bruk identifieringsuppgifter för fysiska personer genom att sköta ärendet vid en finsk beskickning.

Det föreslås att det ska föreskrivas att Myndigheten för digitalisering och befolkningsdata ska vara personuppgiftsansvarig för den plånbok den tillhandahåller och för behandlingen av personuppgifter i samband med tillhandahållandet av den. Den rättsliga grunden för behandlingen av personuppgifter i samband med tillhandahållandet av plånboken grundar sig på artikel 6.1 c i dataskyddsförordningen, om behandlingen av personuppgifter är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Myndigheten för digitalisering och befolkningsdatas status som personuppgiftsansvarig påverkas emellertid av det som i den reviderade eIDAS-förordningen föreskrivs om att uppgifterna i plånboken står under plånboksanvändarens kontroll, vilket plånboken baserar sig på. I praktiken avses med detta att personen själv beslutar om användningen av sina personuppgifter. Myndigheten för digitalisering och befolkningsdatas status som personuppgiftsansvarig och dess förhållande till användarens rätt att själv ha kontroll över informationen beskrivs närmare i specialmotiveringen i det första lagförslaget.

I propositionen föreslås att det föreskrivs att den som fyllt tretton år ska kunna ta i bruk en plånbok självständigt. Den som är yngre än så kan ta i bruk en plånbok med vårdnadshavarens samtycke. Den reviderade eIDAS-förordningen förutsätter inga bestämmelser om en lägsta ålder utan bestämmelsen behövs av nationella skäl. Om det inte föreskrivs om en lägsta ålder skulle det tillämpas olika lagstiftning och således olika åldersgränser på självständigt ibrukttagande av plånböcker som tillhandahålls av den offentliga och den privata sektorn. Den föreslagna minimiåldern på 13 år är förenlig med åldersgränsen i 5 § i dataskyddslagen (1050/2018) som tillämpas när informationssamhällets tjänster erbjuds till barn. Avsikten är inte att genom den föreslagna lagstiftningen ändra på i vilka situationer en 13-åring har rätt att sköta ärenden självständigt, utan att genom lagstiftningen möjliggöra att ärenden sköts med hjälp av en plånbok i de situationer där en 13-åring utifrån andra bestämmelser har rätt till det.

I propositionen föreslås i enlighet med de åsikter intressentgrupperna lade fram att det nationella handlingsutrymmet används i anslutning till öppenheten i den europeiska digitala identitetsplånbokens källkod och kostnadsfriheten för elektroniska underskrifter. I propositionen föreslås att det föreskrivs att en tillhandahållare av en plånbok inte behöver lämna ut en källkod för en plånboks komponenter som inte har installerats på den tekniska utrustningen av en användare, om det föreligger vederbörligen motiverade skäl för detta. En begränsning av kravet på öppen källkod hos plånboken behövs i synnerhet för att främja utvecklingsarbetet och investeringarna i anslutning till plånboken. Dessutom föreslås det i propositionen att det föreskrivs att tillhandahållaren av en plånbok får vidta åtgärder för att begränsa avgiftsfriheten för kvalificerade elektroniska underskrifter som skapats med hjälp av en plånbok för andra än yrkesmässiga ändamål. En begränsning av avgiftsfriheten för elektronisk underskrift behövs särskilt av den anledningen att tillhandahållandet av elektroniska underskrifter numera är verksamhet på marknadsvillkor och ofta avgiftsbelagd.

I propositionen föreslås att identitetsmatchningen i Finland centraliserat genomförs av Myndigheten för digitalisering och befolkningsdata så att den i det första skedet finns tillgänglig för myndigheter och andra som sköter offentliga uppdrag. Dessutom föreslås det att också aktörer inom den privata sektorn i ett senare skede ska ha rätt att använda identitetsmatchning. Identitetsmatchning handlar om att personuppgifter eller identifieringsverktyg för personer som kommer från andra medlemsstater kopplas till befintliga uppgifter om personen i fråga. Det handlar alltså inte om registrering av nya personer utan identitetsmatchning förutsätter befintlig registeridentitet i Finland.

Enligt förordningen är Transport- och kommunikationsverket tillsynsmyndighet för den ram för den europeiska digitala identitet som avses i eIDAS-förordningen. I propositionen föreslås att det i den nya eIDAS-lagen föreskrivs om behövliga befogenheter för Transport- och

kommunikationsverket, som rätt att få information, rätt att utföra inspektioner, rätt att förplikta en aktör att korrigera sin verksamhet i enlighet med förordningen och rätt att förena sitt beslut med vite. Transport- och kommunikationsverket är redan nu tillsynsmyndighet för betrodda tjänster som ingår i tillämpningsområdet för eIDAS-förordningen och dem som tillhandahåller dem samt för de nationella identifieringstjänsterna. I plånboken sammanförs tillhandahållande av betrodda tjänster och stark autentisering om vilka Transport- och kommunikationsverket genom sitt arbete hittills har erfarenhet av och kompetens om. Av den anledningen är det motiverat att den också ska vara tillsynsmyndighet för tillhandahållandet av plånböcker.

Dessutom föreslås det att Transport- och kommunikationsverket ska ha till uppgift att föra ett register över plånböckers förlitande parter och vara personuppgiftsansvarig för det. Enligt den reviderade eIDAS-förordningen ska tillsynsmyndigheten i vissa situationer tillfälligt eller permanent upphäva registreringen av förlitande parter och därför är det ändamålsenligt att tillsynsmyndigheten även är personuppgiftsansvarig för registret i fråga. Enligt propositionen är Transport- och kommunikationsverket också den gemensamma kontaktpunkt som avses i den reviderade eIDAS-förordningen. Transport- och kommunikationsverket föreslås också vara behörig myndighet att påföra tillhandahållare av betrodda tjänster administrativa påföljdsavgifter. I den föreslagna eIDAS-lagen föreskrivs det på det sätt som den reviderade eIDAS-förordningen förutsätter om administrativa sanktionsavgifter som kan påföras tillhandahållare av betrodda tjänster för verksamhet i strid med de krav som föreskrivs i eIDAS-förordningen. De högsta beloppen för de administrativa påföljdsavgifter som föreslås i propositionen håller en nivå motsvarande det lägsta maximibelopp som eIDAS-förordningen tillåter.

För att täcka de kostnader som tillsynsuppgifterna medför för Transport- och kommunikationsverket föreslås att det föreskrivs om tillsynsavgifter som betalas till Transport- och kommunikationsverket. Vissa av avgifterna är nya och vissa redan existerande avgifter som flyttas från autentiseringslagen till den nya eIDAS-lagen. Enligt propositionen ska tillhandahållare av europeiska digitala identitetsplånböcker, tillhandahållare av betrodda tjänster, organ för bedömning av överensstämmelse enligt eIDAS-lagen samt certifierare betala en årlig tillsynsavgift till Transport- och kommunikationsverket. Dessutom kan det tas ut en avgift för behandling av anmälningar och ansökningar som lämnas till Transport- och kommunikationsverket samt för registreringar i enlighet med lagen om grunderna för avgifter till staten, dvs. avgiftens storlek motsvarar den totalkostnad staten har för att producera prestationen. Dessutom föreslås det i propositionen ändringar i de avgifter till Transport- och kommunikationsverket som det föreskrivs om i autentiseringslagen så att de tillsynsavgifter leverantörer av identifieringstjänster och de organ för bedömning av överensstämmelse som avses i autentiseringslagen erlägger fortsättningsvis bestäms enligt autentiseringslagen och det således föreskrivs om dem i lagen i fråga. Tillsynsavgifterna höjs med 3 000 euro. Däremot slopas i lagen utnämnings- och registreringsavgifterna och framöver ska de avgifter som tas ut för anmälningar och ansökningar betalas enligt lagen om grunderna för avgifter till staten. Avgifter tas även ut för Patent- och registerstyrelsens prestationer på det sätt som det särskilt föreskrivs om dem.

I propositionen föreslås att det föreskrivs om organ för bedömning av överensstämmelse, hur de utses och anmäls till kommissionen samt om den tillsyn de utövar över överensstämmelsen. Dessutom föreskrivs det om bedömning av informationssäkerheten för den nationella nod som Myndigheten för digitalisering och befolkningsdata upprätthåller av ett i lagen om bedömningsorgan för informationssäkerhet (1405/2011) avsett godkänt bedömningsorgan för informationssäkerhet, av ett organ för bedömning av överensstämmelse eller av Transport- och kommunikationsverket.

4.1.2 E-legitimation

I propositionen ingår ett förslag till lag om e-legitimation. Genom lagen skapas en rättslig grund för e-legitimation som gör det möjligt att tillförlitligt styrka personuppgifter. E-legitimationen är tillgänglig endast via den europeiska digitala identitetsplånboken och har som grund ett giltigt finskt pass eller finskt identitetskort. E-legitimationen tillhandahålls användarna som ett kvalificerat elektroniskt attributsintyg och den är det första attributsintyget i Finland som kan fås för den europeiska digitala identitetsplånboken. E-legitimationen kan primärt användas för när ärenden sköts på plats.

Rätten till e-legitimation uppkommer i fortsättning i samband med att pass eller identitetskort beviljas. Den första förutsättningen för att ta i bruk e-legitimation är att användaren har tagit i bruk en plånbok genom vilken användaren kan få legitimationen. En andra förutsättning är ett giltigt pass eller identitetskort. Genom propositionen ändras inte förutsättningarna för att få ett pass eller ett identitetskort. Beviljandet av e-legitimation är således bundet till ett pass eller identitetskort som har ansökts och beviljats som sig bör och således grundar sig en e-legitimation på en tillförlitligt styrkt identitet. En e-legitimation tillåter således inget sätt att kringgå de krav som ställs på kontrollen av identiteten i ansökningsfasen. Förutsättningen förhindrar bl.a. effektivt möjligheten att skapa en falsk identitet med hjälp av en e-legitimation. Således är säkerhetsnivån för både fysiska handlingar och den föreslagna digitala uttrycksformen på sin nuvarande höga nivå.

Enligt propositionen uppfyller ett i passlagen avsett pass, provisoriskt pass, diplomat- eller tjänstepass samt i lagen om identitetskort avsett identitetskort, provisoriskt identitetskort som beviljas finska medborgare, identitetskort för utlänningar eller ett identitetskort utan rätt att resa som avses i 17 § 3 mom. under den tid de är giltiga förutsättningen för att få en e-legitimation. Förutsättningen för att få ett identitetskort för utlänningar är att den sökande har ett giltigt uppehållstillstånd eller uppehållskort eller att den sökandes uppehållsrätt har registrerats. Dessutom ska personen ha en hemkommun i Finland enligt lagen om hemkommun (201/1994) och uppgifterna om personen ska ha lagrats i befolkningsdatasystemet.

Det faktum att den behöriga myndighet som beviljar ett pass eller ett identitetskort samtidigt beviljar rätten till e-legitimation kan ses som något som främjar säkerheten och smidigheten. Personuppgifterna samt uppgifterna i passets och identitetskortets säkerhetsegenskaper behandlas i fråga om rätten till e-legitimation således endast av en behörig myndighet i pass- och identitetskortsfrågor som också ansvarar för dem. Förfarandet förhindrar att behörigheten delas upp mellan olika myndigheter och säkerställer en rätlinjig behandling utan extra administrativt arbete.

Ett kvalificerat elektroniskt attributsintyg beviljas utan separat ansökan en finsk medborgare eller en utlänning som vistas i Finland som tillståndsmyndigheten har beviljat rätt till e-legitimation. Myndigheten för digitalisering och befolkningsdata ansvarar för genomförandet av ett kvalificerat elektroniskt attributintyg. Polisen lämnar till Myndigheten för digitalisering och befolkningsdata ut de uppgifter som behövs för att bevilja och föra över det elektroniska attributsintyget till plånboken. Lagen innehåller också bestämmelser om legitimationens giltighetstid, indragning och giltighetens upphörande samt registerföring.

Enligt propositionen kan e-legitimation inte användas som resedokument eftersom EU:s direktiv om fri rörlighet 2004/38/EG förutsätter pass eller identitetskort för fri rörlighet. I EU:s förordning om identitetskort (EU) 2025/1208 definieras identitetskort, och e-legitimationen uppfyller inte definitionen i förordningen. Dessutom är avtal om resedokument i hög grad multilateral internationell verksamhet där FN:s fackorgan för internationell civil luftfart ICAO

har en central roll vid angivandet av internationella standarder. Av de anledningar som ovan lades fram var det inte möjligt att hitta en fungerande nationell lagstiftningslösning för att kunna utnyttja e-legitimation som resedokument. Samtidigt har man på EU-nivå emellertid börjat bereda regelverk om en digital reseapplikation som eventuellt genomförs så att den är interoperabel med plånböcker. I enlighet med propositionen är e-legitimationen en lagstiftningslösning på nationell nivå som främjar en mer omfattande användning av plånböcker.

E-legitimationen är central för att möjliggöra omfattande användning av den europeiska digitala identitetsplånboken i Finland. Dess betydelse framhävs särskilt för att det i många vardagliga situationer när ärenden sköts ingår att visa bestyrkta personuppgifter. Möjligheten att ersätta en fysisk identitetshandling med en e-legitimation som en plånboksapplikation som används på mobiltelefonen är för medborgarna i snitt en attraktiv och praktisk lösning. Ibrukttagandet av plånboken bedöms avancera etappvis i Finland beroende på medborgarnas erfarenheter av användningen och vilken nytta den ger. Därför är det särskilt viktigt att plånbokens innehåll genast i den första fasen svarar mot medborgarnas vardagliga behov på ett mångsidigt sätt. E-legitimationen utgör ett centralt och konkret användningsobjekt som stöder ibrukttagandet av plånböcker och ökar deras värde för användarna.

4.1.3 Nationella behov av ändringar som främjar säkerheten vid stark autentisering

I propositionen föreslås det att det till autentiseringslagen fogas bestämmelser om att leverantörer av identifieringsverktyg är skyldiga att säkerställa att det pass eller identitetskort som används vid den inledande identifieringen är giltigt och att de är skyldiga att förmedla information om att ett identifieringsverktyg som levereras av en annan leverantör av identifieringsverktyg används vid den inledande identifieringen. Transport- och kommunikationsverket ges behörighet att meddela närmare föreskrifter om tekniska detaljer om de uppgifter som ska registreras om den inledande identifieringen. Dessutom uppdateras autentiseringslagen genom vissa andra enstaka ändringar

4.2 De huvudsakliga konsekvenserna

4.2.1 Inledning

Den nya eIDAS-lag som föreslås i propositionen kompletterar EU:s eIDAS-förordning. Dessutom föreslås det i propositionen en ny lag om e-legitimation som delvis lutar sig mot regleringen i eIDAS-förordningen om kvalificerade tillhandahållare av betrodda tjänster, kvalificerade betrodda tjänster och kvalificerade elektroniska attributsintyg. Av denna anledning beskriver konsekvensbedömningen i första hand konsekvenserna av den nationella lag som kompletterar eIDAS-förordningen och av lagen om e-legitimation. Konsekvenserna av eIDAS-förordningen som redan har trätt i kraft beskrivs närmast till den del som de är väsentliga med tanke på den nationella lag som föreslås eller när en beskrivning av konsekvenserna av EU-förordningen har bedömts göra det lättare att skapa sig en bild av de samverkande konsekvenserna av den direkt förpliktande förordningens bestämmelser och den kompletterande lagstiftningen.

Enligt artikel 5a.15 i den reviderade eIDAS-förordningen ska användningen av europeiska digitala identitetsplånböcker vara frivillig. Myndigheten för digitalisering och befolkningsdata genomförde emellertid en medborgarundersökning om europeiska digitala identitetsplånböcker hösten 2025. Undersökningen syftade bl.a. till att utreda medborgarnas intresse för att ta i bruk en applikation för den nya europeiska digitala identitetsplånboken och det relaterade elektroniska identifieringssättet. Sammanfattningsvis kan det utifrån undersökningens resultaten

konstateras att många är intresserade av att ta i bruk den nya europeiska digitala identitetsplånboken. Respondenterna var däremot inte i något större behov av gränsöverskridande e-tjänster. Intresset att använda plånboken avser särskilt elektronisk identifiering i Finland. Dessutom var man intresserad av olika elektroniska intyg. Respondenterna ansåg att viktiga egenskaper i plånboken är att den är säker och enkel att använda. Resultaten från undersökningen presenteras mer detaljerat i avsnitt 4.2.3.1 om allmänna konsekvenser för människogrupper.

Artikel 5f i den reviderade eIDAS-förordningen förpliktar att godta europeiska digitala identitetsplånböcker för identifiering av en person i vissa situationer när ärenden sköts elektroniskt. Den reviderade eIDAS-förordningen förpliktar emellertid inte e-tjänster att möjliggöra att plånböcker används när ärenden uträttas vid fysiska besök. Medlemsstaterna har inte heller enligt den reviderade eIDAS-förordningen skyldighet att producera elektroniska attributsintyg för plånböcker. Däremot kan medlemsstaterna åläggas sådana skyldigheter i den sektorsvisa EU-regleringen. E-tjänsternas skyldighet att godta plånböcker begränsar sig således i den första fasen i stor utsträckning till elektronisk identifiering. Skyldigheten att godta att ärenden sköts och uppgifter styrks med en plånbok kan emellertid utökas i faser om EU:s sektorsvisa reglering förutsätter det.

De ovan beskrivna omständigheterna har betydelse för bedömningen av propositionens konsekvenser. Propositionen och dess samverkande konsekvenser med den reviderade eIDAS-förordningen är dels till en del beroende av i vilken utsträckning medborgarna tar i bruk europeiska digitala identitetsplånböcker, dels i vilken utsträckning e-tjänsterna möjliggör att ärenden sköts med plånböcker och elektroniska attributsintyg hos dem. Av den anledningen är strävan i konsekvensbedömningen att beskriva i synnerhet sådana allmänna konsekvenser som förslagen i propositionen har oavsett antalet användare av de nya tjänsterna. Strävan har även varit att lyfta fram olika alternativa konsekvenser med olika antal användare om bedömningen har kunnat göras på en tillräckligt konkret och sannolik nivå.

4.2.2 Ekonomiska konsekvenser

4.2.2.1 Konsekvenserna för förtroendenätet för elektronisk identifiering

Det har föreskrivits uttömmande om plånboken och kraven på tillhandahållandet av den i den reviderade eIDAS-förordningen och det är inte möjligt att ställa ytterligare nationella krav. Därmed omfattas de europeiska digitala identitetsplånböckerna och tillhandahållarna av dem inte av regleringen om den nationella starka autentiseringen och står därmed också utanför marknaden för nationell stark autentisering, dvs. förtroendenätet. I praktiken innebär detta att de europeiska digitala identitetsplånböckerna bildar ett parallellt system till förtroendenätet för nationell stark autentisering där kraven härrör från den reviderade eIDAS-förordningen och de genomförandeförordningar som kommissionen antagit med stöd av den. Eftersom stark autentisering ändå är möjlig också med en plånbok och den numera tillhandahålls i Finland på en konkurrerad marknad gällde bedömningen när propositionen bereddes konsekvenserna av den reviderade eIDAS-förordningen och det nationella genomförandet av den för de nuvarande leverantörerna av identifieringstjänster.

Förtroendenätets kunder är olika e-tjänster som vill eller är förpliktade att identifiera sina kunder med stark autentisering. I förtroendenätet verkar två slags aktörer: leverantörer av identifieringsverktyg som tillhandahåller personer verktyg för stark autentisering och leverantörer av tjänster för identifieringsförmedling som förmedlar identifieringstransaktioner som utförs med verktyg för stark autentisering till e-tjänsterna. Genomförandet av plånboken har olika konsekvenser för olika aktörer i förtroendenätet. Som det konstateras ovan i

inledningen till konsekvensbedömningen beror konsekvenserna på hur allmänt plånböcker kommer att användas.

Det bedöms att genomförandet av en europeisk digital identitetsplånbok kommer att ha både neutrala och negativa konsekvenser för leverantörer av identifieringsverktyg. Om plånboken börjar användas omfattande kan användningen av de nuvarande identifieringsverktygen minska. Det här kan påverka viljan hos både nuvarande och eventuella nya leverantörer av identifieringsverktyg att investera i utveckling av identifieringsverktyg. Om plånboken börjar användas endast i ringa utsträckning blir konsekvenserna för nuvarande och nya leverantörer av identifieringsverktyg också små.

Det bedöms att den reviderade eIDAS-förordningen och dess nationella genomförande närmast har positiva konsekvenser för leverantörer av tjänster för identifieringsförmedling, men också vissa små negativa konsekvenser. I det andra lagförslaget i propositionen föreslås det att leverantörer av tjänster för identifieringsförmedling kan förmedla identifieringstransaktioner som baserar sig på en europeisk digital identitetsplånbok trots att plånböckerna inte ingår i förtroendenätet. Detta kan öka affärsmöjligheterna för leverantörer av tjänster för identifieringsförmedling. Samtidigt kan genomförandet av plånboken i någon mån minska förmedlingen av identifiering som baserar sig på nuvarande identifieringsverktyg för stark autentisering om plånboken tas i omfattande bruk och användningen av andra verktyg för stark autentisering minskar. Antalet förmedlade identifieringstransaktioner förblir sannolikt detsamma, men identifieringstransaktionerna baserar sig på plånböcker i stället för som nu på identifieringsverktyg. Förmedling av identifiering som baserar sig på en plånbok förutsätter sannolikt att leverantörerna av tjänster för identifieringsförmedling inför nya integreringsmetoder eftersom plånbokens tekniska krav avviker från förtroendenätets nuvarande tekniska krav. Kostnadskonsekvenserna av detta för leverantörer av tjänster för identifieringsförmedling bedöms emellertid bli ringa och de är i varje fall frivilliga eftersom leverantörer av tjänster för identifieringsförmedling inte förpliktas att förmedla identifieringstransaktioner som baserar sig på en plånbok.

Det bedöms att genomförandet av en europeisk digital identitetsplånbok och relaterade tjänster på längre sikt klart ökar affärsmöjligheterna för de nuvarande leverantörerna av tjänster för identifieringsförmedling. I framtiden kan leverantörer av tjänster för identifieringsförmedling om de så vill utvidga sin verksamhet till att omfatta förmedling av olika elektroniska attributsintyg som tillhandahålls för plånböcker. Leverantörer av tjänster för identifieringsförmedling kan t.ex. utvidga sin verksamhet och bli tillhandahållare av betrodda tjänster och förmedla elektroniska attributsintyg om uppgifternas autentiska källor, dvs. om olika register, till plånboken. När propositionen bereddes bedömdes det att detta klart var mer omfattande än affärsverksamheten i anslutning till den nuvarande starka autentiseringen.

4.2.2.2 Konkurrensrättsliga konsekvenser avseende Myndigheten för digitalisering och befolkningsdatas uppgift som tillhandahållare av en europeisk digital identitetsplånbok

Eftersom elektroniska identifieringsverktyg och betrodda tjänster i Finland i princip har tillhandahållits även av tjänsteleverantörer inom den privata sektorn, är den föreslagna statusen för Myndigheten för digitalisering och befolkningsdata som tillhandahållare av en europeisk digital identitetsplånbok förknippad med frågor som rör EU-lagstiftningen om statligt stöd (artikel 107 i fördraget om Europeiska unionens funktionssätt *FEUF*,) och den nationella lagstiftningen om konkurrensneutralitet (4 a kap. i konkurrenslagen (948/2011)). Enligt artikel 107.1 i FEUF är stöd som ges av en medlemsstat eller med hjälp av statliga medel, av vilket slag det än är, som snedvrider eller hotar att snedvrida konkurrensen genom att gynna vissa

företag eller viss produktion, oförenligt med den inre marknaden i den utsträckning det påverkar handeln mellan medlemsstaterna.

Regleringen om konkurrens och statliga stöd gäller enheter som bedriver ekonomisk verksamhet, oavsett deras rättsliga form eller hur de finansieras. Det första steget med tanke på tillämpningen av denna reglering är att bedöma huruvida tillhandahållandet av en europeisk digital identitetsplånbok handlar om ekonomisk verksamhet. När detta bedöms kan man granska t.ex. om det finns en marknad för tjänsterna eller om andra aktörer är villiga och har förmåga att producera tjänsten i fråga. För att förtydliga skillnaden mellan ekonomisk och annan än ekonomisk verksamhet har unionens domstol konsekvent ansett att ekonomisk verksamhet är all verksamhet där varor eller tjänster tillhandahålls på marknaden. Huruvida det existerar en marknad för en viss tjänst kan bero på hur den har ordnats i medlemsstaten i fråga och därför förekommer det variationer mellan medlemsstaterna emellan i huruvida det finns en marknad eller inte. Dessutom kan klassificeringen av en viss verksamhet ändras över tid på grund av politiska val eller den ekonomiska utvecklingen. Något som vid tidpunkten för granskningen inte är ekonomisk verksamhet kan bli det i framtiden och tvärtom (Kommissionens meddelande om definitionen av statligt stöd som avses i artikel 107.1 i FEUF (2016/C262, 12–13 punkten)).

Utöver lagstiftningen om statligt stöd ska det noteras att om en medlemsstat har beslutat att ta i bruk marknadsmekanismer och verksamheten till sin karaktär betraktas som ekonomisk, ska också regleringen i konkurrenslagens 4 a kap. om konkurrensneutralitet tillämpas. Bestämmelserna i 4 a kap. i konkurrenslagen syftar till att ge den nationella myndigheten behörighet i frågor som rör konkurrensneutralitet. Enligt 30 a § i kapitlet i fråga ska Konkurrens- och konsumentverket i första hand förhandlingsvägen försöka undanröja ett förfarande eller en verksamhetsstruktur som tillämpas i den ekonomiska verksamhet som bedrivs av staten eller en enhet som den har bestämmande inflytande över och som när varor eller tjänster erbjuds 1) snedvrider eller kan bidra till att snedvrida förutsättningarna för en sund och fungerande konkurrens på marknaden, 2) hindrar eller kan bidra till att hindra att en sund och fungerande ekonomisk konkurrens uppstår eller utvecklas, eller 3) står i strid med kravet på marknadsmässig prissättning i 128 § i kommunallagen (410/2015) eller 133 § i lagen om välfärdsområden (611/2021). Vidare enligt 30 c § i samma kapitel gäller att om förhandlingen inte leder till resultat, ska Konkurrens- och konsumentverket bl.a. förbjuda staten att använda förfarandet eller verksamhetsstrukturen eller som villkor för förfarandet eller verksamhetsstrukturen meddela ålägganden som säkerställer jämlika verksamhetsförutsättningar på marknaden.

Den europeiska digitala identitetsplånboken består av sådana funktioner och tjänster där vissa redan tillhandahålls av tjänsteleverantörer inom den privata sektorn och där det kan antas att det finns en marknad. Stark autentisering tillhandahålls i förtroendenätet i Finland av flera leverantörer av identifieringsverktyg. Likaså tillhandahålls den betrodda tjänsten för kvalificerad elektronisk underskrift på den interna marknaden av tjänstetillhandahållare inom den privata sektorn. I Finland tillhandahålls elektroniska underskrifter dock närmast som icke-kvalificerade betrodda tjänster. De elektroniska attributsintyg som avses i den reviderade eIDAS-förordningen tillhandahålls ännu inte eftersom det handlar om en ny betrodd tjänst. Numera tillhandahålls det vissa tjänster som på någon nivå kan jämföras med elektroniska attributscertifikat, som inträdesbiljetter i elektroniskt format. I dem är det dock sällan fråga om personuppgifter om användaren eller användarens egenskaper på samma sätt som det förutsätts av attributsintyg.

Enligt artikel 5 a.1 i den reviderade eIDAS-förordningen ska varje medlemsstat tillhandahålla åtminstone en europeisk digital identitetsplånbok inom 24 månader från att kommissionens genomförandeförordningar träder i kraft. Det har emellertid inte föreskrivits att den offentliga

sektorn har ensamrätt att tillhandahålla plånböcker utan de kan enligt artikel 5a.2 c i förordningen tillhandahållas oberoende av en medlemsstat men med den medlemsstatens erkännande. Dessutom tillhandahålls funktioner i anslutning till plånböcker på marknaden på det sätt som beskrivs ovan av tjänsteleverantörer inom den privata sektorn. Därför bedöms det att när plånböckerna granskas enligt funktion handlar det i fråga om europeiska digitala identitetsplånböcker sannolikt om ekonomisk verksamhet. Plånböckerna är emellertid ett helt nytt koncept som till sina funktioner är bredare än de tjänster som tillhandahålls för närvarande och för plånböckerna gäller även särskilda krav beträffande tillförlitligheten och informationssäkerheten. Någon motsvarande helhet av tjänster har inte tidigare tillhandahållits varför det inte heller finns någon existerande marknad för plånböcker som helhet.

Eftersom medlemsstaterna i den reviderade eIDAS-förordningen har ålagts skyldigheten att tillhandahålla åtminstone en europeisk digital identitetsplånbok inom en viss tidsfrist lät finansministeriet utreda huruvida de nuvarande tillhandahållarna inom den privata sektorn har som mål att tillhandahålla en plånbok som uppfyller kraven i den reviderade eIDAS-förordningen inom den föreskrivna tidsfristen. Marknadsundersökningen behandlas även i propositionens avsnitt 5.1.1. Utifrån det som framkom kommer marknadsaktörerna inte att tillhandahålla någon plånbok i enlighet med den reviderade eIDAS-förordningen under de närmaste åren. På lång sikt är aktörerna emellertid eventuellt intresserade av att tillhandahålla en plånbok som uppfyller kraven i eIDAS-förordningen. Utifrån utredningen bedöms verksamheten på marknaden vara ganska bristfällig under de närmaste åren. Med det avses att det inte finns sedvanlig marknadsverksamhet och att plånböcker i enlighet med eIDAS-förordningen inte tillhandahålls inom den angivna tidsfristen (*marknadsbrist*). Därför föreslås det i propositionen att Myndigheten för digitalisering och befolkningsdata ska ha till uppgift att tillhandahålla en europeisk digital identitetsplånbok i Finland. Lagstiftningen om statligt stöd och konkurrens tillämpas inte på Myndigheten för digitalisering och befolkningsdatas verksamhet så länge som marknadsbristen inom tillhandahållandet av plånböcker fortgår, dvs. så länge som det inte uppkommer en konkurrerad marknad för europeiska digitala identitetsplånböcker i Finland. Det är möjligt att följa marknadens utveckling och hur marknadsbristen fortgår utifrån vilka plånböcker Transport- och kommunikationsverket har anmält till Europeiska kommissionen enligt 33 § 2 punkten i eIDAS-lagen.

4.2.2.3 Regleringsbördan och övriga kostnader för e-tjänster

I den reviderade eIDAS-förordningen föreskrivs det om att både offentliga och privata e-tjänster är skyldiga att godta att europeiska digitala identitetsplånböcker används när användarna autentiserar sig i deras tjänster. Dessutom förutsätter den reviderade eIDAS-förordningen att e-tjänster och andra parter som förlitar sig på plånböcker registrerar sig i den medlemsstat där de finns etablerade. I avsnitt 2.2.1 redogörs närmare för det huvudsakliga innehållet i skyldigheterna.

Genom den föreslagna lagstiftningen i anslutning till genomförandet av den reviderade eIDAS-förordningen har man försökt minska eventuella extra kostnader som kan orsakas av skyldigheten i den reviderade eIDAS-förordningen som avser identifieringen av användare med den europeiska digitala identitetsplånboken. För närvarande köper privata e-tjänster sina tjänster för stark autentisering centraliserat från förtroendenätet (se närmare avsnitt 3.1.1). För förtroendenätet och kring det har det alltså byggts behövliga tekniska gränssnitt och övriga förutsättningar för förmedling av identifieringstransaktioner till e-tjänsterna. Om man ser till de privata e-tjänsterna vore de sannolikt tydligast och enklast att fullfölja skyldigheten enligt den reviderade eIDAS-förordningen så att identifieringen av användare som baserar sig på en plånbok kan ske med samma tekniska gränssnitt som identifieringen av användare med de nuvarande identifieringsverktygen för stark autentisering. Förslagen i propositionen gör det

möjligt att leverantörer av tjänster för identitetsförmedling kan förmedla identifiering som baserar sig på en plånbok trots att den inte ingår i förtroendenätet.

För den offentliga sektorns del gör förslagen det möjligt att Suomi.fi-identifieringen framöver kan identifiera en fysisk person som använder den offentliga förvaltningens e-tjänster även med hjälp av en plånbok. Det föreskrivs om en tjänst för identifiering av fysiska personer i 3 § 4 punkten i lagen om förvaltningens gemensamma stödtjänster för e-tjänster (571/2016) (nedan *lagen om stödtjänster*). Enligt den handlar det om en tjänst som identifierar en fysisk person som använder den offentliga förvaltningens e-tjänster med hjälp av en tjänst som tillhandahålls av en sådan leverantör av identifieringstjänster som avses i autentiseringslagen, administrerar identifieringstransaktionen och till användarorganisationen lämnar ut identifieringsuppgifter om en person ur befolkningsdatasystemet. E-tjänsterna inom den offentliga förvaltningen är i princip skyldiga att använda en tjänst för identifiering av fysiska personer.

E-tjänsternas skyldighet att godta en plånbok begränsar sig i den första fasen till elektronisk identifiering och den reviderade eIDAS-förordningen förpliktar inte e-tjänsterna att möjliggöra användningen av en plånbok vid fysiska besök. Däremot kan den sektorsvisa EU-regleringen i framtiden medföra sådana skyldigheter och således kan e-tjänsternas skyldighet att godta att ärenden sköts med en plånbok och att uppgifter verifieras med en plånbok öka stegvis. E-tjänsterna kan emellertid på eget initiativ när som helst godta att ärenden sköts på plats med en plånbok.

Möjligheten att sköta ärenden på plats med en plånbok kan förutsätta utveckling av de befintliga systemen i e-tjänsterna eller införande av nya funktioner samt utbildning av personalen. Vid fysiska besök förutsätter skötseln av ärenden att e-tjänsten har en metod med vilken den begär, tar emot och verifierar de uppgifter som fås med en plånbok. Det här kan ske så att e-tjänsten tar i bruk en separat kontrollapplikation som kan laddas ner på samma sätt som andra applikationer från applikationsbutiken till e-tjänstens mobila terminal. Dessutom är det möjligt att e-tjänsten inkluderar de tekniska gränssnitt som behövs för kontrollen i sina övriga terminaler och övriga system, som kassasystem. Av dessa alternativ kräver det senast nämnda sannolikt mest ändringar i e-tjänstens befintliga system. Dessutom är det möjligt att e-tjänsten använder en egen europeisk digital identitetsplånbok och att informationen går mellan plånböckerna från användaren till e-tjänsten. I praktiken är detta möjligt i synnerhet i situationer då e-tjänsten är en privat näringsidkare.

4.2.2.4 Administrativa påföljdsavgifter för tillhandahållare av betrodda tjänster

I eIDAS-förordningen förutsätts det att medlemsstaterna säkerställer att kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster kan påföras en administrativ sanktionsavgift om de överträder eIDAS-förordningen. Enligt den föreslagna lagstiftningen ska Transport- och kommunikationsverket ha rätt att förena sina tillsynsbeslut med vite och påföra påföljdsavgifter. Som det beskrivs ovan i avsnitt 3.1.2 finns det exakt information att få om tillhandahållare av kvalificerade betrodda tjänster och de betrodda tjänster de tillhandahåller eftersom de sedan länge har varit skyldiga att anmäla sin verksamhet. Däremot har det funnits mer begränsat med information om icke-kvalificerade tillhandahållare av betrodda tjänster. Utifrån anmälningarna enligt cybersäkerhetslagen till Transport- och kommunikationsverket och sakkunnigbedömningar finns det sammanlagt cirka 50 tillhandahållare av betrodda tjänster i Finland som tillhandahåller flera olika betrodda tjänster. Storleken på tillhandahållarna av betrodda tjänster varierar från medelstora till små aktörer. Det är möjligt att alla aktörer inte själva uppmärksammat att det i deras tjänst handlar om tillhandahållandet av en betrodd tjänst.

Också fysiska personer kan vara tillhandahållare av betrodda tjänster och kan därigenom påföras administrativa påföljdsavgifter om de bryter mot kraven i eIDAS-förordningen. Enligt artikel 3.16 i den förordningen avses med betrodd tjänst en elektronisk tjänst som vanligen tillhandahålls mot ersättning. I praktiken handlar det vid tillhandahållande av betrodda tjänster om näringsverksamhet av något slag. En fysisk person kan tillhandahålla betrodda tjänster i sin verksamhet som privat näringsidkare. Betrodda tjänster handlar om tekniska och komplicerade tjänster och det är osannolikt att fysiska personer eller privata näringsidkare skulle tillhandahålla sådana i särskilt stor omfattning. När propositionen bereddes bedömde man att det mest sannolika är att en fysisk person utfärdar icke-kvalificerade attributsintyg, t.ex. ett stamkundskort av något slag eller något annat intyg i anknytning till sin verksamhet.

I propositionen understryks det att rådgivning och vägledning särskilt i den första fasen ska vara tillsynsmyndigheternas primära medel för att ingripa då förordningen överträds. Tillsammans bildar eIDAS-förordningen och de kompletterande genomförandeförordningarna en omfattande och teknisk regleringshelhet som det krävs både juridisk och teknisk kompetens att sätta sig in i. Detta accentueras i fråga om mindre tillhandahållare av betrodda tjänster, vars juridiska kompetens och resurser vanligen är mer begränsade än hos större tillhandahållare. När det gäller i synnerhet fysiska personer kan deras mer begränsade resurser medföra en större risk för att personen inte känner till kraven i eIDAS-förordningen. Dessutom är påförandet av påföljdsavgift förknippat med en helhetsprövning. Med grund i t.ex. erfarenheterna från tillämpningen av dataskydds- och konkurrenslagstiftningen är bedömningen att påföljdsavgiftens belopp mycket sällan sätts så högt som det föreskrivna maximibeloppet. Även om beloppet av de påföljdsavgifter som påförs mindre företag vanligen är mindre till eurobeloppet, har de ändå kunnat vara större i förhållande till företagets omsättning än för större företag. För att bevara påföljdsavgiftens förebyggande effekt har det inte ansetts att påföljdsavgiftens belopp i synnerhet vid allvarigare överträdelser kan vara särskilt lågt. I propositionen föreslås det dock ett lägre belopp än det föreslagna för påföljdsavgiften för fysiska personer än för juridiska personer.

För att få en uppfattning om hur allmänna påföljdsavgifterna är kan man också konstatera att Transport- och kommunikationsverket och dess föregångare i sin tillsynsverksamhet har påfört endast enstaka påföljdsavgifter och att påföljdsavgifter ännu inte alls har påförts med stöd av digitaliserings- eller datalagstiftning. Påföljdskollegiet vid dataombudsmannens byrå har med stöd av den väldigt allmänt tillämpliga dataskyddsförordningen påfört sammanlagt 24 påföljdsavgifter för överträdelser av dataskyddsförordningen mellan våren 2018 och ingången av augusti 2025. Eftersom antalet tillhandahållare av betrodda tjänster som är etablerade i Finland klart och tydligt är mer begränsat, kan man anta att beloppet av de administrativa påföljdsavgifter som påförs finländska tillhandahållare av betrodda tjänster åtminstone under de närmaste åren kommer att vara mycket måttligt.

Det kan bli aktuellt att påföra påföljdsavgift t.ex. när en kvalificerad tillhandahållare av betrodda tjänster inte tillhandahåller Transport- och kommunikationsverket en rapport för överensstämmelsebedömning med vilken den styrker att den uppfyller de krav som det föreskrivs om i eIDAS-förordningen. Här handlar det om en ur tillsynsmyndighetens perspektiv viktig skyldighet eftersom rapporten om överensstämmelsebedömning ger en beskrivning av den kvalificerade betrodda tjänstens överensstämmelse med kraven. Det är således frågan om en viktig handling när tillsynsmyndigheten beviljar den tjänst tillhandahållaren av betrodda tjänster tillhandahåller en kvalificerad status eller bedömer hur denna status har upprätthållits. Både kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster kan påföras en påföljdsavgift om de uppsåtligt eller av oaksamhet inte anmäler säkerhetsincidenter som riktats mot deras tjänst eller störningar som inträffat vid tillhandahållandet av tjänsten. Skyldigheten att anmäla säkerhetsincidenter eller störningar vid tillhandahållandet av

tjänster säkerställer för sin del att tillsynsmyndigheten kan rikta tillsynsåtgärder mot tjänstetillhandahållaren och eventuellt förutsätta korrigerande åtgärder för att säkerhetsincidenter ska kunna undvikas i framtiden.

4.2.2.5 Avgifter för tillhandahållare av en europeisk digital identitetsplånbok, leverantörer av identifieringstjänster och tillhandahållare av betrodda tjänster samt organ för bedömning av överensstämmelse och certifierare

Det föreslås att de nuvarande tillsynsavgifterna för identifieringstjänster och betrodda tjänster samt för organ för bedömning av överensstämmelse och certifierare (i autentiseringslagen för närvarande certifieringsorgan) höjs. Höjningen bedöms inte ha någon betydande inverkan på de nuvarande tjänsteleverantörerna och tjänstetillhandahållarna. Vid den tidpunkt propositionen bereddes (november 2025) fanns det i Transport- och kommunikationsverkets register 18 leverantörer av stark autentisering. Dessutom finns det i Finland en kvalificerad tillhandahållare av en betrodd tjänst. Tills vidare har inte ett enda sådant organ för bedömning av överensstämmelse eller en enda sådan certifierare som avses i eIDAS-förordningen etablerat sig i Finland. Utöver höjningen av befintliga avgifter föreslås det för tillhandahållare av europeiska digitala identitetsplånböcker en ny årlig tillsynsavgift motsvarande den som finns föreskriven för leverantörer av identifieringstjänster och tillhandahållare av betrodda tjänster. I framtiden kan utvecklingen på plånboksmarknaden leda till att antalet tillhandahållare av plånböcker ökar, men då propositionen bereddes fanns det uppgifter endast om en framtida tillhandahållare av plånböcker, dvs. Myndigheten för digitalisering och befolkningsdata. Myndigheten för digitalisering och befolkningsdata verkar redan nu som leverantör av en tjänst för stark autentisering och som enda tillhandahållare av kvalificerade betrodda tjänster. Höjningen av tillsynsavgifterna kommer således att gälla närmast etablerade aktörer. Höjningen gäller också huvudsakligen stora företag, som banker och teleoperatörer, som tillhandahåller merparten av de elektroniska identifieringstjänsterna.

Tillsynsavgifterna enligt autentiseringslagen höjdes förra gången 2016. Höjningen kan utifrån den allmänna kostnadsnivåökningen och de faktiska kostnader som tillsynen orsakar Transport- och kommunikationsverket anses måttliga och motiverade. Höjningarna grundar sig på Transport- och kommunikationsverkets beräkningar som utgår från Statistikcentralens prisindex för de offentliga utgifterna. T.ex. föreslås det att tillsynsavgiften på 14 000 euro för leverantörer av identifieringstjänster och tillhandahållare av betrodda tjänster höjs till 17 000 euro. Höjd med delindexet för löner och övriga personalkostnader i prisindexet för de offentliga utgifterna från 2016 års nivå till 2024 års nivå och något avrundad är avgiften 17 000 euro när den tas i bruk i slutet av 2026. Förutom höjningen av de nuvarande tillsynsavgifterna kan det anses motiverat med en ny tillsynsavgift för plånböcker eftersom plånböckerna orsakar Transport- och kommunikationsverket helt nya tillsynsuppgifter. Eftersom plånböcker möjliggör också stark autentisering för sina användare, vilket aktörer inom den privata sektorn för närvarande tillhandahåller i förtroendenätet, kan den tillsynsavgift som föreslås för plånböckerna anses förenlig även sett till marknadens funktion och jämlika konkurrensförutsättningar. Transport- och kommunikationsverket bedömer att det efter höjningen av tillsynsavgifterna och påförandet av nya tillsynsavgifter årligen inkommer cirka 368 000 euro som täcker 3,68 årsverken. Den nuvarande tilldelningen av resurser till verket för alla uppgifter för eIDAS-förordningen och autentiseringslagen är totalt fyra årsverken och det framtida behovet av tilläggsresurser bedöms vara tre årsverken.

Storleken på registreringsavgiften för identifieringstjänster och betrodda tjänster, ett utsett certifieringsorgan, dvs. en i den föreslagna eIDAS-lagen avsedd certifierare samt utnämningsavgiften för organ för bedömning av överensstämmelse bestäms framöver enligt lagen om grunderna för avgifter till staten (150/1992) och kommunikationsministeriets

förordning om avgifter som tas ut för Transport- och kommunikationsverkets prestationer som gäller elektronisk kommunikation (nedan *förordning om avgifter för elektronisk kommunikation*). Storleken på behandlingsavgiften för att inleda verksamhet fastställs enligt principen om kostnads motsvarighet i lagen om grunderna för avgifter till staten, dvs. avgiftens storlek motsvarar de totala kostnader produktionen av prestationen föranleder staten. För behandlingen av en anmälan tas det ut en avgift enligt tidsåtgången till självkostnadsvärdet. Eftersom det tas ut en avgift för behandling av anmälan eller ansökan endast när verksamheten inleds handlar det om en engångsprestation.

Genom att ändra författningsnivå blir det möjligt att justera avgiftens storlek mer flexibelt enligt förändringar i kostnadsnivån och i samband med att förordningen uppdateras utan behov att ändra avgiften som ett lagprojekt. Dessutom antas det sporra aktörerna att upprätta anmälningarna om att verksamhet har inletts omsorgsfullt om avgiftens storlek bestäms enligt den tjänstetid som det gått åt för att behandla anmälan. För närvarande tas det ut en fast avgift för behandling av anmälan när tjänstetillhandahållare antecknas i det offentliga register som Transport- och kommunikationsverket förvaltar. Således motsvarar avgiftens storlek inte den mängd arbete som gått åt för behandlingen vid Transport- och kommunikationsverket. Att behandla t.ex. en anmälan med bristfälliga uppgifter kan förutsätta ett flertal begäranden om tilläggsuppgifter innan ärendet kan avgöras. En avgift baserad på tidsåtgången för behandlingen bedöms minska antalet bristfälliga anmälningar till myndigheten och också den arbetsbörda begärandena om tilläggsuppgifter orsakar den som lämnar anmälan. Tjänstetillhandahållaren kan själv försöka påverka avgiftens storlek genom att lämna myndigheten en så omsorgsfullt upprättad anmälan eller ansökan som möjligt.

Eftersom avgiften framöver tas ut för behandlingen av anmälan eller ansökan kan det tas ut en avgift även i de fall där tjänstetillhandahållaren inte antecknas i registret eller godkänns som bedömningsorgan eller certifierare. Det kan således antas att ändringen höjer tröskeln för nya tjänstetillhandahållare att söka sig ut på marknaden eftersom det är förenat med en kostnadsrisk att lämna anmälan eller ansökan. Samtidigt minskar ändringen i den logik enligt vilken avgiften tas ut myndigheternas arbetsmängd för bristfälliga eller ogrundade anmälningar.

4.2.2.6 Nationella ändringar som främjar säkerheten vid användning av stark autentisering

De ekonomiska konsekvenserna av de nationella ändringar som främjar säkerheten vid användning av stark autentisering som föreslås i propositionen riktar sig främst mot leverantörer av identifieringsverktyg. De föreslagna ändringarna bedöms emellertid inte ha några betydande ekonomiska konsekvenser för leverantörerna av identifieringsverktyg eller medborgarna.

Kontroll av passets eller identitetskortets giltighet i polisens informationssystem medför inte omedelbara kostnader för leverantörer av identifieringsverktyg eftersom det är avgiftsfritt att använda polisens informationssystem. För att få tillträde till polisens system kan det ändå förutsätta att leverantörerna av identifieringsverktyg inrättar en anslutningsserver i den nationella servicekanalen som kan medföra kostnader av engångsnatur beroende på aktör. För närvarande har cirka hälften av leverantörerna av identifieringsverktyg integrerat mot polisens tjänst för kontroll av passets och identitetskortets giltighetstid. Av t.ex. leverantörerna av identifieringsverktyg har bankerna lagstadgade uppgifter i anslutning till förhindrande av penningtvätt som förutsätter att handlingars giltighet kontrolleras mot polisens register redan i dagsläget.

De ändringar som föreslås i propositionen förutsätter att leverantörerna av identifieringsverktyg lämnar ut information om användningen av ett identifieringsverktyg för stark autentisering vid den inledande identifieringen till vederbörande leverantör av identifieringsverktyget via ett

gränssnitt eller en tjänst för identitetsförmedling. Transport- och kommunikationsverket rekommenderade förmedling av uppgifter om sammankopplad inledande identifiering redan 2023 varför förslaget inte har någon betydande inverkan på leverantörer av identifieringsverktyg. För de aktörer som inte har infört förmedling av uppgifter om sammankopplad inledande identifiering förutsätter de föreslagna ändringarna ändringar i identifieringsverktygens användargränssnitt och de bakomliggande systemen och medför ekonomiska kostnader. Samtidigt bedöms den föreslagna ändringen dock effektivisera utredningen av missbruk och således minska den tid och de resurser som går åt till det.

I propositionen föreslås det inte ändringar i prisregleringen om identifieringstransaktioner. Skyldigheten att förmedla uppgifter om den inledande identifieringen bedöms möjliggöra för leverantörer av identifieringsverktyg vars beviljade verktyg används för sammankopplad inledande identifiering att, om så önskas, ta ut en högre avgift av leverantören av det nya verktyget för förmedling av en identifieringstransaktion.

4.2.2.7 Uppkomsten och spridningen av innovationer på marknaden

De europeiska digitala identitetsplånböckerna tillhandahåller nya metoder för delning av verifierade uppgifter som avser personer och sålunda även nya innovationer i synnerhet i anslutning till tekniska lösningar. För närvarande är det till vissa delar en utmaning att plånböckerna bygger på nya standarder som delvis fortfarande kräver beredning och testning. Ny teknologi ger emellertid leverantörer av teknik möjlighet att utveckla sina egna tjänster och produkter. De kan t.ex. utveckla tjänster för att underlätta ibruktagandet av plånböcker genom att leverera färdiga delkoncept för snabbare och enklare ibruktagande. För att tillhandahållandet av tjänster ska utvecklas är det emellertid en förutsättning att standardernas innehåll permanentas för att man i utvecklingsarbete som grundar sig på dem inte ständigt ska vara tvungen att göra ändringar i de tjänster som utvecklas. Som bäst kan plånböckerna skapa nya affärsmöjligheter för finska företag på den europeiska digitala inre marknaden. I vilket fall som helst skapas genom förslagen i propositionen enhetliga lagstadgade ramar för utveckling av plånböckerna och hithörande tjänster i Finland. Den föreslagna lagstiftningen etablerar delvis en grund för tillhandahållandet av plånböcker och avlägsnar således den osäkerhet som hänförs sig till tillhandahållandet av dem. Den föreslagna regleringen bedöms således underlätta tillhandahållandet av tjänster enligt den reviderade eIDAS-förordningen även för aktörer som fortfarande överväger saken.

Med propositionens förslag i anslutning till genomförandet av den reviderade eIDAS-förordningen om att utnyttja det nationella handlingsutrymmet i samband med öppenheten i plånbokens källkod och kostnadsfria elektroniska underskrifter eftersträvas att främja uppkomsten av innovationer kring europeiska digitala identitetsplånböcker. För närvarande kan tillhandahållare av tjänster redan tillhandahålla applikationer där det kan finnas intresse för att utveckla dem till att bli en del av plånboken, men där den reviderade eIDAS-förordningens krav på öppenhet i plånbokens källkod fördröjer eller förhindrar detta utvecklingsarbete. Kraven på öppen källkod kan ha motsvarande konsekvenser mer allmänt för utvecklingsarbetet i anslutning till plånböckerna och anknyttande innovationer. Genom förslagen i propositionen vill man begränsa sådana konsekvenser genom att möjliggöra att källkoden i fråga om de bakomliggande systemen inte ska behöva lämnas ut om det finns en vederbörlig orsak.

Den omfattande regleringen om informationssäkerhet och dataskydd i fråga om europeiska digitala identitetsplånböcker kan också i någon mån begränsa uppkomsten av innovationer. Med tanke på att användningen blir allt mer omfattande och vanlig är det viktigt att man i standarder som gäller för plånböckerna försöker balansera säkerhet och användbarhet. En annan utmaning för uppkomsten av innovationer är att EU när det gäller plånböcker är något av en föregångare.

Utmaningen kan konkretiseras t.ex. så att man i EU prioriterar interoperabiliteten mellan medlemsstaterna och fäster mindre uppmärksamhet vid behovet av global interoperabilitet i fråga om plånböckerna. På motsvarande sätt behöver man även i fråga om sektorsvisa regleringsalternativ beakta att de som bäst kan främja en allmännare användning av plånböcker, men de ska dock rent faktiskt bygga på de centrala verksamhetsprinciperna för plånböckerna och inte skapa parallella, överlappande eller i värsta fall motstridiga krav.

För att innovationer i samband med plånböckerna ska uppkomma och spridas på marknaden kan man se en viss utmaning i fråga om balansen mellan efterfrågan och utbud. För att det ska uppkomma efterfrågan på e-tjänster som använder en plånbok, ska plånböckerna först på ett tillräckligt sätt erbjuda elektroniska intyg som har potential som e-tjänsterna kan utnyttja. Ett brett utbud av elektroniska intyg främjar sannolikt också en bred användning av plånböcker bland användarna vilket anses vara viktigt också med tanke på att innovationer ska uppkomma och spridas. Särskilt i fråga om e-legitimationen strävar förslagen i propositionen efter att främja en bred användning av plånboken ända från början genom att ge användarna en möjlighet att få det första elektroniska attributsintyget i plånboken. Dessutom eftersträvas med propositionens förslag om Myndigheten för digitalisering och befolkningsdatas roll att vidta åtgärder för kontroll av uppgifter i autentiska källor att främja en allmän användning av elektroniska attributsintyg.

4.2.2.8 Konsekvenser för statsbudgeten

Skötseln av de uppgifter som föreslås i propositionen för genomförandet av den reviderade eIDAS-förordningen är förknippad med flera praktiska osäkerhetsfaktorer varför det är svårt att ge en helt tillförlitlig bedömning av de konsekvenserna. Osäkerhet råder t.ex. om de genomförandeförordningar kommissionen antar med stöd av eIDAS-förordningen och om deras innehåll. Beredningen av genomförandeförordningarna blev ännu inte klar medan propositionen bereddes och dessutom har kommissionen uttryckt att den har för avsikt att uppdatera redan antagna genomförandeförordningar. Genomförandeförordningarna och de standardhänvisningar som ingår i dem har emellertid betydande konsekvenser för hur skyldigheterna enligt den reviderade eIDAS-förordningen tekniskt ska fullgöras. Om innehållet i genomförandeförordningarna ändras väsentligt påverkar det även det planerade sättet att genomföra uppgifterna.

Osäkerheten gäller även prognostiseringen av hur mycket den europeiska digitala identitetsplånboken med tillhörande system och tjänster kommer att utvecklas och användas i framtiden. Det är frivilligt för användarna att ta i bruk en plånbok, men e-tjänsterna är i vissa fall skyldiga att möjliggöra identifiering med hjälp av en plånbok. Antalet användare påverkar också t.ex. kostnaderna för att ta i bruk en plånbok eller rådgivningen om användningen. Dessutom kommer den mer allmänna utvecklingen av plånböckerna och de attributsintyg som används med hjälp av dem att ske i etapper, vilket också påverkar mängden tillsynsuppgifter som hänförs till tjänsterna. Det kan emellertid redan ses att man i ett flertal av EU:s lagstiftningsprojekt försöker verka för att olika elektroniska bevis ska vara interoperabla med plånböckerna och den vägen bidra till en omfattande användning av plånböcker i samhället.

Av anledningar som beskrivs ovan bedömdes det inte vara behövligt att vid beredningen av propositionen föreslå att resurser tilldelas genom tilläggsanslag i statens budget för 2026. Resurstilldelningen ska i första hand möjliggöras genom effektivisering av myndigheternas nuvarande uppgifter och anpassning av verksamheten. Det utvecklingsarbete som genomförandet av den reviderade eIDAS-förordningen förutsätter finansieras av projektet för nationellt genomförande av den reviderade eIDAS-förordningen (se närmare om projektet i avsnitt 1.2). Största delen av uppgifterna i anslutning till den reviderade eIDAS-förordningen,

som t.ex. den europeiska digitala identitetsplånboken och tillhandahållandet av hithörande system och tjänster samt tillsynsuppgifterna inleds i december 2026, men myndigheterna måste förbereda sig på rådgivning och vägledning redan innan dess. Resursbehoven grundar sig på motiverade bedömningar av framtida kostnader för plånboken och tillhandahållandet av system och tjänster och på tillsynsuppgifternas mängd och beskaffenhet. Mer heltäckande och tillförlitlig information om resursbehoven kan emellertid finnas tillgänglig först efter att det finns praktisk erfarenhet av tillhandahållandet av de tjänster som eIDAS-förordningen förutsätter och av genomförandet av uppgifterna.

4.2.3 Övriga konsekvenser för människor och samhälleliga konsekvenser

4.2.3.1 Allmänna konsekvenser

Den europeiska digitala identitetsplånbok som införs som ett led i genomförandet av den reviderade eIDAS-förordningen grundar sig på så kallad egen kontroll över uppgifter. Det handlar om en modell för behandling av personuppgifter där en person själv kan hantera tillhandahållandet av sina personuppgifter från sig själv eller betrodd tredje part till e-tjänster där personuppgifterna behövs. I praktiken kan användaren av en plånbok alltså samla in uppgifter om sig själv i elektronisk form från olika aktörer och lägga dem i plånboken. Därefter kan han eller hon i olika kommunikationssituationer själv visa de uppgifter som finns i plånboken i stället för att e-tjänsten hämtar uppgifterna exempelvis i en myndighets register. I praktiken avser det att en person har egen kontroll över uppgifterna alltså att personen själv bestämmer om användningen av sina personuppgifter. Användningen av plånböcker främjar således användarnas egen kontroll över sina uppgifter i samhället och gör behandlingen av personuppgifter mer transparent. Samtidigt flyttar kontrollen över de egna uppgifterna ansvaret för att personuppgifterna behandlas på ett säkert sätt över personen själv.

Plånboken är också en av kundrelationer oberoende metod för stark autentisering och visande av uppgifter. Med detta avses att användaren inte behöver vara kund hos en viss tjänstetillhandahållare för att kunna ta i bruk en plånbok. I nuläget är erhållandet av de nätbankskoder som används som verktyg för elektronisk identifiering knutet till att personen har en kontorelation hos banken, och nätbankskoder erbjuds inte en person som saknar kundrelation. Likaså är erhållandet av de mobilcertifikat som används som identifieringsverktyg för stark autentisering knutet till en kundrelation för mobilkommunikationsabonnemang. Ett verktyg för elektronisk identifiering som är oberoende av kundrelationer förbättrar allmänt taget medborgarnas likvärdiga möjligheter att kommunicera elektroniskt i olika tjänster i samhället. Det här kan i synnerhet göra det lättare att få ett elektroniskt identifieringsverktyg för personer som vistas i Finland endast tillfälligt och inte har behov av att skaffa banktjänster eller telefonabonnemang. Sådana är exempelvis säsongsarbetare och studerande. Plånboken bedöms emellertid inte åtminstone på kort sikt i någon betydande grad medföra ändringar i hur konsumenten identifierar sig i e-tjänster. De verktyg för stark autentisering som konsumenterna redan i nuläget använder kvarstår i bruk vid sidan av plånboken och det går också i fortsättningen att kommunicera med hjälp av dem i elektroniska tjänster inom den offentliga sektorn.

Utöver elektronisk identifiering gör den europeiska digitala identitetsplånboken det möjligt att skapa kvalificerade elektroniska underskrifter. För närvarande kan konsumenterna skapa motsvarande kvalificerade elektroniska underskrifter främst med identitetskort som innehåller signaturcertifikat. Konsumenterna har emellertid tillgång också till andra lösningar för elektronisk underskrift, såsom avancerade elektroniska underskrifter. Användningen av elektroniska underskrifter har över huvud taget varit rätt liten i dagliga situationer. Kvalificerade elektroniska underskrifter är till sina rättsverkningar jämförbara med underskrifter som gjorts

för hand. Därmed kan en mer utbredd användning av dem i samhället underlätta kommunikationen för konsumenter i samhället och exempelvis minska behovet av fysiska besök för att sköta olika ärenden.

Den europeiska digitala identitetsplånboken möjliggör också användningen av elektroniska attributsintyg. I propositionen föreslås det att Finlands första elektroniska attributsintyg, det vill säga en e-legitimation, införs. Avsikten med införande av e-legitimation är att redan i ett tidigt skede skapa möjligheter för konsumenterna att utnyttja plånboken i olika kommunikationssituationer och detta bedöms för sin del främja ett mer utbrett ibruktagande av plånboken. De oberoende konsekvenserna av detta bedöms nedan i detta avsnitt. Allmänt taget realiserar nyttan i anslutning till elektroniska attributsintyg för konsumenterna först i det skedet när de är mer omfattande tillgängliga inom olika sektorer. Vid beredningen av proposition bedömdes det att till exempel kostnaderna för tillstånd och intyg kan sjunka om ansökan om och produktionen av fysiska handlingar och kort görs elektronisk. Omvandlingen av dessa funktioner till elektroniska processer sänker sannolikt kostnaderna både för dem som beviljar och dem som ansöker om tillstånd och intyg.

Myndigheten för digitalisering och befolkningsdata utförde hösten 2025 en medborgarundersökning om en ny applikation i anslutning till elektronisk identifiering. Avsikten med enkäten var att utreda hur medborgarna använder olika elektroniska identifieringsmetoder och att kartlägga medborgarnas intresse för att ta i bruk en ny applikation och den anknyttande identifieringsmetoden. Enkäten inkluderade också insamling av medborgarnas önskemål om applikationens egenskaper och förslag om namn på applikationen. Uppgiftsinsamlingen utfördes som panelenkät mellan den 1 och den 17 september 2025. De huvudsakliga målgrupperna för undersökningen var finländare i åldern 18–99 år. Totalt 1032 personer besvarade enkäten. Det viktade materialet utgör ett på riksnivå representativt sampel enligt kön, ålder och bostadsområde.

Enkäten visade att medborgarna i rätt stor omfattning använder olika slag av elektronisk utrustning som gör det möjligt att använda den nya applikationen. Av dem som svarade hade 98 procent en pekplatta eller smarttelefon i bruk och som svar på frågorna om bakgrundsinformation uppgav 61 procent att de själv kan söka lösningar på problem med användningen av dem. Dessutom var 45 procent intresserade av nya digitala tjänster och apparater. Däremot hade största delen av respondenterna inte behov av gränsöverskridande kommunikation vid tidpunkten för enkäten. Av respondenterna använde 92 procent inte vid tidpunkten i fråga elektroniska tjänster i någon annan EU-medlemsstat, utan kommunikationen var koncentrerad till e-tjänster i Finland. Majoriteten av respondenterna (63 procent) hade inget behov av att sköta ärenden elektroniskt i någon annan medlemsstats e-tjänster.

Attityden till att använda den nya applikationen var huvudsakligen positiv. Av respondenterna var 51 procent intresserade av att ta i bruk den nya applikationen och 30 procent förhöll sig neutralt till ibruktagande av den. Av respondenterna var 19 procent inte intresserade av att ta applikationen i bruk. Intresset för de funktioner och nya möjligheter inom kommunikation som applikationen erbjuder var mycket stort. Av respondenterna var 73 procent intresserade av att identifiera sig elektroniskt med applikationen i Finland, 74 procent var intresserade av att få olika elektroniska intyg i applikationen, 72 procent var intresserade av att styrka sin identitet med applikationen och 71 procent var intresserade av elektronisk underskrift. Av respondenterna var 20 procent intresserade av att kommunicera elektroniskt i andra EU-medlemsstater.

I användarundersökningen kartlades respondenternas intresse för att få olika tillstånd, intyg eller kort i elektronisk form i den nya applikationen. Enligt beskrivningen ovan är elektroniska

attributsintyg ett nytt sätt att visa uppgifter som gäller en själv elektroniskt och på ett tillförlitligt sätt. Respondenterna var intresserade av rätt vanliga elektroniska intyg i anslutning till den egna vardagen. Av respondenterna önskade 83 procent få exempelvis FPA-kortet i applikationen och 82 procent var intresserade av att få legitimation och körkort i applikationen. Också andra tänkbara intyg som togs upp i enkäten fick understöd och respondenterna föreslog också många andra tänkbara elektroniska intyg. Sådana var exempelvis vapentillstånd, bibliotekskort och EU-intyget om funktionsnedsättning (EU:s funktionshinderkort).

I undersökningen efterfrågades också eventuella hinder för att ta i bruk applikationen. Många respondenter såg inga hinder för att ta i bruk applikationen. De största hinder som nämdes hade att göra med informationssäkerhet och användbarhet. Respondenterna önskade att applikationen ska vara säker, lättanvänd och alternativ. De ville alltså inte att det ska vara obligatoriskt att använda den. Många önskade att de traditionella identifieringssätten kvarstår vid sidan av den nya applikationen och att ibruktagandet inte förutsätter särskilda nya tekniska färdigheter.

Som ett sammandrag av resultaten i medborgarundersökningen kan det konstateras att många är intresserade av att ta i bruk den nya applikationen. Respondenterna hade däremot inte något nämnvärt behov av gränsöverskridande kommunikation. De var intresserade av att använda applikationen i synnerhet för elektronisk identifiering i Finland. Dessutom var de intresserade av olika elektroniska intyg. Att applikationen är lätt att använda och säker var viktiga egenskaper för respondenterna.

En e-legitimation i enlighet med förslaget möjliggör en ny metod för personer att styrka sin identitet vid besök för att sköta ärenden det vill säga vid ett personligt besök hos en tjänstetillhandahållare. Enligt den lagstiftning som föreslås i propositionen kan e-legitimation användas för att styrka identiteten vid besök för att sköta ärenden på samma sätt som man i nuläget använder identitetskort och pass. E-legitimationen kan underlätta exempelvis oplanerade besök för att sköta bankärenden eller annat motsvarande där identiteten måste kunna styrkas på ett tillförlitligt sätt. Förslaget kan på längre sikt ha en positiv effekt på harmoniseringen av metoder för att styrka identiteten vid besök för att sköta olika ärenden. Det kan också till exempel minska personers ovetskap om när körkort duger som identitetsbevis och när det krävs pass eller identitetskort.

Enbart det att en mobil enhet förekommer betyder inte heller i alla situationer automatiskt att också användningen av e-legitimationen äventyras betraktas som en positiv konsekvens av införande av e-legitimation, liksom av andra elektroniska attributsintyg som eventuellt införs i framtiden. Där det till följd av att en fysisk handling förekommer eller stjäls är möjligt att den används obehörigt eller annars för oegentligheter och brott eller för att forcera handlingens säkerhetsfunktioner, kräver användningen av ett elektroniskt attributsintyg via plånboken olika lösenord eller identifieringskoder som plånbokens användare känner till. Dessutom är det möjligt att avsluta giltigheten för attributsintyget omedelbart om den mobila enheten förekommer, blir stulen eller en situation med manipulation uppdagas.

Införande av e-legitimationen som kvalificerat elektroniskt attributsintyg, det vill säga så att den är interoperabel med plånboken, tar också styrkandet av identiteten vidare mot en handlingsmodell som blir vanligare i olika kommunikationssituationer, där en person inte behöver något annat än en mobil enhet för att sköta sina ärenden. Förslaget bedöms underlätta och förenkla medborgarnas kommunikation i olika samhälleliga tjänster. I praktiken kan medborgarnas möjligheter att använda e-legitimation ändå vara olika beroende på de krav som är förknippade med användningen av lösningen samt av ekonomiska orsaker eller orsaker som är relaterade till personens fysiska funktionsförutsättningar.

4.2.3.2 Barn och unga

De lagstiftningsförslag som hänför sig till genomförandet av den reviderade eIDAS-förordningen kan förbättra barns möjligheter att sköta ärenden digitalt i vissa tjänster samt föräldrarnas möjligheter att sköta sina barns ärenden. De här konsekvenserna gäller emellertid huvudsakligen barn som är äldre än 13 år. Enligt förslaget kan en 13-åring självständigt ta i bruk en europeisk digital identitetsplånbok om det är möjligt i enlighet med kraven på tillitsnivån hög. Barn som är yngre än så kan enligt förslaget ta i bruk en plånbok med vårdnadshavarens samtycke. Minderåriga som tar en plånbok i bruk kan med den styrka sin identitet på motsvarande sätt som med de nuvarande verktygen för stark autentisering. Till exempel inom social- och hälsovården är det möjligt att en 13-åring anlitar tjänsterna självständigt utan vårdnadshavare. Då kan möjligheten att styrka sin identitet elektroniskt och använda elektronisk underskrift med den europeiska digitala identitetsplånboken förbättra möjligheterna för personer som fyllt 13 år att sköta ärenden som gäller dem själva elektroniskt. I nuläget är barns möjligheter att få använda ett verktyg för stark autentisering varierande beroende på den som beviljar verktyget och möjligheten är ofta bunden till vilka andra tjänster det är möjligt att erbjuda barnet. Vissa leverantörer av identifieringsverktyg har inga åldersgränser för erhållande av identifieringsverktyg med vårdnadshavarnas samtycke, medan andra tillämpar en åldersgräns (t.ex. 12 år) och krav på samtycke av vårdnadshavarna.

Den föreslagna regleringen kan förbättra skyddet för minderåriga i elektroniska tjänster och således främja elektronisk kommunikation på ett säkert sätt för barn. Med hjälp av en europeisk digital identitetsplånbok är det möjligt att styrka användarens ålder på ett tillförlitligt sätt, vilket kan möjliggöra kontroll av åldersgränser i anslutning till olika elektroniska tjänster och kanaler på sociala medier. I praktiken kan det exempelvis handla om att kontrollera åldersgränserna för mobilspel med hjälp av plånboken. Samtidigt kan ibruktagandet av en europeisk digital identitetsplånbok ha konsekvenser för minderåriga i form av att brottsligheten och identitetsstöldrarna på nätet ökar. Det kan vara svårt för en minderårig att uppfatta till exempel att ett elektroniskt identifieringsverktyg som hamnat i fel händer möjliggör bedrägerier i en annans namn.

Det bör dock observeras att det inte föreslås ändringar när det gäller i vilka situationer och under vilka förutsättningar ett barn kan sköta sina ärenden självständigt. Förslagen i propositionen inverkar inte heller på förutsättningarna för beviljande av olika elektroniska intyg. Med detta avses att även om en minderårig kan få en plånbok i självständigt bruk har han eller hon ändå inte rätt att få sådana elektroniska intyg kopplade till plånboken som inte kan beviljas en minderårig. Propositionens viktigaste konsekvens med tanke på barns elektroniska kommunikation är att det sannolikt kan bli något enklare än i nuläget att få ett verktyg för stark autentisering. Alla digitala tjänster förmår emellertid inte ta emot minderåriga som kommunicerar självständigt om systemen i regel är uppbyggda bara för vuxna. Att göra det möjligt för minderåriga att kommunicera kan förutsätta exempelvis att e-tjänsten har förmåga och behov att identifiera vid vilken ålder personer kan sköta ärenden i tjänsten samt att kontrollen av ålder görs till en del av processen.

4.2.3.3 Utlandsfinländare

En metod för stark autentisering som är oberoende av kundrelationer kan förbättra i synnerhet utlandsfinländares möjligheter att sköta ärenden i finländska e-tjänster. I fråga om utlandsfinländare har det i flera sammanhang tagits upp att det är svårt för dem att sköta ärenden i Finland elektroniskt, eftersom de ofta inte har något verktyg för stark autentisering. En förutsättning för erhållande av ett sådant är på det sätt som beskrivs ovan en kundrelation hos någon finländsk bank eller teleoperatör. Den europeiska digitala identitetsplånboken förutsätter

inte kundrelation hos en finländsk bank eller teleoperatör eller i någon annan tjänst. I praktiken förutsätter ibruktagandet av en identitetsplånbok för en fysisk persons del att han eller hon är registrerad i befolkningsdatasystemet. På den grunden kan han eller hon för plånboken beviljas uppgifter för personidentifiering av en fysisk person.

Den föreslagna regleringen gör det möjligt att ta i bruk en europeisk digital identitetsplånbok också vid ärenden som sköts vid besök hos Finlands utländska beskickningar. Detta kan främja utlandsfinländares möjligheter att i fortsättningen sköta ärenden i den offentliga sektorns digitala tjänster när det är möjligt för dem att få plånboken i bruk på plats vid beskickningen. En europeisk digital identitetsplånbok kan underlätta gränsöverskridande kommunikation för utlandsfinländare till exempel när det gäller pensionsrelaterade elektroniska ärenden. I och med ibruktagandet av en europeisk digital identitetsplånbok får utlandsfinländare dessutom möjlighet att ta i bruk också e-legitimation. Allt som allt utgör utlandsfinländarna emellertid en relativt liten andel av det totala antalet användare av digitala tjänster.

4.2.3.4 Personer med funktionsnedsättning

Den reglering som föreslås i anslutning till genomförandet av den reviderade eIDAS-förordningen kan ha konsekvenser för personer som behöver hjälp av en annan person för att kunna använda en europeisk digital identitetsplånbok. Den föreslagna regleringen innehåller ett förbud mot att överlåta verktyget för att användas av någon annan på samma sätt som det i nuläget förbjuds i autentiseringslagen när det gäller verktyg för stark autentisering. Enligt den föreslagna regleringen ansvarar en person dessutom för användningen av plånboken om han eller hon själv har överlåtit den för att användas av någon annan. I fråga om de verktyg för stark autentisering som finns på marknaden i nuläget har det förekommit utmaningar i fråga om huruvida det går att ha hjälp av en assistent i användningen av identifieringsverktyget. När assistent anlitas måste innehavaren av identifieringsverktyget sannolikt ge verktyget eller de lösenord eller andra verifieringsfaktorer som behövs till assistenten. Detta äventyrar identifieringsverktygets tillförlitlighet på det sätt som man i regel bedömt i samband med eIDAS-förordningen och tillämpningen av den. När det gäller identifieringsverktygets tillförlitlighet är en väsentlig fråga i synnerhet identiteten hos en person som kopplas till ett visst identifieringsverktyg och att säkerställa att endast denna person använder identifieringsverktyget.

Den föreslagna regleringen begränsar emellertid inte regleringen i den reviderade eIDAS-förordningen när det gäller möjligheterna för personer med funktionsnedsättning att använda plånboken likvärdigt. Enligt artikel 5 a.21 i den reviderade eIDAS-förordningen ska europeiska digitala identitetsplånböcker göras tillgängliga för användning av personer med funktionsnedsättning, på samma villkor som andra användare, i enlighet med Europaparlamentets och rådets direktiv (EU) 2019/882 (nedan *tillgänglighetsdirektivet*). Tillgänglighetsdirektivet ställer likvärdiga tillgänglighetskrav på terminalutrustning som säljs på EU:s inre marknad. De nationella lagar som genomför direktivet började tillämpas 2025. Som helhet betraktat kommer möjligheten att använda plånboken alltså att gälla en mycket omfattande skara användare.

Det bör därtill noteras att största delen av terminalutrustningen innehåller rikligt med stödjande teknik av olika slag (t.ex. ändring av storleken på innehållet på skärmen, olika kontrastmöjligheter, talstyrning), varvid plånbokens lagringsmedium i regel är tillgängligt. Dessutom ska den europeiska digitala identitetsplånboken uppfylla tillgänglighetskraven i 3 kap. i lagen om tillhandahållande av digitala tjänster (306/2019). Tjänstens tillgänglighet bedöms i enlighet med nivåerna 2.1 A och AA i riktlinjerna för utformning av tillgängligt innehåll på webben (Web Content Accessibility Guidelines, WCAG). Dessutom säkerställs det

med hjälp av användbarhetstest att tjänsten är användbar och förståelig. Vid utveckling och testning av plånboken beaktas olika människors behov och användningsvanor. Man strävar också efter att göra det möjligt att använda plånboken med olika slag av hjälpmedel. Ett tillgänglighetsutlåtande publiceras om plånboken och i tjänsten inkluderas en elektronisk kanal för tillgänglighetsrespons.

Den föreslagna regleringen kan således förbättra möjligheterna för personer med funktionsnedsättning att kommunicera elektroniskt. Personer som inte kan använda plånboken trots att den är tillgänglig kan ändå få sina ärenden skötta elektroniskt t.ex. genom att befullmäktiga en annan person att sköta ärenden för sig. Då agerar den befullmäktigade i eget namn för en annan persons räkning och styrker sin egen identitet antingen fysiskt eller elektroniskt och kan i e-tjänsten sköta de ärenden som fullmakten omfattar. Ärendet sköts då på motsvarande sätt också t.ex. i situationer som gäller intressebevakning. Också i dessa fall verkar intressebevakaren i eget namn och styrker sin egen identitet och kan därefter vidta de åtgärder som omfattas av intressebevakningen. Den europeiska digitala identitetsplånboken kan i sådana situationer användas för identifiering av den befullmäktigade eller intressebevakaren. I framtiden kan det också vara möjligt att det skapas egna identifieringsuppgifter för olika situationer där användaren sköter ärenden för någon annan och där plånboken används uttryckligen för dessa åtgärder. När fullmakt används är risken för missbruk mindre än när hemliga identifieringsuppgifter som möjliggör användning av ett identifieringsverktyg måste yppas för en annan person. Även om användningen av fullmakt inte direkt kan ersätta möjligheten att sköta ärenden personligen kan det ändå i vissa situationer vara ett ändamålsenligt alternativ.

4.2.3.5 Konsekvenser för myndigheterna

Myndigheten för digitalisering och befolkningsdata. Enligt propositionen ska Myndigheten för digitalisering och befolkningsdata ha i uppgift att tillhandahålla en europeisk digital identitetsplånbok samt anknyttande system och tjänster. Detta begränsar emellertid inte andra tjänsteleverantörers möjligheter att tillhandahålla plånböcker vid sidan av den som Myndigheten för digitalisering och befolkningsdata tillhandahåller. Myndigheten för digitalisering och befolkningsdatas roll som tillhandahållare av en plånbok har bedömts ovan sett till dess konsekvenser för konkurrensen i avsnitt 4.2.2.2 och alternativa handlingsvägar i avsnitt 5.1.1. Vid införandet av den europeiska digitala identitetsplånboken och de anknyttande systemen och tjänsterna handlar det om en ny uppgift. Det är fråga om en omfattande helhet och på grund av att arbetet med genomförandet är av teknisk art är det inte ändamålsenligt att beskriva det uttömmande i denna proposition. Genomförandet av uppgiften innefattar emellertid åtminstone utveckling av en mobilapplikation och publicering av denna i appbutiker samt genomförande av införandet av applikationen. Avsikten är också att plånboken ska göra det möjligt att visa och administrera uppgifter i elektroniska tjänster och vid besök för att sköta ärenden samt att använda kvalificerad elektronisk underskrift. Införande av plånboken i enlighet med kraven i eIDAS-förordningen förutsätter också att flera nya bakomliggande system, såsom register, införs. Dessutom ska Myndigheten för digitalisering och befolkningsdata tillhandahålla användarstöd för användningen av plånboken.

Enligt propositionen ska Myndigheten för digitalisering och befolkningsdata utifrån befolkningsdatasystemet utfärda uppgifter för personidentifiering av fysiska personer som gör det möjligt för dem att styrka sin identitet med hjälp av plånboken. Detta förutsätter att Myndigheten för digitalisering och befolkningsdata genomför ett nytt gränssnitt och identifiering av användaren på ett sådant sätt att kraven för tillitsnivån hög uppfylls. Dessutom förutsätter uppgiften införande av funktioner bland annat för validering av europeiska digitala identitetsplånböcker och skapade av identitetsuppgifter för personer. Dessutom ska

Myndigheten för digitalisering och befolkningsdata enligt propositionen genomföra en tjänst för så kallad identitetsmatchning, vilket i praktiken förutsätter att en funktion av ny typ utvecklas. Tjänsten för identitetsmatchning genomförs som en centraliserad lösning för e-tjänster inom den offentliga förvaltningen och dessutom möjliggörs användningen av den i ett senare skede för aktörer inom den privata sektorn. Befolkningsdatasystemet används som register för identitetsmatchningen och identitetsmatchningen görs mot systemet med hjälp av identifieringsuppgifterna i plånboken eller uppgifter som erhållits med hjälp av elektroniska identifieringsmetoder som anmälts enligt eIDAS-förordningen.

Enligt propositionen får Myndigheten för digitalisering och befolkningsdata också andra uppgifter i anslutning till genomförande av den reviderade eIDAS-förordningen. Dessa är att vidta åtgärder för att säkerställa att kvalificerade leverantörer av betrodda tjänster som tillhandahåller elektroniska attributsintyg kan kontrollera attribut enligt bilaga VI i den reviderade eIDAS-förordningen mot deras autentiska källa. Dessutom ska Myndigheten för digitalisering och befolkningsdata enligt förslaget delta i införandet av e-legitimation genom att bevilja det kvalificerade elektroniska attributsintyg som används som e-legitimation. Myndigheten för digitalisering och befolkningsdata utreder de olika alternativen för genomförande av de uppgifter och tjänster och de delfunktioner som anvisas myndigheten i propositionen. Avsikten är att utreda till vilka delar det är ändamålsenligt att utnyttja det färdiga utbud som finns på marknaden, lösningar för öppen källkod, färdigt utformade mallar eller lösningar som tagits fram i olika pilotförsök och till vilka delar det är ändamålsenligt att utveckla eller upprätthålla partiella genomföranden som eget arbete vid Myndigheten för digitalisering och befolkningsdata.

Flera av de uppgifter som enligt propositionen anvisas Myndigheten för digitalisering och befolkningsdata är förknippade med kommissionens bemyndigande att utfärda genomförandeförordningar och de flesta av dem har redan utfärdats. Kommissionen har emellertid meddelat att den har för avsikt att uppdatera genomförandeförordningarna innan tidsfristen för medlemsstaternas skyldigheter löper ut. Dessutom är en del av genomförandeförordningarna så nya att planeringsarbetet för det nationella genomförandet fortfarande pågår. Det är också i övrigt fråga om reglering av en helhet av helt ny typ, som bygger på tekniska lösningar av ny typ och på nya standarder. Myndigheten för digitalisering och befolkningsdata har hittills emellertid bedömt att resursbehovet för utveckling av en europeisk digital identitetsplånbok samt de anknyttande systemen och tjänsterna är totalt 6 400 000 euro 2025–2026. Dessutom har Myndigheten för digitalisering och befolkningsdata bedömt att resursbehovet för den kontinuerliga tjänsten är 9,5 årsverken 2027, 7,5 årsverken 2028 och därefter 6,5 årsverken 2029 och 2030. Resursbehoven för den kontinuerliga tjänsten omfattar bl.a. genomförande av den europeiska digitala identitetsplånboken och identitetsmatchningen, beviljande av identitetsuppgifter för fysiska personer, uppgifter i anslutning till kund- och intressentgruppssupport samt andra kostnader i anslutning till genomförande och upprätthållande av de föreslagna uppgifterna. Av de ovan beskrivna orsakerna är resursbehoven emellertid fortfarande förknippade med reservationer, och de kan förändras i en eller annan riktning.

Transport- och kommunikationsverket. Enligt propositionen har Transport- och kommunikationsverket till uppgift att inrätta och upprätthålla ett nationellt register över förlitande parter, där europeiska digitala identitetsplånböcker i praktiken kontrollerar förlitande parter och deras uppgifter innan personuppgifter lämnas ut från en plånbok. Kommissionen har antagit en genomförandeförordning vad gäller registrering av förlitande parter (EU) 2025/848, där kraven på registret fastställs. Transport- och kommunikationsverket har genomfört en förutredning för att fastställa hur registret över förlitande parter ska inrättas och vilka ansvarsparterna, intressentgrupperna, resursbehoven och kostnaderna är och vilket tidsschemat

är samt för att fastställa kostnaderna för förvaltning av registret. Transport- och kommunikationsverket har hittills preliminärt bedömt att resursbehovet för registret över förlitande parter är 600 000 euro 2024–2026 för inrättande av registret och från och med 2026 årligen 100 000 euro för förvaltning av registret.

Dessutom ska Transport- och kommunikationsverket enligt propositionen ha till uppgift att verka som tillsynsmyndighet som avses i den reviderade eIDAS-förordningen både i fråga om leverantörer av betrodda tjänster och de tjänster de tillhandahåller och i fråga om lagstiftningen om en europeisk digital identitet. När det gäller leverantörer av betrodda tjänster och de tjänster de tillhandahåller handlar det om att fortsätta med en befintlig uppgift, men när det gäller lagstiftningen om en europeisk digital identitet handlar det om en ny uppgift. Enligt propositionen ska Transport- och kommunikationsverket också vara den gemensamma kontaktpunkt som avses i den reviderade eIDAS-förordningen och ansvara för vissa anmälningar som ska göras till Europeiska kommissionen. I de lagar som ingår i propositionen föreskrivs det om de rättigheter att få information och de befogenheter som behövs för att Transport- och kommunikationsverket ska kunna sköta sina uppgifter. Transport- och kommunikationsverket kan t.ex. ålägga en aktör att korrigera sin verksamhet eller tillfälligt upphäva tillhandahållandet av en tjänst samt förena sitt beslut med vite. Transport- och kommunikationsverket kan också påföra en tillhandahållare av en betrodd tjänst en administrativ påföljdsavgift om denna bryter mot kraven i förordningen. Transport- och kommunikationsverket har bedömt att resurskostnaderna för de ökande tillsynsuppgifterna blir 3 årsverken per år från och med 2026.

Transport- och kommunikationsverket ska dessutom ha till uppgift att vara ägare till certifieringsordningen för de europeiska digitala identitetsplånböcker som tillhandahålls i Finland och således också ansvara för beredningen av plånbokens innehåll och uppdateringen av det. Den nationella certifieringsordningen bereds i samarbete med de nordiska och de baltiska länderna och avsikten är att den certifieringsordning som samarbetet resulterar i ska användas vid certifieringen av den plånbok som Myndigheten för digitalisering och befolkningsdata tillhandahåller. Om också andra europeiska digitala identitetsplånböcker tillhandahålls i Finlands av den privata sektorn är det möjligt att egna nationella certifieringsprofiler måste skapas för dem i samband med den nationella certifieringsordningen. I certifieringsprofilen beaktas de tekniska särdragen i varje plånbok som tillhandahålls. Transport- och kommunikationsverket har bedömt att behovet av engångsresurs för beredning och upprätthållande av en enskild certifieringsprofil är 40 000 euro.

Polisstyrelsen. Enligt förslaget görs ansökan om e-legitimation hos polisen och e-legitimationen genomförs som kvalificerat elektroniskt attributsintyg som beviljas av Myndigheten för digitalisering och befolkningsdata. Således är den interoperabel med den europeiska digitala identitetsplånboken. Beviljandet av e-legitimation och främjandet av användningen av den förutsätter att en mobilapplikation utvecklas i fråga om de visnings- och kontrollgenskaper som behövs vid besök för skötsel av ärenden, att de förfrågningsgränssnitt genomförs som behövs mot polisens system Heko-Passi och mot en e-tjänstplattform, att kapaciteten och servicenivån i vissa system och den elektroniska plattformen utvidgas samt att program och utrustning utvecklas som möjliggör kontrollen av e-legitimationer bl.a. på polisens verksamhetsställen för tillståndsärenden och för fältarbetare. Polisstyrelsen har bedömt att de fortlöpande kostnaderna för att administrera beviljandet av e-legitimationer är 300 000 euro.

De kostnader som upprätthållandet av e-legitimationer orsakar polisen och Myndigheten för digitalisering och befolkningsdata ska täckas genom att lagen om grunderna för avgifter till staten tillämpas på klientavgifterna för pass och identitetskort. Kostnadernas effekt på priset för pass och identitetskort är mycket måttlig, och den kan inte bedömas ha någon betydelse

exempelvis för efterfrågan på handlingarna. Att täcka kostnaderna för e-legitimation kan enligt en preliminär bedömning vid beredningen höja priset på pass och identitetskort med i medeltal 0,39–0,96 euro per handling under en granskningsperiod på drygt tjugo år. Den årliga inverkan varierar i praktiken enligt efterfrågan på handlingarna. Enligt de uppgifter som står till buds är inverkan 2028 enligt en preliminär bedömning cirka 60 cent per handling. Som störst är inverkan under sådana år då antalet ansökta handlingar ligger under medeltalet. I slutet av 2025 var priset för ett pass 55 euro och för ett identitetskort 65 euro. Som helhet granskat är höjningarna alltså mycket måttliga i förhållande till den nuvarande prisnivån på handlingarna.

Patent- och registerstyrelsen. Enligt propositionen beviljar Patent- och registerstyrelsen uppgifter för personidentifiering av juridiska personer för plånboken. Det är fråga om en ny uppgift som förutsätter införande av en ny teknisk funktion. I praktiken handlar det om en egen självständig tjänst som utnyttjar uppgifterna i basregister via gränssnitt. I praktiken utgör tjänsten ett nytt gränssnitt och användargränssnitt som företrädare för juridiska personer kan använda för att begära identifieringsuppgifter om en person och som identifierar företrädaren och kontrollerar att han eller hon har befogenhet att agera för den juridiska personens räkning. Dessutom förutsätter utvecklingen av tjänsten en funktion med vilken uppgifterna för personidentifiering av den juridiska personen skapas, sparas i Patent- och registerstyrelsens databas och lämnas ut till den sökandes plånbok. Patent- och registerstyrelsen har bedömt att resurskostnaderna för utveckling av tjänsten är 540 000 euro och de fortlöpande kostnaderna för upprätthållandet 345 000 euro per år. Där ingår totalt 2 årsverken i anslutning till underhåll av applikationen, produktägande i fråga om identifieringsuppgifterna om den juridiska personen samt stöd för processen.

Utrikesförvaltning. Inte tillnärmelsevis alla utlandsfinländare har finländska bankkoder, mobilcertifikat eller identitetskort med medborgarcertifikat som gör det möjligt att ta i bruk den europeiska digitala identitetsplånboken elektroniskt. Av den anledningen föreslås det i propositionen att en person ska kunna få uppgifter för personidentifiering av en fysisk person och således också en europeisk digital identitetsplånbok genom att besöka en finsk beskickning. I praktiken identifierar den finska beskickningen i dessa situationer den person som ansöker om identifieringsuppgifter för en fysisk person, men också i dessa situationer är det Myndigheten för digitalisering och befolkningsdata som utfärdar personens identifieringsuppgifter. Det är fråga om en mycket begränsad och till karaktären assisterande uppgift i processen för utfärdande av identifieringsuppgifter för fysiska personer. Identifiering vid beskickningarna för att få identifieringsuppgifter för personer ökar emellertid i någon mån arbetsmängden inom kundservice vid de finska beskickningarna i synnerhet i inledningsskedet av ibruktagnandet av plånboken och identifieringsuppgifterna för person.

Preliminärt bedöms det att antalet besök vid beskickningarna för att få identifieringsuppgifter för person är cirka 10 000 under det första ibruktagningsåret. Det kan bedömas att ett besök för att sköta ett enskilt kundärendet vid en beskickning tar i medeltal cirka 15 minuter. Därmed blir den årliga arbetsmängden under det första ibruktagningsåret uppskattningsvis cirka 2 500 timmar och den årliga kostnaden cirka 70 000 euro. Enligt artikel 5a.13 i den reviderade eIDAS-förordningen ska beviljandet, användningen och återkallandet av europeiska digitala identitetsplånböcker vara avgiftsfritt för alla fysiska personer. Utfärdandet av identifieringsuppgifter för fysiska personer är i praktiken en oskiljbar del av beviljandet och ibruktagnandet av den europeiska digitala identitetsplånboken, eftersom uppgifterna för personidentifiering utgör grunden för den elektroniska identifiering som sker med hjälp av plånboken, vilket är en av de obligatoriska egenskaperna i den europeiska digitala identitetsplånboken. Därmed är det inte möjligt att ta ut en avgift av personer för utfärdande av deras identifieringsuppgifter. Den kostnad som orsakas av ökad kundservice ska således täckas

i första hand med utrikesministeriets anslag för omkostnader inom ramen för den gällande anslagsramen.

Besöken koncentreras särskilt till verksamhetsområden för de beskickningar där det finns mycket utlandsfinländare. I fortsättningen kan antalet besök bedömas bli något jämnare, men det är ändå svårt att bedöma det exakta antalet besök i framtiden. Dessutom kan antalet kundkontakter variera från ett år till ett annat, varför det i det här skedet är svårt att framföra någon genomsnittlig uppskattning om antalet kontakter per år. I fortsättningen gör den europeiska digitala identitetsplånboken det möjligt också för utlandsfinländare att använda en identifieringsmetod för stark autentisering i tjänster inom den offentliga förvaltningen. Dessutom möjliggör den elektroniskt ibruktagande av e-legitimation. Ibruktagandet av plånboken minskar i fortsättningen efterfrågan på de tjänster inom offentlig förvaltning som beskickningarna tillhandahåller, om det är möjligt att få samma tjänster genom att elektroniskt vara i direktkontakt med den behöriga finländska myndigheten. Ibruktagandet av e-legitimation med hjälp av plånboken minskar i fortsättningen också efterfrågan på identitetskort på beskickningarna.

Statens ämbetsverk på Åland. Myndigheten för digitalisering och befolkningsdata har inga servicepunkter på Åland, där personer kan ansöka om identifieringsuppgifter för fysiska personer och således ta plånboken i bruk under ett besök. Av den anledningen föreslås det i propositionen att en person ska kunna få uppgifter för personidentifiering av en fysisk person och således också en europeisk digital identitetsplånbok i bruk genom att besöka Statens ämbetsverk på Åland. Motsvarande uppgift föreslås också för de finska beskickningarna. En tjänsteperson på Statens ämbetsverk på Åland identifierar då sökanden, men Myndigheten för digitalisering och befolkningsdata är också i dessa situationer den som beviljar uppgifter för personidentifiering av den fysiska personen. Det är fråga om en noggrant avgränsad och till karaktären assisterande uppgift som ingår i beviljandet av identifieringsuppgifter för fysiska personer. Den nya uppgiften bedöms emellertid i någon mån öka arbetsmängden för Statens ämbetsverk på Åland, i synnerhet i inledningsskedet när plånboken och identifieringsuppgifterna för fysiska personer tas i bruk.

Enligt en preliminär bedömning kommer antalet ansökningar om identifieringsuppgifter för fysiska personer vid besök hos Statens ämbetsverk på Åland att förbli rätt måttligt. Konsekvenserna bedöms vara motsvarande som för de finska beskickningarna. Vid besök hos Statens ämbetsverk på Åland kan det bedömas ta cirka 15 minuter att sköta ett enskilt ibruktagande, varvid konsekvenserna för personalen under det år då plånböckerna tas i bruk inte förväntas vara betydande. Den viktigaste konsekvensen med avseende på personalen gäller att utbilda personalen vid Statens ämbetsverk på Åland att använda Myndigheten för digitalisering och befolkningsdatas tjänstemannaportal, med vilken beviljandet av identifieringsuppgifter för fysiska personer kommer att ske. På samma sätt som i beskrivningen ovan av konsekvenserna för de finska beskickningarna ska ibruktagandet av plånboken enligt den reviderade eIDAS-förordningen vara avgiftsfritt. Därmed är det inte heller möjligt att ta ut en avgift för beviljande av uppgifter för personidentifiering. Kostnaderna för ökad kundbetjäning och nya skyldigheter ska således täckas med ämbetsverkets egna verksamhetsanslag.

Rättsregistercentralen Enligt förslaget ansvarar Rättsregistercentralen för genomförandet av administrativa påföljdsavgifter. På grund av verkställighetsuppgifternas karaktär förutsätter skötseln av uppgiften inte, till skillnad från hur det är för andra centrala myndigheter, att Rättsregistercentralen skaffar sakkunskap av en ny typ, utan det är endast fråga om att mängden verkställighetsuppgifter eventuellt ökar. Utgångsläget i tillsynen över betrodda tjänster är handledning och rådgivning och det väntas inte att någon betydande mängd administrativa påföljdsavgifter påförs med stöd av den föreslagna eIDAS-lagen. Rättsregistercentralen

ansvarar i nuläget för verkställandet av mer än 60 olika administrativa påföljder av straffnatur. Trots detta ökar det nya påföljdsslaget allmänt taget Rättsregistercentralens behov av personarbete exempelvis på grund av kundkontakter och utredning av felsituationer i anslutning till verkställande. Vid beredningen av propositionen bedömdes det ändå att påföljdsavgifter som ska påföras leverantörer av betrodda tjänster orsakar endast ett litet behov av tilläggsresurser hos Rättsregistercentralen.

Dataombudsmannen. Enligt den reviderade eIDAS-förordningen kan man med hjälp av den europeiska digitala identitetsplånboken rapportera misstänkta begäranden om uppgifter från förlitande parter direkt till Dataombudsmannen. Vid beredningen av propositionen bedömdes det emellertid att konsekvenserna för Dataombudsmannen åtminstone i initialskedet kommer att vara små, eftersom de förlitande parterna huvudsakligen kommer att vara aktörer inom den offentliga förvaltningen. Aktörer inom den offentliga förvaltningen kan bedömas i regel agera i enlighet med dataskyddsregleringen när de begär uppgifter av personer. Uppgifter som myndigheter behandlar är typiskt reglerade i lag eller annars relativt noggrant fastställda. Antalet parter som förlitar sig på plånboken kan bedömas öka fram till utgången av 2027, då också aktörer inom den privata sektorn i vissa situationer är skyldiga att godkänna identifieringar med plånboken i sina tjänster. Det är möjligt att antalet anmälningar till Dataombudsmannen då ökar en aning. Antalet misstänkta begäranden om uppgifter som rapporteras till Dataombudsmannen är emellertid beroende av i hur stor omfattning den europeiska digitala identitetsplånboken tas i bruk.

4.2.3.6 Konsekvenser för informationshanteringen

De förslag som hänför sig till genomförandet av den reviderade eIDAS-förordningen har konsekvenser för informationshanteringen vid Myndigheten för digitalisering och befolkningsdata. Myndigheten för digitalisering och befolkningsdata lämnade under beredningen i februari 2025 en begäran om yttrande till finansministeriet i enlighet med 9 § i lagen om informationshantering inom den offentliga förvaltningen (906/2019). I begäran om yttrande och i finansministeriets yttrande bedöms konsekvenserna för informationshanteringen av den planerade revideringen.

Den föreslagna regleringen medför nya lagstadgade uppgifter för Myndigheten för digitalisering och befolkningsdata och behov av nya informationssystem och datalager i anslutning till fullgörandet av uppgifterna samt behov av att utveckla befintliga tjänster. Avsikten är att Myndigheten för digitalisering och befolkningsdata i fortsättningen producerar den europeiska digitala identitetsplånboken med anknytande system och tjänster. Myndigheten för digitalisering och befolkningsdata ska också vara leverantörer av betrodda tjänster i fråga om flera tjänster. Enligt förslaget ska Myndigheten för digitalisering och befolkningsdata tillhandahålla också en tjänst för så kallad identitetsmatchning (se närmare om vad skyldigheten innehåller i avsnitt 2.2). Enligt förslagen till lagstiftning i propositionen ska Myndigheten för digitalisering och befolkningsdata producera tjänsten som centraliserad tjänst för e-tjänsterna inom den offentliga förvaltningen.

Avsikten är att de europeiska digitala identitetsplånböckerna ska fungera som mobila applikationer. Med deras hjälp kan medborgarna enkelt hantera och använda sina egna uppgifter i olika situationer i vardagen. Som en samlad konsekvens av regleringen i anslutning till den reviderade eIDAS-förordningen och genomförandet av den uppstår nya handlingsmodeller, med vilka personuppgifter och elektroniska attributsintyg med uppgifter visas när ärenden sköts hos myndigheterna och även annars i tjänster i samhället. I fortsättningen kan en person exempelvis styrka sin identitet på ett sätt som är jämförbart med pass eller identitetskort med den e-legitimation som ingår i plånboken. Centralt i den nya handlingsmodellen är att den som

använder plånboken själv kan visa information som den innehar för andra myndigheter och aktörer inom den privata sektorn, för en annan plånbok eller någon annan som använder plånboken. Det är således fråga om en ny handlingsmodell när det gäller sättet att lämna ut uppgifter, där uppgifterna kommer från personen själv. Genom att modellen utvecklas kan den stödja automatiserat avgörandeförfarande i framtiden. När det gäller handlingsmodellen är det centrala att uppgifterna är försedda med digital underskrift eller stämpel och att integriteten, aktualiteten och giltigheten har säkerställts mot den ursprungliga källan. På så sätt kan den som utnyttjar uppgifterna vara viss om att de är riktiga också när de erhålls direkt av den användare som de gäller. I den här nya modellen är det inte nödvändigt att kontrollera uppgiften direkt mot den ursprungliga källan t.ex. på grund av lagstadgad rätt att få information

I och med den nya handlingsmodellen har användare av plånböcker ett större ansvar för att de egna personuppgifterna används på ett informationssäkert sätt efter att han eller hon har fått uppgifterna i bruk i sin plånbok. Kontrollen över transaktioner för utlämnande av uppgifter övergår från den ursprungliga uppgiftskällan till användaren själv. Därför måste det göras möjligt för användare att veta exakt vilka uppgifter som lämnas ut, till vem de lämnas ut och när utlämnandet har skett. När en person lämnar ut uppgifter måste han eller hon dessutom kunna försäkra sig om att uppgifterna endast används för det avgränsade användningsändamålet. I enlighet med kraven i den reviderade eIDAS-förordningen tillhandahåller Myndigheten för digitalisering och befolkningsdata medborgarna en vy för kontroll av de egna logguppgifterna. Med tanke på myndighetens informationshantering innehas de logguppgifter som behövs för eventuell fortsatt behandling av användaren. Den som beviljar en uppgift eller tillhandahåller en europeisk digital identitetsplånbok kan inte spåra användningen av plånboken, utan logguppgifterna över transaktioner innehas av användaren själv och finns i transaktionsuppgifter i de enskilda e-tjänsterna.

Även om den reviderade eIDAS-förordningen och den föreslagna regleringen vid användning av plånboken stöder sig på en identitet som är under användarens egen kontroll och personen bättre än tidigare kan besluta om hanteringen och användningen av sina egna uppgifter, kan det ändå uppstå situationer där uppgifter som användaren visar genom plånboken inte räcker till för att inleda kommunikationen i en e-tjänst. Det är i regel en uppgift för den som tillhandahåller e-tjänsten att ange de uppgifter som behövs för kommunikationen. Sådana krav är alltså ofta e-tjänstspecifika och avgörs utifrån behoven och processerna i en enskild e-tjänst. Om en användare exempelvis inte kommer vidare till en e-tjänst på grund av att någon viss uppgift saknas informerar plånboken användaren om eventuella uppgifter som saknas.

Förslaget innehåller register med personuppgifter som kommer att ingå i personuppgiftsansvaret vid Myndigheten för digitalisering och befolkningsdata, såsom ett register för identifieringsuppgifter över personer och ett register för bevis över plånboksenheter, som innehåller uppgifter om plånböcker som tagits i bruk. Den föreslagna reformen ändrar inte i regel personuppgiftsansvaret för register som innehåller personuppgifter. Myndigheten för digitalisering och befolkningsdata ansvarar som personuppgiftsansvarig för adekvat administration av uppgifter som lagras i register som uppkommer hos myndigheten på grund av att den tillhandahåller plånboken och i de anknytande systemen och tjänsterna. För riktigheten i och behandlingen i den autentiska källan av uppgifter som tillhandahålls via plånboken ansvarar för sin del den personuppgiftsansvarige för den aktuella informationsresursen. Den myndighet som tar emot uppgifter ansvarar för behandlingen av dem i sin egen ärendehantering. Myndigheten för digitalisering och befolkningsdatas status som personuppgiftsansvarig och myndighetens relation till användarens egen kontroll över uppgifterna i plånboken beskrivs närmare i specialmotiveringen till det första lagförslaget.

4.2.3.7 Säkerheten i elektronisk kommunikation

Vid beredningen av propositionen bedömdes det att den reviderade eIDAS-förordningen och genomförandet av den tillsammans kan minska missbruket av personuppgifter, eftersom de krav och handlingsprinciper som gäller europeiska digitala identitetsplånböcker gör det svårare att kombinera personuppgifter och att utföra profilering som gäller personer. Plånböckerna möjliggör exempelvis utnyttjande av pseudonyma identifieringskoder. Med detta avses att plånboken bildar exempelvis en identifieringskod för personen som är specifik för en viss e-tjänst och som inte innehåller uppgifter som är kopplade till användaren. Kommunikation med pseudonymer ska vara möjlig i situationer som inte förutsätter att användaren identifieras. Med hjälp av pseudonymer kan man undvika exempelvis situationer där ett dataintrång i en e-tjänst leder till att personbeteckningar i stor omfattning hamnar i fel händer. Genom användning av pseudonymer kan man alltså eventuellt avsevärt minska identitetsstöld och minska effektiviteten i nätbrottslingars informationsfiske. I och med de förfaranden som plånböckerna erbjuder för att förbättra identitetsskyddet bedöms det också bli enklare att ingripa i situationer med missbruk.

Certifiering av europeiska digitala identitetsplånböcker samt anknytande bedömningar av överensstämmelsen för elektroniska betrodda tjänster, såsom elektroniska attributsintyg och elektroniska underskrifter skapar i regel en mycket tillförlitlig och säker omvärld för plånböckerna och anknytande tjänster (se närmare om kraven på kvalificerade betrodda tjänster i avsnitt 3.1.2). I och med efterlevnaden av kraven i de certifieringsordningar som gäller plånböckerna och tillsynen över plånböckerna och de aktörer som tillhandahåller dem erbjuder plånböckerna också i sig en ytterst säker plattform för olika personuppgifter och elektroniska attributsintyg. I propositionen föreslås som regel att e-legitimation som förutsätter särskild tillförlitlighet och säkerhet tillhandahålls i plånboken som kvalificerat elektroniskt attributsintyg. Detta främjar för sin del också tillhandahållandet av andra elektroniska attributsintyg som kräver särskild säkerhet för plånboken i framtiden.

Till plånböckerna och de anknytande tjänsterna kan anslutas också betrodda tjänster av icke-kvalificerade leverantörer av betrodda tjänster t.ex. när det gäller elektroniska attributsintyg. Även om dessa aktörer inte berörs av de regelbundna bedömningarna av överensstämmelse omfattas de ändå som leverantörer av betrodda tjänster av vissa krav som gäller informationssäkerhet som grundar sig på regleringen om cybersäkerhet. Över huvud taget kan man med hjälp av plånböckerna uppnå bättre informationssäkerhet och tillförlitlighet i e-tjänster, då en större del än tidigare av identifieringen grundar sig på en plånbok som fungerar på tillitsnivån hög och elektroniska underskrifter i stället för på en grundläggande eller avancerad säkerhetsnivå görs som kvalificerade elektroniska underskrifter.

Ett viktigt mål för de ändringar som främjar säkerheten i nationell stark autentisering är att främja säkerheten och tillförlitligheten i elektronisk identifiering genom bättre möjligheter för leverantörer av identifieringstjänster att reagera effektivt i störningssituationer samt att förhindra användningen av olovligt ibruktaga elektroniska identifieringsverktyg. Bestämmelser om skyldigheten för den som tillhandahåller ett nytt identifieringsverktyg att anmäla sammankopplad inledande identifiering underlättar utredningen av situationer med missbruk, när olovliga inledande identifieringar kan spåras omedelbart. Den föreslagna anmälningsskyldigheten gör det också möjligt att ta ut rätt pris för inledande identifiering och förtydligar ansvarsfördelningen enligt 17 § i autentiseringslagen i felsituationer. Till denna del förtydligar skyldigheten att förmedla information om sammankopplad inledande identifiering också tillämpningen av den gällande lagen.

Den skyldighet som i propositionen föreslås för leverantörer av identifieringsverktyg i polisens informationssystem säkerställa uppgiften om en handlings giltighet förbättrar säkerheten vid beviljandet av identifieringsverktyg. När en handlings giltighet i fortsättningen alltid kontrolleras i polisens informationssystem kan ett indraget identitetsbevis inte längre användas i samband med inledande identifiering.

4.2.3.8 Informationssamhället

Den reviderade eIDAS-förordningen och förslagen i anslutning till genomförandet kan ha konsekvenser för utvecklingen av den grundläggande digitala infrastrukturen i samhället och de europeiska digitala identitetsplånböckerna kan i framtiden utgöra en betydande del av den. Plånböckerna ändrar på sätten att dela information, när uppgifterna i regel inte längre hämtas ur register via gränssnitt i samband med skötseln av ärenden utan uppgifterna lämnas ut direkt från användare som har dem sin besittning. Viktigt med tanke på de tjänster som uppstår kring plånböckerna och den övriga relaterade omvärlden är att det uppkommer tillräckligt med olika aktörer och tjänstetillhandahållare för att rollerna inte ska komma att vila på enskilda aktörers axlar. Av denna anledning föreslås det i propositionen att bara vissa uppgifter anvisas namngivna aktörer, såsom tillsynsuppgiften i anslutning till plånböckerna anvisas Transport- och kommunikationsverket. I propositionen begränsas emellertid inte andra aktörers möjligheter att verka som tillhandahållare av europeiska digitala identitetsplånböcker vid sidan av Myndigheten för digitalisering och befolkningsdata och propositionen innehåller t.ex. inte något förslag om en exaktare definition av vilka aktörer som kan erbjuda olika elektroniska intyg för plånboken.

Det informationsutbyte som grundar sig på plånböckerna ändrar inte på något betydande sätt den hantering av registeruppgifter som äger rum i det ursprungliga registret. I vissa situationer kan det förutsättas effektivare hantering av informationens livscykel, för att också de elektroniska intyg som erbjuds plånboken, såsom fullmakter, ska kunna hanteras effektivt under livscykeln. Utmaningen i anslutning till livscykelhanteringen kan emellertid hanteras också genom att elektroniska attributsintyg utfärdas så att giltighetstiden är kort (t.ex. något antal timmar). Detta gör det möjligt att utnyttja dem i kommunikationssituationer, men förutsätter inte att det genomförs komplicerade lösningar för hantering av informationens livscykel i det ursprungliga registret.

Plånböckerna kan förbättra också kriställigheten i samhället när elektronisk identifiering, underskrift och behandling av bevis kan få stöd av på lösningar som inte är beroende av centraliserade komponenter. Utnyttjandet av plånböcker är emellertid förknippat med vissa centraliserade roller, såsom registret över förlitande parter, och i fråga om dem måste användbarheten säkerställas för att det ska vara möjligt att använda dem också vid situationer med olika slag av avvikelser.

Med hjälp av plånboken kan olika uppgifter och intyg sannolikt delas effektivare än i nuläget, när en större del av tjänsterna kan produceras digitalt. I fortsättningen kan t.ex. köer på fysiska serviceställen undvikas om intygen kan delas elektroniskt eller om verktyg för elektronisk underskrift på kvalificerad nivå gör det möjligt för aktörer inom den offentliga förvaltningen att vara mindre beroende av handlingar som undertecknats för hand och en större del av handlingarna kan skrivas under elektroniskt. T.ex. den föreslagna e-legitimationen kan bedömas förkorta den tid som behövs för att identifiera en person. Jämfört med traditionella fysiska handlingar kan kontrollen nästan i sin helhet inriktas på att säkerställa att personen i fråga är den vars uppgifter förmedlas när e-legitimationen används. När det gäller traditionella fysiska handlingar ska vid man vid en kontroll alltid beakta möjligheten att den handling som visas är förfalskad eller att uppgifterna i den har manipulerats på något annat sätt. När det är fråga om

e-legitimation finns inte någon sådan fara, eftersom det inte går att avläsa uppgifterna om det inte är fråga om aktuella och tillförlitliga uppgifter.

Dessutom behöver man i framtiden eventuellt färre avtal som möjliggör informationsutbyte, när en större del av de uppgifter som är kopplade till personer kan delas vidare till e-tjänster inom den privata och den offentliga sektorn direkt från plånböckerna. Plånböckerna kommer emellertid inte att vara det enda sättet för elektronisk identifiering eller delning av personrelaterade uppgifter. E-tjänsterna behöver fortfarande göra sin egen bedömning av i vilka situationer plånböckerna är det mest ändamålsenliga sättet för informationsutbyte. I varje fall kommer en omfattande användning av plånböckerna sannolikt att avancera stegvis och baserad på användarnas frivilliga användning.

4.2.3.9 Dataskydd

Den reviderade eIDAS-förordningen och genomförandet av den kan bedömas främja dataskyddet i synnerhet på grund av den teknik av ny typ som utnyttjas i de europeiska digitala identitetsplånböckerna. Plånböckerna möjliggör exempelvis selektivt visande av uppgifter, varvid personer själva bättre kan besluta vilka uppgifter de delar med olika e-tjänster. Om ärendet t.ex. kräver uppgift om personens födelsedatum, kan det visas med hjälp av e-legitimationen på ett sådant sätt att bara uppgiften om personens födelsedatum och en bild av personens ansikte visas i e-tjänsten. I nuläget utlämnas i motsvarande situation där t.ex. identitetskort används oundvikligen bl.a. personens alla förnamn, efternamnet samt andra uppgifter till e-tjänsten som inte är nödvändiga i situationen. Selektivt visande av uppgifter främjar principen om minimering av data enligt den allmänna dataförordningen och bidrar till att till tjänsterna utlämnas endast data som faktiskt behövs.

Dessutom förbättrar pseudonyma identifieringskoder integritetsskyddet i situationer där e-tjänsterna inte förutsätts kräva stark autentisering av användaren. Också de övriga nya tekniker som plånböckerna utnyttjar, såsom s.k. nollkunskapsbevis, kan förbättra integritetsskyddet. Sådana kan i praktiken utnyttjas t.ex. i situationer där e-tjänsterna inte behöver datainnehållet i det egentliga elektroniska intyget, utan det för tjänsterna räcker med den information som härleds ur attributet. I praktiken kan det här exempelvis i anslutning till styrkande av ålder med e-legitimation innebära att bara den uppgiften att personen är över 18 år lämnas ut, men inte uppgift om personens födelsedatum eller om hur gammal personen är. Plånböckerna erbjuder också användarna sådana egenskaper för användarna som bättre än tidigare kan främja uppfyllelsen av målen enligt den allmänna dataskyddsförordningen. Med hjälp av plånboken kan användaren utnyttja sin rätt enligt den allmänna dataskyddsförordningen att begära att en e-tjänst raderar hans eller hennes personuppgifter. Dessutom kan användaren med hjälp av plånboken meddela dataombudsmannen om misstänkta begäranden om uppgifter som kommit från en e-tjänst.

I och med plånböckerna är användarna själva allt mer centrala i fråga om användningen av de egna personuppgifterna och kan bättre besluta om användningen och delandet av sina egna uppgifter. Samtidigt medför detta också mera ansvar för användarna för användningen av de egna personuppgifterna. Plånböckerna är också mer allmänt uppbyggda kring en sådan metod för informationsutbyte där användarna själva ger sitt uttryckliga samtycke till att uppgifter lämnas till e-tjänster. Detta skapar mer transparens för användaren i hur uppgifterna om honom eller henne används i de olika e-tjänsterna och vilka uppgifter en viss e-tjänst över huvud taget behöver för att tillhandahålla sina tjänster. Tillvägagångssättet avviker från den nuvarande metoden för informationsutbyte där utbytet sker främst mellan olika register på ett sätt som är osynligt för användaren. Användaren är emellertid i fråga om visandet av sina egna uppgifter ansvarig också då de säkerhetsmekanismer som plånboken erbjuder anger att uppgifterna inte

bör lämnas ut. Varningar av den här typen är endast informativa för användaren och användaren kan, om han eller hon vill, lämna ut uppgifter på eget beslut trots varningarna.

Aktörer som tillhandahåller plånböckerna och anknyttande tjänster eller som utför relaterade uppgifter förutsätts bedöma dataskyddskonsekvenserna.

Avsikten med de säkerhetsfrämjande ändringarna i den nationella starka autentiseringen är särskilt att trygga användarna genom att förhindra att identifieringsverktygen hamnar i fel händer och att underlätta utredningen av misstankar om missbruk. Således anses de föreslagna ändringarna ha effekter som förbättrar skyddet för personuppgifter.

4.2.4 Gränsöverskridande konsekvenser

4.2.4.1 Förordningen om ett interoperabelt Europa och interoperabilitetsbedömning

Europaparlamentets och rådets förordning om åtgärder för en hög nivå av interoperabilitet inom den offentliga sektorn i hela unionen (nedan *förordningen om ett interoperabelt Europa*) förutsätter i artikel 3.1 att en unionsentitet eller en offentlig myndighet, innan ett beslut fattas om nya eller väsentligt ändrade bindande krav, ska utföra en interoperabilitetsbedömning. Med bindande krav avses enligt artikel 2.15 skyldighet, förbud, villkor, kriterium eller gräns av rättslig, organisatorisk, semantisk eller teknisk art som fastställs av en unionsentitet eller en offentlig myndighet avseende en eller flera transeuropeiska digitala offentliga tjänster och som har inverkan på gränsöverskridande interoperabilitet. Enligt skäl 18 i förordningen inbegriper de bindande kraven skyldigheter, förbud, villkor, kriterier eller begränsningar av rättslig, organisatorisk, semantisk eller teknisk art inom ramen för lagar, förordningar, administrativa bestämmelser, kontrakt, anbudsinfördrar eller andra officiella handlingar. Bindande krav påverkar hur transeuropeiska digitala offentliga tjänster och de nätverks- och informationssystem som används för att tillhandahålla dem utformas, upphandlas, utvecklas och genomförs, vilket påverkar in- och utgående dataflöden för dessa tjänster.

När ett förslag om nya bindande krav ingår i EU-reglering görs interoperabilitetsbedömningen av Europeiska kommissionen. Om ett förslag om nya bindande krav ingår i nationell lagstiftning, såsom i nationell lagstiftning som kompletterar EU-regleringen, görs interoperabilitetsbedömningen som en del av konsekvensbedömningen av regeringens proposition av det ministerium som bereder den kompletterande nationella regleringen. Interoperabilitetsbedömningen görs av myndigheten om den på eget beslut ställer krav på interoperabiliteten, dvs. på hur informationsutbytet genomförs. Förordningen om ett interoperabelt Europa har tillämpats sedan den 12 januari 2025. Den tillämpas inte retroaktivt på beslut som fattats före den 12 januari 2025.

I bestämmelserna i den reviderade eIDAS-förordningen om en europeisk digital identitetsplånbok kan det anses vara fråga om sådana bindande krav som avses i förordningen om ett interoperabelt Europa och om vilka en interoperabilitetsbedömning ska göras. Exempelvis i artikel 5 a i den reviderade eIDAS-förordningen anges flera olika krav och skyldigheter och begränsningar som gäller plånbokens funktion. Plånboken är en tjänst som är avsedd att användas i gränsöverskridande e-tjänster samt för hantering av användarens uppgifter och utlämnande av uppgifterna från plånboken. Den reviderade eIDAS-förordningen trädde emellertid i kraft den 20 maj 2024, dvs. innan förordningen om ett interoperabelt Europa började tillämpas. Europeiska kommissionen har därmed inte gjort någon interoperabilitetsbedömning av eIDAS-förordningen.

Vid beredningen av propositionen har det bedömts att en interoperabilitetsbedömning inte heller behöver göras på grund av den nationella reglering som kompletterar den reviderade eIDAS-förordningen. Den reviderade eIDAS-förordningen innehåller mycket begränsat med nationellt handlingsutrymme (se närmare i avsnitt 2.2) och den nationella kompletterande regleringen består främst av anvisande av skyldigheterna och uppgifterna enligt den reviderade eIDAS-förordningen till olika aktörer. I den nationella regleringen ställs inga krav på plånboken som avviker från eller kompletterar den reviderade eIDAS-förordningen och fastställs inte något närmare om det tekniska genomförandet av plånboken. Vid beredningen av propositionen bedömdes det alltså att den nationella kompletterande regleringen inte innehåller några beslut om nya eller väsentligt ändrade bindande krav på det sätt som avses i förordningen om ett interoperabelt Europa. Vid beredningen av propositionen identifierade man emellertid att det i samband med inrättandet av en nationell certifieringsordning ska bedömas särskilt om en interoperabilitetsbedömning måste göras i fråga om certifieringsordningen. I propositionen föreslås det att ägaren till den nationella certifieringsordningen i Finland är Transport- och kommunikationsverket. Närmare bestämmelser om den nationella certifieringsordningen finns i förordningen om certifiering av plånböcker.

4.2.4.2 EU-förordningen om en gemensam digital ingång

Europaparlamentets och rådets förordning (EU) 2018/1724 av den 2 oktober 2018 om inrättande av en gemensam digital ingång för tillhandahållande av information, förfaranden samt hjälp- och problemlösningstjänster och om ändring av förordning (EU) nr 1024/2012 (EU-förordningen om en gemensam digital ingång, nedan *SDG-förordningen*) förutsätter att medlemsstaterna genomför det så kallade OOTS-systemet (Once-Only Technical System). I och med SDG-förordningen kan medlemsstaternas elektroniska tjänster inom den offentliga förvaltningen begära bevismaterial från andra medlemsstaters officiella register, när användaren har identifierats och gett sitt samtycke till att uppgifterna hämtas. Således är det både i OOTS-systemet och i europeiska digitala identitetsplånböcker som är förenliga med den reviderade eIDAS-förordningen fråga om att information överförs och visas gränsöverskridande mellan medlemsstaterna i EU-området. SDG-förordningen och den reviderade eIDAS-förordningen ställer emellertid inte motstridiga eller överlappande krav på medlemsstaterna, utan de kompletterar varandra.

Kommissionen och medlemsstaterna har främjat synergier mellan europeiska digitala identitetsplånböcker enligt eIDAS-förordningen och OOTS-systemet enligt SDG-förordningen i en separat arbetsgrupp. Arbetsgruppens arbete har resulterat i en rad rekommendationer med målet att främja interoperabiliteten mellan plånböckerna och OOTS-systemet. En dialog om det nationella genomförandet av dessa rekommendationer har förts också i Finland. Den viktigaste synergien är förknippad med identifieringen av användare i OOTS-systemet med hjälp av gränsöverskridande elektroniska identifieringsverktyg som har notifierats enligt eIDAS-förordningen. Ett annat viktigt område för interoperabilitet gäller de autentiska källor som avses i den reviderade eIDAS-förordningen. Uppgifter i källorna kan erbjudas som elektroniska attributsintyg i plånboken som användaren kan hantera, men de kan också utbytas via OOTS-systemet direkt mellan myndigheter. OOTS-systemet kan fungera som tekniskt gränssnitt till autentiska källor om den leverantör av betrodda tjänster som tillhandahåller elektroniska attributsintyg är en aktör inom den offentliga sektorn. Dessutom möjliggör OOTS användning av enhetliga semantiska informationsmodeller inom hela EU.

4.2.4.3 Gränsöverskridande konsekvenser för konsumenterna

Funktionerna i de europeiska digitala identitetsplånböckerna är tillgängliga för konsumenterna i hela EU. Införandet av plånboken främjar således gränsöverskridande kommunikation. När

det gäller elektronisk identifiering har det i Finland hittills huvudsakligen funnits tillgång till identifieringsverktyg som uppfyller kraven på tillitsnivå väsentlig (t.ex. bankkoder, mobilcertifikat), eftersom de nationella kraven på stark autentisering har harmoniserats med kraven i fråga. I och med den europeiska digitala identitetsplånboken får konsumenterna vid sidan av det medborgarcertifikat som Myndigheten för digitalisering och befolkningsdata tillhandahåller tillgång till ett annat elektroniskt identifieringsverktyg som uppfyller kraven på tillitsnivå hög och som godkänns för gränsöverskridande bruk. Detta kan framför allt göra det lättare att använd andra medlemsstaters e-tjänster, eftersom de i hög grad förutsätter användning av identifieringsverktyg som uppfyller tillitsnivån hög, och tillitsnivån väsentlig inte är tillräcklig för att de ska kunna användas.

4.2.4.4 Gränsöverskridande konsekvenser för företagen

Kommissionen lade den 19 november 2025, medan propositionen var under beredning, fram ett förslag till Europaparlamentets och rådets förordning om införande av europeiska företagsplånböcker (COM(2025) 838 final). Förslaget handlar om gemensam lagstiftning om europeiska företagsplånböcker. Med hjälp av företagsplånboken kan företagen sköta ärenden i tjänster inom den offentliga sektorn gränsöverskridande inom EU samt kommunicera också med varandra. Kommissionens förslag har konsekvenser också för den reviderade eIDAS-förordningen, eftersom den europeiska digitala identitetsplånboken enligt förslaget i fortsättningen ska kunna användas endast av fysiska personer (inkl. olika situationer där dessa agerar som företrädare). Den europeiska företagsplånboken ska således införas vid sidan av den europeiska digitala identitetsplånboken. Vid beredningen av propositionen bedömdes att de gränsöverskridande konsekvenserna av den reviderade eIDAS-förordningen på grund av initiativet om företagsplånböcker sannolikt koncentreras till situationer där företagen är förlitande parter.

Företagen kan som förlitande parter utnyttja plånboken för stark autentisering och för utnyttjande av uppgifter som ingår i elektroniska attributsintyg i sin egna e-tjänster. Eftersom det är fråga om en lösning på EU-nivå kan den europeiska digitala identitetsplånboken göra det möjligt för företag att utvidga sin kundbas när det är möjligt att enkelt sköta ärenden elektroniskt från andra medlemsstater i företagets tjänster. Detta kan också effektivisera företagets verksamhet på den inre marknaden. Trots att plånböckerna utvecklas allmäneuropeiskt på gemensamma tekniska standarder och protokoll kan det samtidigt finnas skillnader mellan de olika medlemsstaterna t.ex. i fråga om uppgiftsinnehållet i en persons identifieringsuppgifter eller i elektroniska attributsintyg. Också förfarandena t.ex. vid registrering av förlitande parter kan vara olika i olika medlemsstater. Av denna anledning kan företag som verkar i flera medlemsstater bli tvungna att utarbeta skraddarsydda lösningar för de olika medlemsstaterna, vilket kan öka deras kostnader.

5 Alternativa handlingsvägar

5.1 Handlingsalternativen och deras konsekvenser

5.1.1 Tillhandahållande av den europeiska digitala identitetsplånboken i Finland

I Finland grundar sig stark autentisering i nuläget i stor utsträckning på identifieringsverktyg som tillhandahålls av leverantörer av identifieringsverktyg inom den privata sektorn och den offentliga sektorns roll på marknaden är mindre. Den reviderade eIDAS-förordningen gör det möjligt att den europeiska digitala identitetsplånboken tillhandahålls av aktörer inom den offentliga eller den privata sektorn. Av denna anledning ansågs det vid beredningen viktigt att utreda och bedöma om någon av de nuvarande aktörerna kan tillhandahålla också en europeisk

digital identitetsplånbok i Finland. Som stöd för bedömningen lät finansministeriet göra en marknadsundersökning vid årsskiftet 2023–2024 för att kartlägga kompetensen hos de tillhandahållare av centrala betrodda tjänster och identifieringstjänster som för närvarande finns på marknaden att tillhandahålla en plånbok i Finland som uppfyller kraven i den reviderade eIDAS-förordningen. Marknadsundersökningen avgränsades till att gälla nationella aktörer samt aktörer i EU- och EES-länderna med fokus på nordeuropeiska aktörer.

De aktörer som deltog i marknadsundersökningen var i allmänhet intresserade av att utveckla plånböckerna på lång sikt, men vid tidpunkten för undersökningen hade inga beslut fattats om att inleda arbete med att utveckla en europeisk digital identitetsplånbok. Tillhandahållandet av en plånbok ansågs vara förknippat med eventuella utmaningar i synnerhet när det gäller att investeringarna betalar sig tillbaka, modellerna för affärsverksamheten och de tekniska kraven på plånboken. I synnerhet aktörerna inom den privata sektorn verkade inte ha de förutsättningar som behövs för att producera en plånbok som uppfyller kraven i eIDAS-förordningen inom den tidsfrist som förordningen förutsätter. Således bedömdes det vid beredningen att Myndigheten för digitalisering och befolkningsdata har de bästa förutsättningarna för att tillhandahålla en plånbok inom utsatt tid. Aktörerna inom den privata sektorn har emellertid hela tiden möjlighet att utveckla plånböcker enligt eIDAS-förordningen och tillhandahålla dem i Finland vid sidan av den europeiska digitala identitetsplånbok som Myndigheten för digitalisering och befolkningsdata tillhandahåller.

5.1.2 Alternativ att lagstiftning som kompletterar den reviderade eIDAS-förordningen ingår i autentiseringslagen

Autentiseringslagen stiftades 2009 och syftet var att främja utbudet av tjänster för stark autentisering och att skapa grundläggande marknadsregler för tillhandahållandet av tjänster (RP 36/2009 rd). Målen för stiftandet av autentiseringslagen var alltså förknippade i första hand med nationella behov. Den reglering som kompletterar den ursprungliga eIDAS-förordningen passade trots dessa ursprungliga nationella syften ihop med lagens tillämpningsområde, eftersom mängden reglering som kompletterar förordningen är begränsad och till sakinnehållet motsvarar den befintliga regleringen i autentiseringslagen. Också den kompletterande nationella reglering som den reviderade eIDAS-förordningen förutsätter skulle till sakinnehållet kunna passa ihop med autentiseringslagen. Den reviderade eIDAS-förordningen gäller fortfarande gränsöverskridande elektronisk identifiering samt elektroniska betrodda tjänster, och den anknyttande nationella regleringen ingår på det sätt som beskrivs ovan i nuläget i autentiseringslagen.

I den reviderade eIDAS-förordningen föreskrivs det emellertid också om en helhet av ny typ, dvs. om europeiska digitala identitetsplånböcker. Det är fråga om att lägga till något nytt också i tillämpningsområdet för autentiseringslagen. Utöver den kompletterande regleringen om plånböcker finns det ett behov av att utfärda också annan reglering som kompletterar den reviderade eIDAS-förordningen. Vid beredningen av propositionen bedömdes det att den kompletterande nationella reglering som den reviderade eIDAS-förordningen förutsätter som helhet är rätt stor i förhållande till den befintliga regleringen i autentiseringslagen och att lagen blir längre om den nya regleringen läggs till. Den kompletterande regleringen formuleras i punktform, eftersom det centrala innehållet i de olika frågorna regleras i den reviderade eIDAS-förordningen. I den kompletterande regleringen används också terminologi av samma slag som i den gällande autentiseringslagen, men den kompletterande reglering som gäller den reviderade eIDAS-förordningen gäller emellertid delvis endast gränsöverskridande ärenden eller sådant som är kopplat till plånböckerna. Vid beredningen av propositionen bedömdes det att dessa faktorer tillsammans skulle kunna göra regleringen svårtydd för dem som tillämpar lagen och

skapa oklarhet hos tillhandahållare av tjänsterna i fråga om vilka av lagens krav de ska tillämpa i respektive situation.

Även om eIDAS-förordningen och autentiseringslagen fortsättningsvis kontextmässigt står nära varandra är målen i och tillämpningen av eIDAS-förordningen mer inriktade på främjande av elektronisk gränsöverskridande kommunikation mellan EU:s medlemsstater medan målen i autentiseringslagen snarare är inriktade på att utveckla den nationella starka autentiseringen på marknadsvillkor och på att främja säker elektronisk kommunikation. I och med den reviderade eIDAS-förordningen fortsätter den nationella kompletterande regleringen i anslutning till gränsöverskridande mål att öka. Av de ovan beskrivna orsakerna bedömdes det vid beredningen av propositionen att det för den som tillämpar lagen är tydligast att de nationella kraven på stark autentisering och den kompletterande regleringen i anslutning till eIDAS-förordningen i fortsättningen ingår i separata lagar.

5.1.3 Utnyttjande av det nationella handlingsutrymmet

Den reviderade eIDAS-förordningen innehåller nationellt handlingsutrymme när det gäller öppenheten i plånbokens källkod samt möjligheten att göra elektronisk underskrift med hjälp av plånboken avgiftsfri för juridiska personer. Handlingsutrymmet beskrivs närmare i avsnitt 2.2. Vid beredningen av propositionen bedömdes med tanke på helheten ett alternativ där det nationella handlingsutrymmet inte utnyttjas. Detta skulle minska behovet av nationell reglering som kompletterar eIDAS-förordningen och främja målen för förordningen fullt ut. Målet för den öppna källkoden är att främja det samhällseliga förtroendet för plånboken och godkännandet av plånboken bland användarna. Dessutom är avsikten att säkerställa att plånboken fungerar så transparent som möjligt i synnerhet med tanke på behandlingen av personuppgifter. Med öppenheten hos källkoden för plånböckerna vill man också säkerställa deras säkerhet. Avsikten med avgiftsfria elektroniska underskrifter är för sin del att stödja det allmänna målet för plånboken att användarna själva ska kunna hantera sina uppgifter och besluta om användningen av dem.

Finansministeriet ordnade i samband med beredningen av propositionen en rundabordsdiskussion för de centrala intressentgrupperna i fråga om stark autentisering samt elektroniska betrodda tjänster för att utreda om det nationella handlingsutrymmet borde utnyttjas dels i fråga om kraven på öppen källkod i plånboken, dels i fråga om avgiftsfria elektroniska underskrifter. I fråga om båda helheterna var intressentgrupperna eniga om att det nationella handlingsutrymmet bör användas fullt ut.

Det ansågs behövt begränsa kravet på öppen källkod i plånboken i synnerhet med tanke på orsaker som är relaterade till affärsverksamhet, men också säkerhetsaspekter togs upp. En begränsning av kraven på öppen källkod kan möjliggöra att plånboken är en del av en större applikationshelhet. De nuvarande aktörerna kan ha satsat på att utveckla egna applikationer och plånboken kan eventuellt betraktas som en tilläggsföremål som är knuten till dessa andra tjänster. Dessutom sågs en begränsning av kravet på öppen källkod till vissa delar som ett incitament för utvecklingsarbete i anslutning till plånboken, när det inte är nödvändigt att öppet överlåta investeringar som använts för utveckling av källkoden. Under diskussionen konstaterades det emellertid att kravet i förordningen ändå inte innebär att källkoden utan vederlag ska överlåtas för att användas av någon annan aktör. Trots detta ansågs det vara behövt att det nationella handlingsutrymmet utnyttjas och att det främjar intresset för plånboken också bland aktörer inom den privata sektorn.

Att avgiftsfriheten för elektroniska underskrifter begränsas ansågs behövt i synnerhet av den anledningen att tillhandahållandet av elektronisk underskrift i nuläget är verksamhet som

bedrivs på marknadsvillkor och det är viktigt att minimera de negativa konsekvenser som regleringen i den reviderade eIDAS-förordningen eventuellt har för marknaden. Dessutom togs det upp att prissättningen bör vara baserad på marknadsvillkor och inte på reglering. Samtidigt konstaterades det att den elektroniska underskriften består av delområden av många olika slag och att den är avgiftsfri för användaren inte innebär att inkomstflöden inte kan uppstå för den som tillhandahåller tjänsten.

Vid beredningen uppdagades det inga faktorer som gör att man inte under rundabordsdiskussioner skulle kunna främja enhälliga åsikter som intressentgrupperna framför när det gäller att utnyttja det nationella handlingsutrymmet. Således innehåller propositionen förslag till lagstiftning där det nationella handlingsutrymmet utnyttjas.

5.1.4 Den nationella regleringen av plånböcker som enbart används i Finland

En central utgångspunkt för den reviderade eIDAS-förordningen är att det ska gå att sköta ärenden inom hela EU-området med en europeisk digital identitetsplånbok som är förenlig med förordningen. I praktiken är det möjligt att tillhandahålla också en plånbok som kan användas exempelvis bara inom en medlemsstats område. Då skulle det emellertid inte vara fråga om en sådan plånbok som avses i förordningen. Den reviderade eIDAS-förordningen hindrar inte medlemsstaterna från att nationellt reglera sådana plånböcker som inte uppfyller kraven i förordningen.

Sannolikt kommer plånböckerna att användas i flera olika situationer, men en stor del av människors behov av att sköta ärenden skulle tills vidare gälla ärenden i Finland. Vid beredningen av propositionen har man av denna anledning bedömt behovet av nationell reglering som skulle gälla plånböcker som endast används nationellt. Denna reglering skulle kunna bygga på kraven i den reviderade eIDAS-förordningen, men vara administrativt lättare. Regleringen skulle framför allt kunna gälla kraven på en nationell plånbok och bedömning av dess överensstämmelse. Avsikten med denna reglering skulle vara att möjliggöra styrkande av plånböckers tillförlitlighet.

I de rundabordsdiskussioner som beskrivs ovan i avsnitt 5.1.3 utreddes intressentgruppernas åsikter också om behovet av reglering av nationella plånböcker. Intressentgrupperna var eniga om att ingen nationell reglering behövs, eftersom det är fråga om en bransch under utveckling. Enligt intressentgruppernas åsikter är det i detta skede viktigt att möjliggöra innovationer och utveckling av olika handlingsmodeller samt att Finland kvarstår som en öppen marknad. Utvecklingen av plånböckerna kan stödja sig på självreglering inom branschen (såsom avtal och regelböcker). Således stannade man vid beredningen för att man i detta skede inte bereder någon separat plånboksreglering i Finland för plånböcker som endast fungerar nationellt. Detta motsvarar också målet i regeringsprogrammet om att minimera den nationella tilläggsregleringen.

5.2 Handlingsmodeller som används eller planeras i andra medlemsstater

Under beredningen av propositionen utreddes för vissa medlemsstater hur de planerar att vidta eller redan har vidtagit åtgärder i anslutning till genomförande av den reviderade eIDAS-förordningen. Förordningen i sig är som sådan direkt tillämplig och förpliktande reglering, men till vissa delar möjliggör den utnyttjande av nationellt handlingsutrymme. Vid beskrivningen av handlingsmodeller som används eller planeras i andra medlemsstater har hänsyn tagits också till arbetet i pågående och avslutade omfattande pilotprojekt med finansiering från EU:s Digital Europe Programme. Funktionerna i den europeiska digitala identitetsplånboken testades under 2023–2025 i fyra olika konsortier, och Finland var med i tre av dem. Konsortierna gick under

namnen DC4EU, där Finland deltog i synnerhet i arbetspaketet för studieintyg inom högskolesektorn, och EWC, där Finland deltog i synnerhet i arbetspaketet för juridiska personers digitala identitet, samt Potential, där Finland deltog i synnerhet i arbetspaketet för anslutning till intyg över körtillstånd.

5.2.1 Sverige

I Sverige har man gjort en utredning om säker och tillgänglig digital identitet, och slutbetänkandet färdigställdes i juni 2024. Utredningen lämnades till ministern för civilärenden Erik Slottnér den 17 juni 2024 (Kompletterande bestämmelser till EU:s reviderade förordning om elektronisk identifiering, <https://www.regeringen.se/contentassets/9291c089f96948e6828c55b32be55ae6/kompletterande-bestammelser-till-eus-reviderade-forordning-om-elektronisk-identifiering-sou-202445.pdf>). Slutbetänkandet tog ställning till hur skyldigheterna enligt den reviderade eIDAS-förordningen och i synnerhet regleringen av den europeiska digitala identitetsplånboken ska genomföras nationellt. Enligt utredningen förhåller sig Sveriges regering positivt till förslagen i slutbetänkandet, och härnäst fortsätter beredningen av dessa i statsrådets kansli.

I följande skede av beredningen kommer Sveriges regering att utse den myndighet som producerar en nationell certifierad plånbok för både fysiska personer och juridiska personer. I utredningen bedömdes det att Myndigheten för digital förvaltning, DIGG, är lämpligast för denna uppgift. Myndigheten i fråga ska ansvara också för identitetsmatchning av fysiska personer. När det gäller juridiska personer finns det ingen särskild myndighet i Sverige som har registreringsansvar för alla juridiska personer. I utredningen föreslås det att regeringen, för att garantera effektiviteten, ska utse en myndighet med uppgift att sköta identifieringen av juridiska personer, t.ex. att utfärda identifieringsuppgifter. Bolagsverket bedömdes i utredningen vara lämpligast för den här uppgiften. Med utredningen som grund har Digg inlett åtgärder för att producera en plånbok som tillhandahålls av den offentliga sektorn (<https://www.digg.se/digitala-tjanster/digital-identitetsplanbok/diggs-roll-och-samverkan-med-andra->). Diggs plånbok kan tillhandahållas senast i slutet av 2026, medan övriga aktörer kan börja tillhandahålla sina plånböcker från och med 2027.

Certifieringen av den europeiska digitala identitetsplånboken kommer i Sverige att grunda sig huvudsakligen på certifiering enligt cybersäkerhetsakten. I Sverige är Försvarets materielverk (FMV) nationell certifieringsmyndighet för cybersäkerheten. Av denna anledning bedömdes det i utredningen att Försvarets materielverk är bäst lämpat för uppgiften att utse ansvarigt organ för certifiering av digitala identiteter och system för elektronisk identifiering i Sverige. Sverige deltar också i ett projekt som med finansiering från Nordiska ministerrådet utvecklar ett gemensamt certifieringssystem för identitetsplånböcker för de nordiska och de baltiska länderna.

Post- och Telestyrelsen (PTS) kommer enligt nuvarande uppgifter att ansvara för registret över förlitande parter. Dessutom ska Post- och Telestyrelsen vara tillsynsmyndighet, och således ansvara för tillsynen över leverantörer av betrodda tjänster och påförande av relaterade administrativa böter. Den lagreglering som är nödvändig med anledning av inrättandet av en europeisk digital identitetsplånbok och kraven om utfärdande av sanktionsavgifter ska, enligt förslagen i utredningen, införas huvudsakligen i lagen med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering. Sverige deltog under 2023–2025 i EU-finansierade pilotprojekt kring de digitala identitetsplånböckerna i DC4EU- och WWC-konsortierna.

5.2.2 Estland

I Estland ansvarar myndigheten för statens informationssystem (Riigi Infosüsteemi Amet, RIA) för styrningen av utvecklingen av den europeiska digitala identitetsplånboken. Ansvaret för utvecklingsarbetet i anslutning till den egentliga plånboken bärs av RIA:s avtalspart AS Cybernetica. I Estland har alla medborgare redan en digital identitet i bruk, och målet är att i och med ibruktagandet av plånboken förbättra de digitala tjänsterna ytterligare. RIA:s avtalspart AS Cybernetica har sammanställt en analys av arkitekturen för den tekniska plånbokslösningen samt dess interoperabilitet med det redan existerande ekosystemet för digital identitet. Analysen publicerades mot slutet av 2023 (Digikukru-I-etapi-analuu.pdf, ria.ee). Estland tog i samband med Potential-konsortiets pilotprojekt upp utmaningarna med interoperabilitet i situationer där det inte i alla medlemsstater finns tillgång till en permanent identifierande kod för personer. Estlands nuvarande ekosystem för elektronisk identifiering stöder sig på att personer har identifierande koder. Estland deltar också i ett av Nordiska ministerrådet finansierat projekt, där man utvecklar ett gemensamt certifieringssystem för plånböckerna för de nordiska och de baltiska länderna.

I Estland har arbetet med att utveckla en plånboksapplikation pågått sedan januari 2024. Utvecklingsarbetet utgår från AS Cyberneticas ovannämnda analys. Den första versionen av den europeiska digitala identitetsplånboken, dvs. den minsta livskraftiga produkten, är redan klar och lämnades till RIA i juni 2024. Beslutsfattandet om den fortsatta utvecklingen av plånboken sker på politisk nivå och utvecklingsarbetet fortsätter utifrån dessa riktlinjer. Estland deltog under 2023–2025 i EU-finansierade pilotprojekt kring plånböckerna i EWC- och Potential-konsortierna. Den exempelpånbok som Estland använde i Potential-konsortiet är tillgänglig i tjänsten Github (<https://github.com/open-eid/eudi-wallet-poc>). Enligt Potential-konsortiets slutrapport kommer Estland ytterligare att konkurrensutsätta genomförandet av den slutliga europeiska digitala identitetsplånboken. I praktiken är det alltså fortfarande osäkert om plånboken genomförs av en aktör inom den offentliga eller den privata sektorn. Konkurrensutsättningen omfattar åtminstone upphandling av den tekniska plattformen för plånboken, tillhandahållande av identifieringsuppgifter för personer, tillhandahållande av kvalificerade certifikat och elektronisk underskrift på kvalificerad nivå samt administration av åtkomstcertifikat.

5.2.3 Tyskland

I Tyskland finns det en arbetsgrupp, GovLabDE Digital Identities, som är verksam mellan flera ministerier och som främjar förbundsstatens ministeriers gemensamma projekt. Arbetsgruppen utvecklar digitala identiteter och möjligheter för identifiering som staten tillhandahåller. I Tyskland är ett online-identitetskort redan i bruk. Det är fråga om ett identifieringsverktyg som staten producerat. Dessutom är det möjligt för medborgarna att använda verktyget BundID vid kommunikation, vilket i praktiken är ett elektroniskt identitetsbevis. Med hjälp av BundID kan en medborgare identifieras tillförlitligt på nätet. I framtiden kommer den europeiska digitala identitetsplånboken, som är förenlig med den reviderade eIDAS-förordningen, att läggas till som ny egenskap i samband med online-identitetskortet. Tyskland har framfört att landet kommer att gå vidare med ibruktagandet av europeiska digitala identitetsplånböcker etappvis.

Förbundsstatens inrikesministerium (Bundesministerium des Innern und für Heimat, BMI) inledde den 7 juni 2023 en arkitektur- och samrådsprocess för planering av ett helhetssystem för digitala identiteter i samband med fullgörandet av skyldigheterna enligt den reviderade eIDAS-förordningen. Ansvaret för det praktiska genomförandet av projektet har burits av SPRIND, på uppdrag av BMI. Målet har varit att utveckla en prototyp för plånbokens infrastruktur tillsammans med medborgarna, föreningar, universitet, den privata sektorn samt

aktörer inom den offentliga sektorn. Arkitekturbeskrivningar och andra beskrivningar som har uppkommit under processens gång har publicerats i Open CoDE-portalen och de kan läsas av vem som helst. Målet har varit en öppen, engagerande och transparent process för utveckling av plånboken. Som en del av Potential-konsortiets pilotprojekt har Tyskland rapporterat om utmaningar i synnerhet när det gäller halvfärdiga standarder och specifikationer i anslutning till genomförandet av den europeiska digitala identitetsplånboken, ekosystemets interoperabilitet, genomförandet av kapaciteter som garanterar integritetsskyddet och olika plånboksarkitekturer. En annan utmaning som lyfts fram är att balansera mellan en användbar plånbok och en plånbok med hög säkerhet. För att tackla utmaningarna kommer Tyskland att producera bl.a. en portal för ett plånboksekosystem och en testmiljö som är isolerad från produktionen. Med hjälp av dessa kan plånboksrelaterad information delas till tyska intressentgrupper.

Som en del av arkitektur- och samrådsprocessen genomfördes en innovationstävling om plånboken. De team som godkännts till innovationstävlingen valdes av en jury i Leipzig i maj 2024. I innovationstävlingen deltog sex team med finansiering av SPRIND och fem team som inte finansierades. Innovationstävlingen pågick från maj 2024 till oktober 2025. Tyskland deltog under 2023–2025 i de EU-finansierade pilotprojekten kring plånböcker i DC4EU-, EWC-, NOBID- och Potential-konsortierna. Som fortsättning på SPRIND-försöket kommer Tyskland att producera minst en plånbokslösning som uppfyller villkoren i förordningen och som tillhandahålls av staten.

5.2.4 Nederländerna

I Nederländerna ansvarar ministeriet för inrikesfrågor och samarbetsrelationer (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, BZK) för genomförandet av skyldigheterna i enlighet med förordningen i anslutning till den europeiska digitala identitetsplånboken. Ministeriet har inrättat ett program för genomförandet av den reviderade eIDAS-förordningen. Målet för programmet är att utveckla och producera en referensplånbok som i slutet av programmet publiceras också för produktionsbruk. Utvecklingen görs öppet och transparent och så att användarna görs delaktiga. Den öppna utvecklingen av plånboken och det nationella EDI-systemet sker med hjälp av tjänsterna GitHub och Figma. Målet är att producera en plånbok som kan användas inte bara av fysiska personer utan också av juridiska personer. Ett pilotförsök med den första testversionen av plånboken gjordes under 2024. Nederländerna förutser att de nationella lagstiftningsändringar som den reviderade eIDAS-förordningen förutsätter kan antas under 2027. Nederländerna ser det som en viktig utmaning i ibruktagandet av plånböckerna att en stor del av medborgarna inte har ett befintligt elektroniskt identifieringsverktyg för stark autentisering som uppfyller tillitsnivån hög. Den elektroniska identifieringen i samhället stöder sig i stället i stor utsträckning på utnyttjande av elektroniska identifieringsverktyg för stark autentisering som uppfyller tillitsnivån väsentlig.

Det nederländska ekonomi- och klimatministeriet beställde en rapport om den reviderade eIDAS-förordningens konsekvenser för betrodda tjänster. Rapporten producerades av INNOPAY och publicerades i april 2024 (<https://www.innopay.com/en/publications/innopay-delivers-report-dutch-ministry-economic-affairs-and-climate-impact-eidas>). Enligt rapporten innebär den reviderade eIDAS-förordningen både möjligheter och utmaningar för betrodda tjänster i Nederländerna. En fördel ansågs vara att förordningen eventuellt skapar nya, ökande användningsfall och nya inkomstflöden, men samtidigt förutsätter den också strängare överensstämmelse med reglerna och kan således leda till en koncentration på marknaden. I rapporten lyftes det också fram att Nederländernas ekonomi- och klimatministeriums aktiva deltagande är ytterst viktigt för genomförandet av förordningen, för att möjligheterna och tillväxtpotentialen ska kunna utnyttjas fullt ut vid säkerställandet av marknaden för betrodda

tjänster i den digitala ekonomin. Nederländerna deltog 2023–2025 i de EU-finansierade plånbokspilotprojekten i DC4EU-, EWC- och Potential-konsortierna.

5.2.5 Danmark

I Danmark ansvarar Digitaliseringsstyrelsens kontor för eID och applikationer för det nationella genomförandet i enlighet med kraven i EU-lagstiftningen och för samordningen av detta. Kontoret ansvarar för den gränsöverskridande användningen av digitala personbeteckningar (eID) samt för utvecklingen och administrationen av relaterade applikationer. Dessutom ansvarar kontoret för uppgifter enligt den reviderade eIDAS-förordningen i anslutning till ibruktagande av den europeiska digitala identitetsplånboken.

Danmark deltog 2023–2025 i de EU-finansierade plånbokspilotprojekten i DC4EU-, EWC- och NOBID-konsortierna.

6 Remissvar

Yttranden begärdes om utkastet till regeringsproposition under tiden 12.6–29.8.2025 i tjänsten utlåtande.fi. Remissinstanserna var totalt 115, varav 13 meddelade att de inte har något att yttra och två meddelade att de inte lämnar något yttrande i ärendet. I begäran om yttrande ombads remissinstanserna ge sina observationer separat om den nationella reglering som kompletterar eIDAS-förordningen, regleringen om e-legitimation, ändringarna för att förbättra säkerheten i den nationella starka autentiseringen samt den nationella ekosystembeskrivningen. Alla remissinstanser yttrade sig inte om alla helheter som specificerades i begäran. Remissvaren finns samlade i form av ett sammandrag, där det viktigaste innehållet i yttrandena beskrivs. Yttrandena och sammandraget finns tillgängliga i den offentliga tjänsten på adressen <https://vm.fi/hanke?tunnus=VM059:00/2024>.

6.1 Remissvar om genomförandet av den reviderade eIDAS-förordningen

Remissinstanserna förhöll sig positivt till de nationella regleringsförslag som kompletterar den reviderade eIDAS-förordningen. Målen för propositionen ansågs vara motiverade och de föreslagna lösningarna inverkar positivt på genomförandet av myndighetstjänsterna i synnerhet i situationer där ärenden sköts över landsgränserna. Rådgivningen och stödet till medborgarna betraktades som ytterst viktigt vid införandet av de nya tjänsterna. Dessutom ansåg remissinstanserna att verktygen och tjänsterna för elektronisk identifiering blir mer heltäckande och likvärdigt tillgängliga för medborgarna.

Enligt remissvaren är det viktigt att möjligheten att använda andra identifieringsverktyg och alternativa sätt att sköta ärenden kvarstår. Konsekvensbedömningen i propositionen har till denna del kompletterats för att det ska vara klart att det nuvarande betrodda nätverket för stark autentisering bevaras vid sidan av de europeiska digitala identitetsplånböckerna. Dessutom tog Transport- och kommunikationsverket i sitt yttrande upp behovet av att precisera förhållandet mellan tillämpningen av den föreslagna eIDAS-lagen och autentiseringslagen i situationer där tillhandahållarna av tjänster för identifieringsförmedling förmedlar identifiering som grundar sig på en plånbok. Dessutom ansåg Findynet Osuuskunta att det är behövligt att förtydliga förmedling som grundar sig på plånboken och rollen för tillhandahållaren av plånboken i dessa situationer. Motiveringen till det andra lagförslaget har till denna del preciserats så att förmedling av identifiering som grundar sig på en plånbok förutsätter att tillhandahållaren av tjänsten för identifieringsförmedling är registrerad i registret över förlitande parter i anslutning till den europeiska digitala identiteten och att kraven i eIDAS-förordningen också i övrigt tillämpas. I motiveringen ströks dessutom beskrivningen av möjligheten för tillhandahållare av

en plånbok att begränsa förmedlingen av identifiering som grundar sig på plånboken. Plånboken och de uppgifter den innehåller är i användarens uteslutande besittning och den som tillhandahåller en plånbok kan inte begränsa användarens verksamhet.

Rollen för Myndigheten för digitalisering och befolkningsdata som tillhandahållare av plånboken understöddes, men samtidigt betraktades det som viktigt att aktörer inom den privata sektorn ges möjlighet att tillhandahålla en plånbok. Konkurrens- och konsumentverket ansåg att den konkurrensrättsliga analysen i propositionen innehåller utmaningar. Konkurrens- och konsumentverket ansåg att plånböckerna i stället för som en helhet bör bedömas utifrån delfunktionerna i plånboksapplikationerna, och enligt verket innehåller plånböckerna funktioner som kan höra till en befintlig nyttighetsmarknad. Också Posti Group Abp och arbets- och näringsministeriet tog i sina yttranden upp konkurrensrättsliga aspekter på rollen för Myndigheten för digitalisering och befolkningsdata som tillhandahållare av en plånbok. Enligt remissvaren får det inte uppstå omotiverad konkurrensfördel för Myndigheten för digitalisering och befolkningsdata med anledning av myndighetens ställning eller finansiering när det gäller tillhandahållandet av plånboken.

Vid den fortsatta beredningen av propositionen fördes diskussioner med Konkurrens- och konsumentverket. Den konkurrensrättsliga analysen i propositionen har ändrats utifrån remissvaren så att den svarar mot den konkurrensrättsliga oro som framfördes i remissvaren och att det är tydligt att regleringen inte begränsar Konkurrens- och konsumentverkets befogenhet att ingripa i konkurrensen på marknaden i enlighet med konkurrenslagen. I den konkurrensrättsliga analysen förs nu tydligare fram att tillhandahållandet av en plånbok i regleringen anförtros Myndigheten för digitalisering och befolkningsdata av den anledningen att sedvanlig marknadsverksamhet inte finns och inga plånböcker som uppfyller kraven i den reviderade eIDAS-förordningen kommer att tillhandahållas inom den utsatta tiden (*marknadsbrist*). Propositionen begränsar emellertid inte andra aktörers möjligheter att tillhandahålla en plånbok vid sidan av den plånbok som Myndigheten för digitalisering och befolkningsdata tillhandahåller. Justitieministeriet tog i sitt yttrande upp behovet av att bedöma om den uppgift som föreskrivs för Myndigheten för digitalisering och befolkningsdata eventuellt, om den överförs på en privat aktör, utgör en offentlig förvaltningsuppgift, vilket i så fall kräver lagstiftning på det sätt som förutsätts i 124 § i grundlagen (731/1999). Specialmotiveringen om Myndigheten för digitalisering och befolkningsdatas uppgift har till denna del kompletterats.

Bland annat Utbildningsstyrelsen och Folkpensionsanstalten understödde förslaget att Myndigheten för digitalisering och befolkningsdata har rollen att centraliserat tillhandahålla identitetsmatchning. Den reviderade eIDAS-förordningen förutsätter att identitetsmatchningen säkerställs endast i e-tjänster inom den offentliga sektorn. I anslutning till detta tog bl.a. Olycksfallsförsäkringscentralen och Pensionsskyddscentralen upp de privata aktörer som sköter offentliga förvaltningsuppgifter och ansåg att det är viktigt att dessa aktörers roll beaktas i propositionen, liksom även möjligheten att använda den identitetsmatchning som Myndigheten för digitalisering och befolkningsdata tillhandahåller. Vid den fortsatta beredningen har bestämmelsen om identitetsmatchning i det första lagförslaget i propositionen preciserats så att också aktörer som sköter offentliga förvaltningsuppgifter kan använda den identitetsmatchning som Myndigheten för digitalisering och befolkningsdata tillhandahåller. Dessutom önskade exempelvis arbetspensionsförsäkringsbolagen, Findynet Osuuskunta och Nordea Bank Abp i sina remissvar att identitetsmatchningstjänsten över huvud taget utvidgas till aktörer inom den privata sektorn och att den föreslagna regleringen inte ska begränsa den fortsatta utvecklingen av matchningstjänsten och tillhandahållandet av den i större utsträckning till den privata sektorn. Vid den fortsatta beredningen har man i propositionen lagt till en uttrycklig bestämmelse om att aktörer inom den privata sektorn har rätt att använda den identitetsmatchning som Myndigheten

för digitalisering och befolkningsdata tillhandahåller. Tillämpningen av bestämmelsen inleds emellertid i ett senare skede, efter att skyldigheten för e-tjänster inom den privata sektorn att godkänna identifiering med europeisk digital identitetsplånbok har införts.

Den föreslagna åldersgränsen på 13 år för självständigt ibruktagande av en europeisk digital identitetsplånbok fick brett understöd i synnerhet i remissvaren från social- och hälsovårdsministeriets samt undervisnings- och kulturministeriets förvaltningsområden. Centralkriminalpolisen och Polisstyrelsen önskade i sina yttranden en högre åldersgräns för självständigt ibruktagande av en plånbok. De såg orsak till oro i synnerhet i relation till en ökad mängd identitetsstöld och bedrägeribrottslighet och allmänt minskad tillit till elektronisk kommunikation. Vid den fortsatta beredningen har det utifrån remissvaren bedömts att åldersgränsen för ibruktagande inte behöver höjas. Motiveringen till och konsekvensbedömningen av den föreslagna åldersgränsen har emellertid kompletterats på grundval av remissvaren och riskerna med den föreslagna åldersgränsen har lyfts fram tydligare, liksom även nyttan med att minderåriga kan sköta sina ärenden elektroniskt.

I synnerhet utrikesministeriet och Suomi-Seura ry ansåg att det bör göras möjligt att ta i bruk en plånbok också genom besök hos Finlands utländska beskickningar när en person inte har möjlighet att ta i bruk plånboken elektroniskt. Vid den fortsatta beredningen har bestämmelserna om i det första lagförslaget beviljande av identifieringsuppgifter för en fysisk person i det första lagförslaget kompletterats så att personen kan ansöka om identifieringsuppgifter för en fysisk person också genom att besöka en finländsk beskickning utomlands. Beviljandet av identifieringsuppgifter för fysiska personer är en del av beviljandet och ibruktagandet av en europeisk digital identitetsplånbok och de föreslagna ändringarna motsvarar således det som önskats i remissvaren.

Förbudet i den föreslagna regleringen om att överlåta plånboken för att användas av någon annan sågs i synnerhet i diskrimineringsombudsmannens yttrande som en utmaning i synnerhet för personer som behöver en personlig assistent för att kunna använda plånboken. Under den fortsatta beredningen av propositionen fördes det diskussioner med diskrimineringsombudsmannens byrå. På grundval av remissvaren gjordes inga ändringar i bestämmelserna om användarens ansvar i det första lagförslaget, men motiveringen till bestämmelserna har preciserats så att det tydligare framgår att regleringen inte begränsar de åtgärder och anpassningar som tillhandahållaren av en europeisk digital identitetsplånbok gör för att möjliggöra en likvärdig och tillgänglig användning av plånboken. I motiveringen har det också preciserats att den föreslagna bestämmelsen endast reglerar användarens ansvar.

I remissvaren lyftes det fram att eIDAS-förordningen bör samordnas med SDG-förordningen samt det anknyttande OOTS-systemet. Dessutom betraktades det som viktigt att man säkerställer att genomförandet av den reviderade eIDAS-förordningen inte leder till överlappande eller motstridiga tekniska lösningar. Inga ändringar har gjorts i den föreslagna regleringen utifrån remissvaren. Den reviderade eIDAS-förordningen och SDG-förordningen är EU-förordningar och ska i princip harmoniseras på EU-nivå. Det är inte heller möjligt för medlemsstaterna att låta bli att fullgöra skyldigheter som följer av någondera förordningen på den grunden att skyldigheten är överlappande eller står i strid med en annan EU-förordning. Bedömningen av propositionens gränsöverskridande konsekvenser har emellertid kompletterats utifrån remissvaren, och harmoniseringen av förordningarna på EU-nivå har beskrivits.

I remissvaren ansågs avgränsningen av propositionen till juridiska personer som är införda i handelsregistret vara alltför smal. Remissinstanserna önskade att propositionen utvidgas och preciseras så att alla aktörer som bedriver ekonomisk verksamhet och har ett FO-nummer kan få identifieringsuppgifter. Det önskades också att även offentliga sammanslutningar och

registrerade föreningar och stiftelser ska kunna delta i digital kommunikation. Dessutom fördes det fram att det bör gå att sköta ärenden för andras räkning och att använda fullmakter på ett tydligt och tryggt sätt.

Det fanns flera orsaker till att man stannade för den regleringslösning som föreslås, och dessa orsaker ansågs fortfarande vara relevanta vid den fortsatta beredningen. För det första kan identifieringsuppgifter för en juridisk person enligt den reviderade eIDAS-förordningen beviljas endast juridiska personer. Exempelvis en privat näringsidkare är inte en juridisk person och kan därför inte beviljas identifieringsuppgifter för en juridisk person. För det andra har propositionen begränsats så att den gäller endast juridiska personer som är införda i handelsregistret. Orsaken till detta är det strama tidsschemat för det nationella genomförandet samt de begränsade resurserna. Beviljandet och förvaltningen av identifieringsuppgifter samt de olika skedena i en identifieringsuppgifts livscykel är förknippade med öppna frågor, och det är motiverat att man löser dessa genom riktade pilotprojekt i inledningsskedet. För det tredje är avsikten med propositionen framför allt att göra det möjligt att utfärda identifieringsuppgifter för juridiska personer, vilket skapar förutsättningar för ibruktage av en företagsplånbok. Denna referensram kan utvidgas stegvis, också på annat sätt än genom lagstiftning.

I remissvaren påpekades det att det finns ideella föreningar och stiftelser som bedriver näringsverksamhet och som är införda i handelsregistret. Vid den fortsatta beredningen bedömdes det att dessa aktörer är några hundra till antalet. När det gäller andra juridiska personer innehåller handelsregistret heltäckande uppgifter om den juridiska personens ansvarspersoner, dvs. dem som har rätt att företräda den juridiska personen. Däremot antecknas ansvarspersonerna för ideella föreningar och stiftelser inte i handelsregistret och det är inte motiverat att ge dessa identifieringsuppgifter om inte lagstiftningen i ett senare skede utsträcks till att omfatta också aktörer som är införda i förenings- och stiftelseregistret. Propositionen har vid den fortsatta beredningen ändrats till denna del så att ideella föreningar och stiftelser som är införda i handelsregistret inte i inledningsskedet beviljas identifieringsuppgifter för en juridisk person. Under beredningen har också andra användningsfall och behov i anslutning till bedrivande av näringsverksamhet identifierats och de motsvarar i stor utsträckning de behov som lyfts fram i remissvaren. Dessa har emellertid i detta skede uteslutits ur propositionen av de orsaker som anges ovan.

Vid den fortsatta beredningen av propositionen följdes också noggrant utvecklingen av EU-lagstiftningen. Kommissionen lämnade den 19 november 2025 ett förslag till Europaparlamentets och rådets förordning om införande av europeiska företagsplånböcker. Kommissionen föreslår bl.a. att företagsplånboken ger alla ekonomiska aktörer en digital identitet, möjliggör delning av data och gränsöverskridande åtkomst till elektroniska tjänster samt möjliggör användningen av betrodda tjänster. EU-lagstiftningen om företagsplånböcker bedöms ha betydande konsekvenser också för den nationella referensramen, och det har inte i den aktuella propositionen setts som ändamålsenligt att på ett nationellt plan gå in för lösningar som eventuellt måste ändras på grund av ny EU-reglering.

Förslaget om att utnyttja det nationella handlingsutrymmet i fråga om den öppna källkoden fick understöd, men t.ex. TietoEVERY Abp och Finanssiala ry önskade i sina yttranden preciseringar i den föreslagna regleringen när det gäller beskrivningen av och motiveringen till den öppna källkoden. Vid den fortsatta beredningen preciserades formuleringen i bestämmelserna i enlighet med yttrandena så att tillhandahållaren av en plånbok inte behöver lämna ut källkoden till den del den omfattas av handlingsutrymmet när det finns en sakligt grundad orsak till detta. Vid den fortsatta beredningen bedömdes dessutom hur omfattande det nationella handlingsutrymmet är och man kom fram till att alla preciseringar och begränsningar som framförts i yttrandena inte kan beaktas, eftersom de inte faller inom det nationella

handlingsutrymmet. De europeiska digitala identitetsplånböckerna är inte beroende av enskilda bibliotek, utan alternativ till dem kan erbjudas där tillhandahållarna av plånböcker kan välja det lämpligaste biblioteket t.ex. utgående från licenserna eller möjligheterna till integrering. De bibliotek som står till buds kan emellertid inte begränsas inom ramen för det nationella handlingsutrymmet. Dessutom önskade bl.a. Tullen och FiCom ry preciseringar i möjligheterna att använda elektronisk underskrift och i de villkor som gäller arbets- och tjänsteuppgifter. De föreslagna bestämmelserna om avgiftsbelagd elektronisk underskrift har preciserats på grundval av yttrandena. I propositionen preciseras eller avgränsas dock inte de möjliga användningsändamålen för elektronisk underskrift, eftersom detta är en fråga som varje aktör själv ska bedöma.

Bland annat riksdagens justitieombudsman och justitieministeriet föreslog i sina yttranden preciseringar i Transport- och kommunikationsverkets rättigheter att lämna ut och få information. Bestämmelserna i det första lagförslaget har preciserats i enlighet med remissvaren. Justitieministeriet ansåg därtill att motiveringen till bestämmelserna om den personuppgiftsansvarige för den plånbok som Myndigheten för digitalisering och befolkningsdata tillhandahåller behöver preciseras och att det måste säkerställas att motiveringen är i linje med den allmänna dataskyddsförordningen med hänsyn till kraven i den reviderade eIDAS-förordningen om användarens egen kontroll över uppgifterna i plånboken. UF-centret efterlyste dessutom i sitt yttrande klarhet i personuppgiftsansvarigas skyldigheter i fråga om elektroniska attributsintyg. Motiveringen till den paragraf i det första lagförslaget som gäller den personuppgiftsansvarige för den plånbok som Myndigheten för digitalisering och befolkningsdata tillhandahåller har preciserats på basis av remissvaren, och en tydligare beskrivning av de olika aktörernas och användarens ansvar i fråga om uppgifterna i plånboken har eftersträfvats.

Finlands Kommunförbund rf, Findynet Osuuskunta och TietoEVERY Abp önskade vid den fortsatta beredningen klarhet i hur kontrollen av attribut mot autentiska källor ska genomföras i samband med det nationella genomförandet. Propositionen har kompletterats på grundval av remissvaren genom att det i det första lagförslaget har tagits in en uttrycklig paragraf om skyldigheten för Myndigheten för digitalisering och befolkningsdata att utarbeta nationella anvisningar om de elektroniska medel som kvalificerade leverantörer av betrodda tjänster kan använda när de vill kontrollera de attribut som avses i bilaga VI till eIDAS-förordningen mot autentiska källor i Finland.

I fråga om administrativa påföljder och påföljdsavgifter ansåg Riksdagens justitieombudsman i sitt yttrande att den föreslagna regleringen är omsorgsfullt beredd. Enligt yttrandet bör emellertid förbudet mot dubbel straffbarhet bedömas med tanke på EU:s rättspraxis. Också Suomen Asianajajat förde i sitt yttrande fram behovet av att vid den fortsatta beredningen bedöma om en och samma gärning kan vara straffbar också med stöd av brott mot någon annan reglering, och vilken myndighet som i en sådan situation fattar avgörandet i det enskilda fallet. Vid den fortsatta beredningen ändrades propositionen så att en påföljdsavgift som påförts med stöd av en bestämmelse (eIDAS-förordningen, NIS 2-direktivet/cybersäkerhetslagen eller den allmänna dataskyddsförordningen) inte ska vara ett hinder för påförande av påföljdsavgift med stöd av en annan bestämmelse. Motiveringar till denna regleringslösning fogades till avsnitt 12.4 i propositionen.

Justitieministeriet ansåg i sitt yttrande att det är viktigt att andra administrativa påföljder används i första hand och att påförande av administrativ påföljdsavgift ska tillgripas först i sista hand. Motiveringen till propositionen har till denna del preciserats för att det ska vara tydligt att myndigheten i första hand genom rådgivning och vägledning ska styra aktörerna till att bedriva sin verksamhet i enlighet med den föreslagna lagstiftningen och den reviderade eIDAS-

förordningen. En administrativ påföljdsavgift är således inte den metod som ska användas i första hand för att ingripa i verksamhet som står i strid med lagstiftningen. Rättsregistercentralen understödde inte möjligheten att påföra myndigheter påföljdsavgifter av straffkaraktär, och enligt centralen bör ett utlåtande i frågan begäras av grundlagsutskottet. Vid den fortsatta beredningen har det vidare bedömts att den reviderade eIDAS-förordningen inte lämnar handlingsutrymme för att utesluta myndigheter från administrativa påföljdsavgifter. Propositionen har inte ändrats på grundval av yttrandet, men det föreslås att grundlagsutskottet ska lämna ett utlåtande om propositionen.

Arbets- och näringsministeriet, Patent- och registerstyrelsen, kommunikationsministeriet samt Transport- och kommunikationsverket tog i sina yttranden upp de fortlöpande kostnader som ämbetsverken orsakas av de uppgifter som föreslås i propositionen. Patent- och registerstyrelsen ansåg att kostnaderna för beviljande och upprätthållande av identifieringsuppgifter för juridiska personer ska täckas fullt ut med avgifter som tas ut för prestationerna i fråga. Dessutom tog Transport- och kommunikationsverket i sitt yttrande upp behovet av att göra ändringar i de avgifter som ämbetsverket tar ut. Transport- och kommunikationsverket föreslog också att det i propositionen tas in en bestämmelse om prioritering av Transport- och kommunikationsverkets uppgifter, med stöd av vilken ämbetsverket kan placera sina styrnings- och tillsynsuppgifter i ordning enligt prioritet och tillgängliga resurser. Vid den fortsatta beredningen av propositionen har det, i enlighet med det som Transport- och kommunikationsverket föreslog i sitt yttrande, lagts till en tillsynsavgift som ska betalas till den som tillhandahåller en europeisk digital identitetsplånbok. Dessutom har det föreslagits att de tillsynsavgifter som redan finns höjs och att en del av de avgifter som i nuläget är på lagnivå i fortsättningen regleras på förordningsnivå. Till det första lagförslaget har dessutom fogats bestämmelser som gör det möjligt för Transport- och kommunikationsverket att prioritera sina uppgifter.

Transport- och kommunikationsverket föreslog i sitt yttrande också annan preciserande reglering om de uppgifter, befogenheter och bemyndiganden att meddela föreskrifter som gäller ämbetsverket. De åsikter som ämbetsverket framförde har huvudsakligen beaktats i den fortsatta beredningen av förslaget. I synnerhet har man preciserat Transport- och kommunikationsverkets uppgift i anslutning till inrättandet och förandet av registret över förlitande parter i anslutning till den europeiska digitala identitetsplånboken. Transport- och kommunikationsverket föreslog också att den som tillhandahåller den europeiska digitala identitetsplånboken efter att plånboken har certifierats ska ansöka om Transport- och kommunikationsverkets godkännande eller erkännande för plånboken så att den erkänns i Finland och kan anmälas till EU-kommissionen. Vid den fortsatta beredningen har det bedömts att den som tillhandahåller plånboken endast mycket begränsat, om alls, kan åläggas nationella skyldigheter. Transport- och kommunikationsverkets yttrande har emellertid beaktats så att den som tillhandahåller plånboken ska meddela Transport- och kommunikationsverket de uppgifter som behövs för anmälan av plånboken till Europeiska kommissionen. I detta sammanhang kan Transport- och kommunikationsverket som tillsynsmyndighet säkerställa att plånboken uppfyller kraven enligt den reviderade eIDAS-förordningen. Om Transport- och kommunikationsverket bedömer att kraven uppfylls anmäler det plånboken till Europeiska kommissionen varvid plånboken betraktas som erkänd i Finland.

Många andra organisationer, t.ex. social- och hälsovårdsministeriet, Skatteförvaltningen och Kesko Abp, förde i sina yttranden fram att ibruktagandet av plånboken och i synnerhet besök för att sköta ärenden orsakar kostnader och systemändringar i e-tjänsterna samt behov av att utbilda personalen. Vid den fortsatta beredningen har bedömningen av konsekvenserna av propositionen kompletterats i syfte att beakta de konsekvenser som tagits upp i yttrandena. Det har emellertid också preciserats i propositionen att den reviderade eIDAS-förordningen inte innehåller någon skyldighet att möjliggöra besök för att sköta ärenden med plånboken, utan

detta är något som erbjuds enligt tjänstetillhandahållarens eget övervägande. Den reviderade eIDAS-förordningen medför en skyldighet att godkänna plånboken endast i elektronisk kommunikation.

Remissvaren innehöll flera mer tekniska observationer om den föreslagna regleringen. Lantmäteriverket fäste uppmärksamhet vid ansvarsregleringen vid elektronisk identifiering och underskrift med plånboken. Transport- och kommunikationsverket fäste uppmärksamhet vid den terminologi som i propositionen och i den föreslagna lagstiftningen används i fråga om den reviderade eIDAS-förordningen och den europeiska digitala identitetsplånboken. Dessutom önskade Riksdagens justitieombudsman i sitt yttrande att rollen för Myndigheten för digitalisering och befolkningsdata och myndighetens ansvar som upprätthållare för den nationella noden förtydligas. Vid den fortsatta beredningen ansågs det emellertid inte vara möjligt att göra de föreslagna preciseringarna, eftersom det inte föreslås några ändringar i lagstiftningen i förhållande till det som i nuläget föreskrivs i autentiseringslagen. Utsökningsverket lyfte i sitt yttrande fram att man med teknisk plattform i allmänhet hänvisar till en virtuell program- eller systemmiljö, som inte är knuten till en fysisk enhet och ansåg att mobiltelefonen snarare är en enhetsplattform. Definitionerna i propositionen har preciserats på basis av yttrandet.

Riksdagens justitieombudsman och justitieministeriet fäste i sina yttranden uppmärksamhet vid bestämmelserna om organ för bedömning av överensstämmelse och önskade förtydliganden exempelvis i anslutning till subdelegering av offentliga förvaltningsuppgifter. Vid den fortsatta beredningen har bestämmelserna om bedömning av överensstämmelse och organ för bedömning av överensstämmelse i det första lagförslaget förtydligats på det sätt som förutsatts i yttrandena. Dessutom har det i bestämmelserna om bedömning av överensstämmelse gjorts sådana ändringar som krävs enligt bestämmelser i kommissionens genomförandeförordningar som fastställts efter remissbehandlingen.

I remissvaren önskades det att uppmärksamhet ägnas åt konsekvensbedömningarna. Exempelvis Dataombudsmannen och Rättsregistercentralen önskade konsekvensbedömningar ur sitt eget ämbetsverks perspektiv, UF-centret önskade att konsekvenserna i anslutning till gränsöverskridande kommunikation preciseras och Företagarna i Finland rf önskade att konsekvenserna för företag preciseras. Konsekvensbedömningen av propositionen har i den fortsatta beredningen kompletterats utifrån remissvaren.

6.2 Remissvar om e-legitimation

I remissvaren påpekades att terminologin i lagutkastet bör vara tydlig och konsekvent. Flera av remissinstanserna, såsom Findynet Osuuskunta och TietoEVERY Abp ansåg att terminologin kring den digitala identitetsplånboken bör förenklas. Som ett problem betraktades i synnerhet att e-legitimation i utkastet definieras som en rätt att få ett attributsintyg, vilket orsakar förvirring för både medborgarna och tjänstetillhandahållarna. Formuleringen ”kvalificerade elektroniska attributsintyg som används som e-legitimation” ansågs vara svårbegriplig och obekant.

TietoEVERY Abp föreslog att lagen ska innehålla en separat bestämmelse om rätt till digital identitet som beviljas av polisen samt om e-legitimation som beviljas av Myndigheten för digitalisering och befolkningsdata. Findynet Osuuskunta föreslog en motsvarande lösning där den digitala identiteten och e-legitimationen tydligt hålls isär. Inrikesministeriet ansåg att det är viktigt att myndighetsuppgifterna preciseras så att processen blir smidigare och föreslog en modell där polisens beslut om beviljande av pass eller identitetskort samtidigt är ett positivt beslut när det gäller e-legitimation. Polisstyrelsen lyfte i sitt yttrande fram att regleringen

medför mer byråkrati och föreslog en modell där e-legitimationen knyts direkt till en fysisk handling och handlingens giltighetstid, varvid inget separat beslut om beviljande behövs. Modellen ansågs vara kostnadseffektiv och motsvara de nuvarande informationssystemen. Dessutom föreslogs en modell där användaren ansöker om ett digitalt attributsintyg direkt hos Myndigheten för digitalisering och befolkningsdata, som identifierar den sökande och säkerställer att villkoren uppfylls, varefter polisen kontrollerar att handlingen är giltig och lämnar de fastställda uppgifterna till ämbetsverket. Myndigheten för digitalisering och befolkningsdata ska ansvara för tillverkningen av e-legitimationen och för dess livscykel. Modellen ansågs förtydliga myndighetsansvaret och förbättra medborgarperspektivet. Vid den fortsatta beredningen stannade man för att föreslå en lösning i stil med den som föreslogs i yttrandena, där en behörig tillståndsmyndighet vid beviljande av i lagen avsett pass eller identitetskort samtidigt beviljar rätt till e-legitimation. På den grunden är Myndigheten för digitalisering och befolkningsdata behörig att tillhandahålla ett motsvarande kvalificerat elektroniskt attributsintyg.

Arbets- och näringsministeriet fäste uppmärksamhet vid vissa inkonsekvenser i lagutkastet i de definitioner som gäller utlänningar. Vid den fortsatta beredningen har definitionerna förenhetligats både inom lagförslaget och i förhållande till den gällande lagstiftningen om pass och identitetskort. Polisstyrelsen poängterade behovet av att säkerställa giltigheten för ett pass eller identitetskort i polisens register i samband med ibruktagandet, så att användningen av handlingar som makulerats eller förkommit kan förhindras. Vid den fortsatta beredningen granskades lagutkastet ur detta perspektiv och det gjordes betydande ändringar som tar hänsyn till det ovannämnda behovet av att säkerställa en handlings giltighet.

Vikten av att e-legitimationen är lätt att använda betonades med tanke på särskilda aktörsgrupper såsom ensamföretagare. Flera av remissinstanserna önskade att det förtydligas hur e-legitimationen i fortsättningen ska utnyttjas i samband med inledande identifiering.

I remissvaren poängterades vikten av att e-legitimationerna och plånböckerna fungerar och är interoperabla ur ett tekniskt och användarvänligt perspektiv. Flera remissinstanser poängterade att det måste säkerställas att e-legitimationen och plånboken är interoperabla och att lösningarna ska genomföras i enlighet med referensramen för europeisk interoperabilitet. Myndigheten för digitalisering och befolkningsdata lyfte fram behovet av att bevara det enhetliga datainnehållet i e-legitimationen oavsett vilket verktyg som används.

I vissa yttranden betonades vikten av att förtydliga förfarandena för fysiska besök för att sköta ärenden, i synnerhet när det gäller jämförelse av ansiktsbild med ögonmått, samt den ur dataskyddsperspektiv viktiga principen om uppgiftsminimering och situationsbundet samtycke. När det gäller konsumentskyddet poängterades också vikten av en spärri lista i realtid, höga krav på användbarhet och en fungerande spärri kanal.

Remissinstanserna ansåg att det är viktigt att föreskriva att användningen av ansiktsbild begränsas till manuell, sinnesbaserad jämförelse och att automatiserade metoder inte är tillåtna utan separat reglering. En eventuell senare reglering ska bygga på konsekvensbedömning och innehålla en tydlig, exakt rättsgrund och auditeringsskyldighet.

Centralhandelskammaren underströk att ibruktagandet av det nya plånbokssystemet inte i oskälig grad får försvåra verksamheten för aktörer som inte har beredskap att använda digital plånbok, och föreslog att alternativa tillvägagångssätt, såsom assisterade tjänster, tryggas. Teknologiateollisuus ry ansåg att det är viktigt att man vid ålderskontroll inte förutsätter utlämnande av individualiserande uppgifter och lyfte fram nollkunskapsbevis (zero knowledge proof). Inrikesministeriet ansåg att begreppet åldersbevis bör förtydligas i lagutkastet och

föreslog en regleringslösning som möjliggör verifiering av att en person är vuxen men inte utesluter andra bevis för åldersgrupp. Vid den fortsatta beredningen utvecklades lagutkastet i denna riktning.

I yttrandet poängterades betydelsen av strukturen, konsekvensen och tydligheten i regleringen om e-legitimation. Transport- och kommunikationsverket ansåg att lagens syfte och definitioner bör anges tydligt så att det framgår vad man avser att uppnå genom e-legitimationen och var den ska användas. I synnerhet bestämmelserna i definitionsparagrafen i lagutkastet och specialmotiveringen till dem har vid den fortsatta beredningen bearbetats i den riktning som föreslås i yttrandet.

Myndigheten för digitalisering och befolkningsdata påpekade att lagutkastet innehåller definitioner av två företeelser – e-legitimationer och kvalificerade elektroniska attributsintyg – på något olika sätt, trots att det i själva verket är fråga om olika former av samma datainnehåll. Eftersom attributsintygets innehåll inte har definierats lika noggrant som innehållet i e-legitimationen kan det leda till oklarhet i tjänsteproduktionen och behandlingen av uppgifter. Dessutom har vissa processer, såsom bestämmelserna om giltighetens upphörande, i utkastet definierats separat för båda företeelserna, vilket ansågs kunna leda till många olika tolkningar. Vid den fortsatta beredningen har man å ena sidan strävat efter att samordna dessa företeelser i fråga om deras datainnehåll och å andra sidan tydligare försökt skilja dem från varandra till den del regleringen gäller olika myndigheters uppgifter och behörighet.

Polisstyrelsen och inrikesministeriet lyfte fram behovet av reglering om huruvida en person kan ha flera e-legitimationer samtidigt. Polisstyrelsen ansåg att det är nödvändigt att begränsa antalet legitimationer för att missbruk ska kunna förhindras och föreslog att en person ska kunna ha endast en legitimation åt gången. Inrikesministeriet föreslog för sin del ett maximiantal på tre e-legitimationer på olika enheter, vilket skulle tillåta användning t.ex. på en personlig telefon och en arbetstelefon samt på ytterligare en enhet. Vid den fortsatta beredningen har man stannat för att föreslå två som maximiantal.

Tullen betraktade det som motiverat att ett villkor för e-legitimation är ett giltigt pass eller identitetskort, men lyfte som en brist fram att e-legitimation inte kan användas som resedokument. Transport- och kommunikationsverket lyfte fram att regleringsstrukturen kan bli oklar om en separat lag stiftas om e-legitimationer. Enligt ämbetsverket kan det leda till splittrade lösningar och belasta lagberedningen, eftersom det i framtiden i så fall finns många myndighetsbevis som införs i plånboken. Ämbetsverket föreslog att det stiftas en allmän lag om de intyg som kan införas i en elektronisk tillståndsplånbok.

I yttrandet fästes uppmärksamhet vid frågor i anslutning till ansökan om och beviljande av e-legitimation. Transport- och kommunikationsverket konstaterade att det i 7 § i lagförslaget föreskrivs om Myndigheten för digitalisering och befolkningsdatas ansvar att tillhandahålla ett kvalificerat elektroniskt attributsintyg, men att det inte beaktas att ämbetsverket ska ansöka om godkännande hos tillsynsmyndigheten och uppfylla kraven på betrodda tjänster under hela livscykeln. Också inrikesministeriet ansåg att bestämmelserna måste preciseras så att e-legitimation beviljas av en kvalificerad leverantör av betrodda tjänster och att den ska beviljas som kvalificerat elektroniskt attributsintyg.

Inrikesministeriet föreslog i sitt yttrande ändringar i villkoren i 3 § för att få e-legitimation och ansåg att det är nödvändigt att hänvisningen till 14 § i lagen om identitetskort stryks (Utfärdande av ett identitetskort för utlänningar), om inget hinder för detta följer av den nationella lagstiftningen eller EU-regleringen, samt att kritiskt granska tillämpligheten av 3 c § i passlagen (provisoriskt pass). Vid den fortsatta beredningen kunde det dock konstateras att regleringen i

den gällande lagen om identitetskort, bestämmelserna i den föreslagna lagen och den reviderade eIDAS-förordningen tillsammans garanterar tillräckliga säkerhetsfaktorer för att den strykning som tidigare ansetts nödvändig inte behöver göras. När det gäller provisoriska pass fokuserade man i den fortsatta beredningen på tillgodoseende av likvärdighet och trygghet av rättigheterna för särskilda grupper, såsom personer med funktionsnedsättning och äldre personer. Till den delen ansågs det inte finnas något ändringsbehov.

Inrikesministeriet poängterade betydelsen av avläsning på distans när ansökan inleds för att dokumentets säkerheten ska kunna säkerställas och föreslog att det ska vara möjligt att kombinera ibruktagande av plånboken och ansökan om e-legitimation vid distansavläsning. Myndigheten för digitalisering och befolkningsdata ansåg för sin del att regleringen blir tydligare om bestämmelser om tillhandahållande av attributsintyg finns i bara en paragraf. I yttrandet underströks också allmänt ett behov av att förtydliga myndigheternas roller och ansvar. Myndigheten för digitalisering och befolkningsdata påpekade att det i propositionen hänvisas till polisen och Polisstyrelsen som tillhandahållare av e-legitimation, men att det t.ex. i 6 § används en passivform "e-legitimation beviljas" utan att någon ansvarig aktör anges tydligt. Ämbetsverket ansåg att ansvaret för beviljande ska uttryckas konsekvent i alla paragrafer.

Transport- och kommunikationsverket förde fram flera behov av precisering. I yttrandet föreslogs det bl.a. att definitionerna bör förenhetligas med det första lagförslaget samt att användningen av termen "europeisk digital identitetsplånbok" i enlighet med eIDAS-förordningen bör preciseras. Ämbetsverket föreslog också att motiveringen förtydligas i fråga om den tekniska delen och att ansvarsfördelningen preciseras i 7 § när det gäller utlämnande av uppgifter och myndigheternas roller. Dessutom underströks det att eIDAS-förordningen och genomförandeförordningarna skapar förutsättningar för styrkande av identiteten innan attributsintyg beviljas och att den nationella regleringen inte får stå i strid med förordningen eller orsaka överlappningar. När det gäller 8 § ansåg ämbetsverket att det är oklart om det krävs en separat ansökan eller andra åtgärder av den sökande för att få attributsintyg från Myndigheten för digitalisering och befolkningsdata.

I remissvaret underströks behovet av att förtydliga regleringen om indragning av och giltighetens upphörande för e-legitimation och elektroniska attributsintyg samt att säkerställa att den är enhetlig och att administrationen är lätt. Myndigheten för digitalisering och befolkningsdata föreslog att grunderna för indragning enligt 10 § (t.ex. missbruk, äventyrande av säkerheten, användarens begäran) i fortsättningen omfattas av Myndigheten för digitalisering och befolkningsdatas behörighet när det gäller attributsintyg. Ämbetsverket betonade också att det finns ett behov av reglering om giltighetens upphörande för elektroniska attributsintyg och av en så enhetlig reglering som möjligt om båda företeelsernas livscykel.

Findynet Osuuskunta och TietoEVERY Abp ansåg att regleringen om giltighetens upphörande i 12 § behöver preciseras. Båda föreslog att det i paragrafen tydligt ska konstateras att myndigheten är skyldig att anteckna att intygets giltighet har upphört när villkoren uppfylls och att det att giltighetstiden löper ut antecknas som en uttrycklig orsak till giltighetens upphörande. TietoEVERY Abp föreslog därtill att giltighetens upphörande, indragning och avbrott hålls isär i regleringen, att tidpunkten för ikraftträdandet definieras, att bevislig delgivning till innehavaren säkerställs samt att information förmedlas till förlitande parter i realtid.

Transport- och kommunikationsverket ansåg att det är oklart hur indragning av elektroniska attributsintyg påverkar giltigheten för e-legitimationer och vice versa. Transport- och kommunikationsverket föreslog att det i 13 § ska föreskrivas om att giltigheten för ett attributsintyg upphör också när e-legitimationen dras in. Nordea Bank Abp förde fram en praktisk synvinkel om att giltigheten för en e-legitimation inte bör vara helt bunden till

giltigheten för ett pass eller identitetskort, utan att den bör fortsätta under en bestämd tid efter att handlingen blivit föråldrad. Vid den fortsatta beredningen har man stannat för att föreslå en sådan lösning.

Polisstyrelsen ansåg att användningen av e-legitimation som verktyg för att styrka identitet bör bekräftas också i annan lagstiftning och föreslog att det till autentiseringslagen fogas ett omnämnande av e-legitimationens lämplighet som verktyg för inledande identifiering. Dessutom bör det till 1 § i statsrådets förordning om pass och identitetskort fogas en bestämmelse om att e-legitimation kan användas som identifieringshandling vid ansökan om pass eller identitetskort. Polisstyrelsen underströk att om styrkande av identitet på annat håll i lagstiftningen begränsas till vissa handlingar, måste regleringen ändras så att e-legitimation godkänns som parallellt alternativ.

Polisstyrelsen förde också fram behovet av att se över de bestämmelser som hänvisar till autentiseringslagen och eIDAS-lagen. I yttrandet konstaterades det att det kan uppstå oklarheter när en del av den gällande regleringen flyttas till en annan lag. Exempelvis i 6 § 4 mom. finns det en hänvisning till ett identifieringsverktyg som definieras i autentiseringslagen. Eftersom regleringen om plånboken grundar sig på den reviderade eIDAS-förordningen uppfyller den inte villkoret i passlagen. Även om eIDAS-förordningen är direkt tillämplig EU-lagstiftning ansåg Polisstyrelsen att det är viktigt att hänvisningsbestämmelserna preciseras också i den nationella lagstiftningen. Dessutom bör hänvisningsbestämmelserna i de anslutande lagarna i regeringens proposition uppdateras när autentiseringslagens namn ändras. Polisstyrelsen lyfte också fram lagen om befolkningsdatasystemet, där det finns hänvisningar till autentiseringslagen i fråga om organisations- och medborgarcertifikat. Dessutom konstaterades det att man vid den fortsatta beredningen bör säkerställa att lagen om behandling av personuppgifter i polisens verksamhet är i överensstämmelse med de lagändringar som nu föreslås, i synnerhet när det gäller bestämmelserna om polisens rätt att få och lämna ut information.

Polisstyrelsen fäste uppmärksamhet vid att propositionsutkastet inte tar ställning till inom vilket geografiskt område myndigheterna kan behandla uppgifterna i e-legitimationer. Enligt propositionen är det möjligt att behandla uppgifter inom EU- och EES-området i enlighet med principen om fri rörlighet för uppgifter. Polisstyrelsen ansåg att detta inte är konsekvent i förhållande till bestämmelserna i passlagen och lagen om identitetskort, där det förutsätts att individualisering och kvalitetskontroll av handlingarna sker innanför Finlands gränser. Bestämmelsen i fråga har fogats till passlagen på initiativ av grundlagsutskottet och avsikten är att skydda uppgifter som är viktiga med tanke på den inre säkerheten, såsom fotografier och fingeravtryck. Polisstyrelsen konstaterade att en e-legitimation är en manifestation av ett pass eller identitetskort och att datainnehållet i stor utsträckning motsvarar den fysiska handlingen. Om behandling av uppgifterna i e-legitimationer tillåts inom ett större geografiskt område oimtetgörs bestämmelserna om datasäkerhet i passlagen och lagen om identitetskort. Inrikesministeriet underströk i sitt yttrande att den datamängd som det är fråga om är nationellt kritisk och att behandlingen av den är förknippad med särskilda säkerhetskrav. Vid den fortsatta beredningen har man stannat för att föreslå en lösning där regleringen följer passlagen och lagen om identitetskort och uppgifterna kan behandlas endast i Finland.

Myndigheten för digitalisering och befolkningsdata konstaterade att propositionsutkastet inte tar ställning till utrikesförvaltningens roll i beviljandet av e-legitimation, trots att Finlands beskickningar i utlandet beviljar pass och identitetskort. Ämbetsverket ansåg att det finns skäl att precisera regleringen till den del den handlar om hur finska medborgare som bor utomlands ska kunna ansöka om pass, identitetskort och e-legitimation samt hur styrningen och stödet i

anslutning till ansökan och ibruktagande ska ordnas. Suomi-Seura ry underströk att möjligheten att skaffa en europeisk e-legitimation också utomlands är viktig för utlandsfinländarna.

6.3 Remissvar om de ändringar som förbättrar säkerheten i den nationella starka autentiseringen

I yttrandena understöddes huvudsakligen de ändringar som främjar säkerheten i den nationella starka autentiseringen, och många av remissinstanserna ansåg att det är viktigt att försöka förbättra säkerheten.

På grundval av remissvaren har förslaget om att ge användaren möjlighet att förbjuda användningen av ett identifieringsverktyg för sammankopplad inledande identifiering strukits. I yttrandena betraktades förslaget som ineffektivt för att lösa problemet och nyttan ansågs obetydlig. Därtill bedömde remissinstanserna att ändringen kan orsaka betydande kostnader för tjänstetillhandahållarna.

Finlands Näringsliv rf föreslog i fråga om den föreslagna skyldigheten att kontrollera ett pass eller identitetskorts giltighet i polisens system ett reservarrangemang, för att tjänstetillhandahållarna ska kunna kontrollera en handling också t.ex. under systemstörningar. Avsikten med den föreslagna regleringen är att säkerställa aktuell information om en handlingens giltighet. Regleringen medför ingen skyldighet att använda ett gränssnitt utan giltigheten kan säkerställas elektroniskt också på annat sätt. Dessutom beaktas det i motiveringen att giltighetskontrollen vid exempelvis störningar i datakommunikationerna eller andra driftsavbrott kan göras också i efterhand. Således bedöms inrättandet av ett reservarrangemang inte medföra någon tilläggsnytta.

Dessutom önskade Transport- och kommunikationsverket kompletterande reglering när det gäller ibruktagande av ett identifieringsverktyg på en annan enhet när användaren redan har ett giltigt identifieringsverktyg. Propositionen innehåller förslag till nya bestämmelser om återaktivering av ett identifieringsverktyg. Dessutom innehåller den gällande lagen bestämmelser om beviljande, utlämnande och förnyande av identifieringsverktyg, där det på samma sätt som i fråga om den föreslagna återaktiveringen av identifieringsverktyg hänvisas till kraven i förordningen om tillitsnivåer. Förordningen om tillitsnivåer innehåller inga särskilda krav som gäller nytt ibruktagande på en annan enhet. Till denna del har inga ändringar gjorts i propositionen.

6.4 Utlåtande av rådet för bedömning av lagstiftningen

I utlåtandet konstateras det att de målgrupper som är viktigast med tanke på den föreslagna lagstiftningen har identifierats och att konsekvenserna har behandlats mångsidigt och huvudsakligen grundligt. I utlåtandet lyfts det fram att den föreslagna lagstiftningen kan omfatta sådana grupper av människor som kan behöva en assistent vid ibruktagande och användning av den digitala identitetsplånboken. Enligt utlåtandet skulle det vara bra att i förslaget förtydliga huruvida det är tillåtet t.ex. för en intressebevakare att använda en europeisk digital identitetsplånbok för en sådan persons räkning som inte själv kan använda den t.ex. på grund av funktionsnedsättning eller sjukdom. Vid den fortsatta beredningen har konsekvensbedömningen kompletterats med en beskrivning av hur elektronisk identifiering ska gå till i situationer med intressebevakning.

Rådet för bedömning av lagstiftningen ansåg i sitt utlåtande att det skulle vara bra att i förslaget lyfta fram dess möjliga positiva konsekvenser för sådana personer för vilka den digitala identitetsplånboken kan öppna upp möjligheter för stark autentisering i Finland utan att personer

behöver ha en kundrelation hos en finländsk bank eller en finländsk teleoperatör. Vid den fortsatta beredningen bedömdes det att den fråga som rådet lyfter fram redan i viss mån bedöms i avsnitt 4.2.3.1 i propositionen. Konsekvensbedömningen har emellertid kompletterats med en exempelförteckning över grupper av människor för vilka identifiering oberoende av kundrelationer särskilt kan ha positiva konsekvenser.

I utlåtandet ansågs det ytterligare att det behöver preciseras vilken nytta den föreslagna regleringen innebär t.ex. för företag som inte för närvarande kan tillhandahålla en plånbok, men som överväger att på längre sikt tillhandahålla konsumenterna en plånboksapplikation. Vid den fortsatta beredningen har konsekvensbedömningen i anslutning till konkurrensen mellan företag och marknadens funktion kompletterats med en beskrivning av nyttan för de aktörer som rådet för bedömning av lagstiftningen lyfte fram.

Utlåtandet innehöll ett förslag om att, om möjligt, spegla de i propositionen beskrivna alternativa handlingsvägarna mot de genomförandeåtgärder i anslutning till eIDAS-förordningen som används eller planeras i andra länder. Dessutom konstaterades det i utlåtandet att det i beskrivningen av andra länders genomförandeåtgärder skulle vara bra att lyfta fram hurdan nytta eller skada man har uppnått genom åtgärder eller andra motsvarande system och om det finns forskningsbaserad information om detta. Vid den fortsatta beredningen har det emellertid inte varit möjligt att göra de föreslagna kompletteringarna i fråga om genomförandeåtgärder i andra medlemsstater, eftersom det finns väldigt begränsat med information om dem. Medlemsstaterna vidtar åtgärder för att fullgöra skyldigheterna enligt den reviderade eIDAS-förordningen samtidigt i enlighet med varje medlemsstats egna administrativa processer och det är för alla medlemsstater fråga om ett utvecklingsarbete som tekniskt är av ny typ. Av den anledningen är det svårt att få tillgång till aktuell och forskningsbaserad information om hur verkställandet framskrider.

7 Specialmotivering

7.1 Lag om vissa tjänster som möjliggör gränsöverskridande e-tjänster

1 kap. Allmänna bestämmelser

1 §. Tillämpningsområde. Enligt propositionen föreskrivs det i paragrafen om tillämpningsområdet för lagen om vissa tjänster som möjliggör gränsöverskridande e-tjänster, dvs. eIDAS-lagen. Enligt *1 mom.* föreskrivs det i lagen om tillsynen över efterlevnaden av bestämmelserna i förordning (EU) Nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, sådan den lyder senast ändrad genom förordning (EU) 2024/1183, samt om bestämmelser som kompletterar förordningen i fråga.

Vid revideringen av eIDAS-förordningen var det inte fråga om en helhetsreform där den ursprungliga eIDAS-förordningen upphävdes och en ny förordning antogs i dess ställe. Däremot antogs en reviderad förordning (EU) 2024/1183, där en del av de befintliga artiklarna i eIDAS-förordningen ändrades och nya artiklar togs in i förordningen. Således är en del av de ursprungliga artiklarna i eIDAS-förordningen fortfarande giltiga i oförändrad form och den kompletterande nationella reglering som gäller dem behövs fortsättningsvis. Den nationella reglering som kompletterar eIDAS-förordningen har emellertid tidigare ingått i autentiseringslagen. Det föreslås att dessa bestämmelser flyttas från autentiseringslagen till denna lag, så att all nationell kompletterande reglering som gäller eIDAS-förordningen i fortsättningen finns i en och samma lag. Denna lag innehåller alltså bestämmelser både om sådant för vilket det har funnits och fortfarande finns ett behov av nationell reglering för

tillämpningen av den ursprungliga eIDAS-förordningen och om sådant som det behövs nationell reglering om för tillämpningen av den reviderade eIDAS-förordningen.

I 2 mom. föreskrivs det att lagen tillämpas endast på europeiska digitala identitetsplånböcker som tillhandahålls i Finland. Med europeisk digital identitetsplånbok som tillhandahålls i Finland avses en plånbok som tillhandahålls i Finland på något av de sätt som avses i artikel 5a.2 i eIDAS-förordningen. Enligt artikeln i fråga kan plånböcker tillhandahållas direkt av en medlemsstat, på uppdrag av en medlemsstat eller oberoende av en medlemsstat men med den medlemsstatens erkännande. I praktiken kan en europeisk digital identitetsplånbok alltså tillhandahållas av den offentliga sektorn, men också av den privata sektorn så att plånboken är erkänd i Finland. I den föreslagna 33 § föreskrivs det att Transport- och kommunikationsverket har till uppgift att anmäla europeiska digitala identitetsplånböcker som tillhandahålls i Finland. En plånbok betraktas som erkänd och tillhandahållen i Finland när Transport- och kommunikationsverket har gjort anmälan i fråga till Europeiska kommissionen. Enligt bestämmelsen tillämpas lagen således inte på europeiska digitala identitetsplånböcker som tillhandahålls av någon annan medlemsstat. Exempelvis bestämmelserna om åldersgränsen för ibruktage av plånboken eller eventuell avgift för elektronisk underskrift med plånboken tillämpas inte på plånböcker som tillhandahålls av en annan medlemsstat. Bestämmelsen begränsar emellertid inte möjligheten att i Finland använda plånböcker som tillhandahålls av andra medlemsstater.

I 3 mom. föreskrivs det att på gränsöverskridande system för elektronisk identifiering som ska anmälas till Europeiska kommissionen tillämpas autentiseringslagen, om inte något annat följer av denna lag eller eIDAS-förordningen. I eIDAS-förordningen föreskrivs det också i fortsättningen om de tre tillitsnivåerna för elektronisk identifiering (låg, väsentlig och hög) och i förordningen om tillitsnivåer för elektronisk identifiering specificeras kraven på system för elektronisk identifiering på olika tillitsnivåer. System för elektronisk identifiering ska uppfylla något krav som gäller tillitsnivån för att identifieringssystemen i fråga ska kunna anmälas till Europeiska kommissionen för gränsöverskridande bruk. Bestämmelser om anmälandet finns i artikel 9 i eIDAS-förordningen och enligt den ska den anmälande medlemsstaten anmäla exempelvis uppgifter om det tillämpliga systemet för tillsyn och information om systemet för skadeståndsansvar.

Det har bestämts att kraven på nationella identifieringsverktyg för stark autentisering ska harmoniseras med kraven enligt tillitsnivån väsentlig som avses i eIDAS-förordningen. Med detta avses att nationella identifieringsverktyg för stark autentisering förutsätts uppfylla minst kraven enligt tillitsnivån väsentlig. I Finland tillhandahålls emellertid också identifieringsverktyg som uppfyller kraven enligt tillitsnivån hög. Avsikten med att harmonisera kraven var att göra det lättare för aktörer inom stark autentisering i Finland att för sitt eget identifieringsverktyg ansöka om ställning som så kallat gränsöverskridande identifieringsverktyg (RP 74/2016 rd, s. 12). Bestämmelser om dessa krav finns i autentiseringslagen. Till denna del är det dock inte fråga om reglering som kompletterar eIDAS-förordningen och som ska ingå i den föreslagna eIDAS-lagen, utan om reglering av den nationella starka autentiseringen. När kraven emellertid har harmoniserats med kraven enligt tillitsnivån väsentlig i eIDAS-förordningen och regleringen i autentiseringslagen således innehåller alla de element som förutsätts när ett elektroniskt identifieringssystem anmäls enligt eIDAS-förordningen, ska tillhandahållaren av identifieringstjänsten tillämpa regleringen i autentiseringslagen vid tillhandahållande av sitt identifieringsverktyg om tillhandahållaren vill anmäla identifieringsverktyget i enlighet med eIDAS-förordningen.

2 §. Definitioner. Enligt förslaget föreskrivs det i paragrafen om de centrala definitioner som används i lagen. Definitionerna motsvarar till vissa delar definitionerna i den reviderade eIDAS-förordningen.

I 1 punkten definieras europeisk digital identitetsplånbok. Med detta avses detsamma som med den europeiska digitala identitetsplånbok som definieras i artikel 3.42 i den reviderade eIDAS-förordningen. Enligt artikeln i fråga avser detta ett medel för elektronisk identifiering som gör det möjligt för användaren att på ett säkert sätt lagra, hantera och validera personidentitetsuppgifter och elektroniska attributsintyg i syfte att tillhandahålla dem till förlitande parter och andra användare av europeiska digitala identitetsplånböcker, och att underteckna med kvalificerade elektroniska underskrifter eller att stämpla med kvalificerade elektroniska stämplat.

I 2 punkten definieras identifieringsuppgifter för personer. Dessa avser i enlighet med artikel 3.3 i den reviderade eIDAS-förordningen uppgifter som gör det möjligt att fastställa identiteten på en fysisk eller juridisk person eller på en fysisk person som företräder en annan fysisk person eller en juridisk person. Uppgifter för personidentifiering har i fråga om elektroniska identifieringssystem definierats i bilagan till kommissionens genomförandeförordning (EU) 2015/1501 och i fråga om den europeiska digitala identitetsplånboken i bilagan till kommissionens genomförandeförordning (EU) 2024/2977. Identifieringsuppgifter för personer indelas i obligatoriska och frivilliga uppgifter för personidentifiering. I plånboken är obligatoriska identifieringsuppgifter för en fysisk person personens nuvarande förnamn, nuvarande efternamn, födelsedatum och födelseort samt nationalitet.

I 3 punkten definieras förlitande part. Med det avses i enlighet med artikel 3.6 i den reviderade eIDAS-förordningen en fysisk eller juridisk person som förlitar sig på elektronisk identifiering, europeiska digitala identitetsplånböcker eller andra medel för elektronisk identifiering eller på en betrodd tjänst. Förlitande parter är t.ex. e-tjänster inom den offentliga eller den privata sektorn, där den europeiska digitala identitetsplånboken kan utnyttjas för identifiering av kunder i tjänsten.

I 4 punkten definieras nationell nod. Detta avser i enlighet med kommissionens genomförandeförordning (EU) 2015/1501 en förbindelsepunkt som utgör en del av den interoperativa arkitekturen för elektronisk identifiering och som medverkar vid gränsöverskridande autentisering av personer och som har förmågan att känna igen och behandla eller vidarebefordra överföringar till andra noder genom att bringa den nationella elektroniska identifieringsinfrastrukturen i en medlemsstat i kontakt med nationella elektroniska identifieringsinfrastrukturer i andra medlemsstater. Med nationell nod avses i praktiken alltså ett nationellt gränssnitt genom vilket identifieringstransaktioner som föreskrivs i eIDAS-förordningen förmedlas mellan Finland och andra länder. Den nationella noden upprätthålls enligt den föreslagna 19 § av Myndigheten för digitalisering och befolkningsdata.

Med organ för bedömning av överensstämmelse avses i enlighet med 5 punkten de organ för bedömning av överensstämmelse som avses i artikel 3.18 i eIDAS-förordningen och de certifieringsorgan som avses i de bestämmelser som utfärdats med stöd av artikel 5 c. Enligt artikel 3.18 i eIDAS-förordningen avses med organ för bedömning av överensstämmelse ett organ enligt definitionen i artikel 2.13 i förordning (EG) nr 765/2008 som i enlighet med den förordningen är ackrediterat för överensstämmelsebedömning av en kvalificerad tillhandahållare av en betrodd tjänst och den kvalificerade betrodda tjänst som denne tillhandahåller eller för att certifiera europeiska digitala identitetsplånböcker eller medel för elektronisk identifiering. Enligt artikel 2.9 i den genomförandeförordning som antagits med stöd av artikel 5c.6 i eIDAS-förordningen, dvs. förordningen om certifiering av plånböcker

avses med ett certifieringsorgan ett externt organ för bedömning av överensstämmelse som ansvarar för certifieringsordningens funktion. I praktiken avses med organ för bedömning av överensstämmelse ett organ som Transport- och kommunikationsverket utser med stöd av 26 § och anmäler till kommissionen och som ackrediterats vara behörig att bedöma överensstämmelse av en kvalificerad tillhandahållare av en betrodd tjänst och den betrodda tjänst som denne tillhandahåller eller att certifiera europeiska digitala identitetsplånböcker eller metoder för elektronisk identifiering.

Med teknisk utrustning avses enligt 6 punkten en mobil enhet eller annan motsvarande utrustning som användaren av den europeiska digitala identitetsplånboken innehar och i vilken plånboken har tagits i bruk. I praktiken kan det vara fråga om exempelvis en mobiltelefon eller en pekplatta.

2 kap. Europeisk digital identitetsplånbok och medel för elektronisk identifiering

3 §. Utfärdande av identifieringsuppgifter för fysiska personer. Enligt förslaget föreskrivs det i paragrafen om utfärdande av identifieringsuppgifter för fysiska personer. Identifieringsuppgifter för personer definieras i 2 § 2 punkten. Uppgifter för personidentifiering definieras i fråga om den europeiska digitala identitetsplånboken närmare i bilagan till kommissionens genomförandeförordning (EU) 2024/2977. I plånboken är obligatoriska identifieringsuppgifter för en fysisk person personens nuvarande förnamn, nuvarande efternamn, födelsedatum och födelseort samt nationalitet. Regleringen behövs för genomförande av de skyldigheter för medlemsstaterna som anges i artikel 5a i den reviderade eIDAS-förordningen och i kommissionens genomförandeförordning (EU) 2024/2977, som antagits med stöd av den. I genomförandeförordningen definieras tillhandahållare av personidentifieringsuppgifter och enligt definitionen ansvarar tillhandahållaren för att utfärda och återkalla personidentifieringsuppgifter och säkerställa att en användares personidentifieringsuppgifter är kryptografiskt bundna till en plånboksenhet.

Enligt 1 mom. utfärdas identifieringsuppgifter för fysiska personer av Myndigheten för digitalisering och befolkningsdata. I praktiken är alltså Myndigheten för digitalisering och befolkningsdata i fråga om identifieringsuppgifter för fysiska personer den tillhandahållare av personidentifieringsuppgifter som avses i kommissionens genomförandeförordning (EU) 2024/2977. När det gäller uppgifter för personidentifiering handlar det i praktiken, på det sätt som beskrivs ovan, om basuppgifter om personens identitet. I Finland betraktas befolkningsdatasystemet som ett register över basuppgifter om personer, och det är ändamålsenligt att de identifieringsuppgifter för fysiska personer som utfärdas för europeiska digitala identitetsplånböcker som tillhandahålls från Finland bygger på uppgifterna i befolkningsdatasystemet. Eftersom Myndigheten för digitalisering och befolkningsdata är personuppgiftsansvarig för befolkningsdatasystemet är det motiverat att myndigheten också utfärdar identifieringsuppgifter för fysiska personer. I praktiken innebär detta att en förutsättning för att identifieringsuppgifter för fysiska personer ska utfärdas är att personen är registrerad i befolkningsdatasystemet. Bestämmelser om utfärdande av identifieringsuppgifter för juridiska personer finns i 5 §.

Utfärdande av identifieringsuppgifter för fysiska personer för plånböcker förutsätter att användaren har installerat en applikation för en europeisk digital identitetsplånbok på en teknisk utrustning, t.ex. en telefon, och att applikationen har aktiverats så att det går att ladda ner identifieringsuppgifterna för personen och andra uppgifter. I praktiken erhålls identifieringsuppgifterna för personen så att användaren startar ibruktagandet av identifieringsuppgifter i applikationen. Myndigheten för digitalisering och befolkningsdata begär i egenskap av tillhandahållare av identifieringsuppgifter för fysiska personer via

plånboken användaren att identifiera sig i enlighet med villkoren för säkerhetsnivån hög. Efter en godkänd identifiering utfärdar myndigheten identifieringsuppgifterna. Identifieringsuppgifter för personer kan utfärdas också på ett serviceställe med assistans av en tjänsteperson. Användaren ska då styrka sin identitet för tjänstepersonen med en handling som styrker identiteten, såsom pass, identitetskort eller en jämförbar handling. Tjänstepersonen ska på ett tillförlitligt sätt länka samman användaren, den handling som styrker användarens identitet och användarens europeiska digitala identitetsplånbok. Användaren får till sin europeiska digitala identitetsplånbok information om att identifieringsuppgifterna för person har utfärdats.

I 2 mom. föreskrivs det om möjligheterna för en användare av en europeisk digital identitetsplånbok att ansöka om identifieringsuppgifter för en fysisk person genom ett besök hos en finsk beskickning eller Statens ämbetsverk på Åland. Det är fråga om en sådan situation som beskrivs ovan när identifieringsuppgifter för en person utfärdas med assistans av en tjänsteperson vid ett serviceställe. Med finländska beskickningar avses de ambassader, legationer, generalkonsulat, konsulat, vicekonsulat och konsularagenturer som räknas upp i 9 § 1 mom. i lagen om konsulära tjänster (498/1999). Myndigheten för digitalisering och befolkningsdata utfärdar också i dessa situationer identifieringsuppgifter för fysiska personer, men den finländska beskickningen eller Statens ämbetsverk på Åland identifierar personerna och tar emot de uppgifter som behövs för utfärdande av identifieringsuppgifter samt registrerar dem i det system som Myndigheten för digitalisering och befolkningsdata använder vid utfärdande av identifieringsuppgifter för fysiska personer. Den finländska beskickningen eller Statens ämbetsverk på Åland ansvarar för att de uppgifter som registreras där är tillförlitliga och korrekta. Det är fråga om en mycket begränsad och till karaktären assisterande uppgift i processen för utfärdande av identifieringsuppgifter för fysiska personer.

Enligt 3 mom. ska Myndigheten för digitalisering och befolkningsdata utfärda identifieringsuppgifter för fysiska personer för sådana europeiska digitala identitetsplånböcker som Transport- och kommunikationsverket har anmält till Europeiska kommissionen i enlighet med 33 §. De plånböcker för vilka anmälan i fråga har gjorts anses vara plånböcker som tillhandahållits från Finland. Enligt artikel 5a.2 i den reviderade eIDAS-förordningen kan en europeisk digital identitetsplånbok tillhandahållas direkt av en medlemsstat, på uppdrag av en medlemsstat eller oberoende av en medlemsstat men med den aktuella medlemsstatens erkännande. I praktiken är utfärdandet av identifieringsuppgifter för fysiska personer alltså knutet till att plånboken har anmälts till kommissionen.

Enligt 3 mom. kan Myndigheten för digitalisering och befolkningsdata utfärda identifieringsuppgifter för fysiska personer också för andra än i Finland tillhandahållna europeiska digitala identitetsplånböcker. Myndigheten för digitalisering och befolkningsdata har ändå inte någon skyldighet till detta. Med andra europeiska digitala identitetsplånböcker avses i praktiken plånböcker som tillhandahålls av andra EU-medlemsstater. Myndigheten för digitalisering och befolkningsdata offentliggör emellertid en förteckning över alla europeiska digitala identitetsplånböcker som den stöder i egenskap av tillhandahållare av identifieringsuppgifter för fysiska personer. Enligt artikel 3.6 i kommissionens genomförandeförordning (EU) 2024/277, som antagits med stöd av artikel 5a i den reviderade eIDAS-förordningen ska medlemsstaterna offentliggöra en förteckning över plånbokslösningar som stöds av tillhandahållare av personidentifieringsuppgifter som ingår i den medlemsstatens system för elektronisk identifiering. I momentet föreskrivs det att denna skyldighet är en uppgift för Myndigheten för digitalisering och befolkningsdata. Detta innebär att Myndigheten för digitalisering och befolkningsdata ska upprätthålla en förteckning över de tillhandahållare av plånböcker som den i egenskap av tillhandahållare av identifieringsuppgifter för fysiska personer godkänner.

4 §. Registret över identifieringsuppgifter för fysiska personer. Paragrafen föreslås innehålla bestämmelser om ett register i anslutning till utfärdandet av identifieringsuppgifter för fysiska personer, som Myndigheten för digitalisering och befolkningsdata för i anslutning till sin uppgift enligt 3 § att utfärda identifieringsuppgifter för fysiska personer. Rättsgrunden för behandling av personuppgifter i anslutning till registerföringen är artikel 6.1 c i dataskyddsförordningen, där det anges att behandlingen av personuppgifter i situationer som avses där är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Artikel 5a.4 led a i den reviderade eIDAS-förordningen förutsätter att användaren på olika sätt ska kunna hantera uppgifter för personidentifiering med den europeiska digitala identitetsplånboken. Enligt artikel 3.1 i kommissionens genomförandeförordning (EU) 2024/2977, som antagits med stöd av artikel 5a i den reviderade eIDAS-förordningen ska tillhandahållare av personidentifieringsuppgifter utfärda personidentifieringsuppgifter för plånboksenheter samt i enlighet med artikel 5 möjliggöra återkallande av personidentifieringsuppgifter. I bilagan till kommissionens genomförandeförordning (EU) 2024/2977 föreskrivs det om obligatoriska personidentifieringsuppgifter för fysiska personer som varje medlemsstat ska tillhandahålla för europeiska digitala identitetsplånböcker samt frivilliga personidentifieringsuppgifter som medlemsstaterna tillhandahåller enligt eget övervägande. Ovan i 3 § föreskrivs det som komplettering till den reviderade eIDAS-förordningen att Myndigheten för digitalisering och befolkningsdata utfärdar identifieringsuppgifter för fysiska personer för europeiska digitala identitetsplånböcker. Således bildar den reviderade eIDAS-förordningen, kommissionens genomförandeförordning som antagits med stöd av förordningen och den kompletterande nationella lagstiftningen tillsammans en rättslig förpliktelse som åvilar Myndigheten för digitalisering och befolkningsdata.

Enligt 1 mom. införs i registret de uppgifter som behövs för utfärdande, giltighet, uppdatering och återkallande avseende identifieringsuppgifter för fysiska personer med beaktande av artikel 5a i eIDAS-förordningen och de bestämmelser som utfärdats med stöd av den. I registret införs t.ex. en individualiserande uppgift om utfärdade personidentifieringsuppgifter, en individualiserande uppgift om den europeiska digitala identitetsplånbok för vilken uppgifterna har utfärdats samt användarens kontaktinformation. I registret införs dessutom uppgifter om status för identifieringsuppgifterna för en fysisk person, dvs. uppgift om huruvida identifieringsuppgifterna är giltiga. I registret införs också uppgift om huruvida personidentifieringsuppgifterna har återkallats.

I 2 mom. föreskrivs det om bevaringstiden för uppgifterna i registret över identifieringsuppgifter för fysiska personer. Uppgifterna i anslutning till identifieringsuppgifter för fysiska personer bevaras så länge som uppgifterna är giltiga. När identifieringsuppgifterna har upphört att gälla bevaras de i ytterligare fem år. Det kan vara nödvändigt att i efterhand verifiera t.ex. för vilken europeisk digital identitetsplånbok identifieringsuppgifterna för en fysisk person har tagits i bruk och vilket innehållet i de utfärdade identifieringsuppgifterna har varit. Verifiering av dessa uppgifter kan vara nödvändigt, t.ex. för att det ska kunna utredas om rätt person har tagit i bruk den europeiska digitala identitetsplånboken eller om plånboken är i rätt persons besittning.

5 §. Utfärdande av identifieringsuppgifter för juridiska personer. Enligt förslaget föreskrivs det i paragrafen om utfärdande av identifieringsuppgifter för juridiska personer. Enligt paragrafen har Patent- och registerstyrelsen rätt att utfärda identifieringsuppgifter för juridiska personer för europeiska digitala identitetsplånböcker. Formuleringen avviker från det förslag som gäller identifieringsuppgifter för fysiska personer så till vida att regleringen möjliggör utfärdande av identifieringsuppgifter för juridiska personer. Det är ännu osäkert om det kommer att skapas europeiska digitala identitetsplånböcker för juridiska personer. Patent- och registerstyrelsen ges som ny uppgift att enligt 3.3 i eIDAS-förordningen utfärda identifieringsuppgifter för juridiska personer, om sådana tillhandahålls i framtiden. I fråga om innehållet i identifieringsuppgifterna

ska Patent- och registerstyrelsen följa det som föreskrivs i kommissionens genomförandeförordning (EU) 2024/2977. Identifieringsuppgifterna för juridiska personer definieras i punkt 2 i bilagan till genomförandeförordningen och de ska alltid innehålla minst den juridiska personens juridiska namn och en unik identifieringskod. Dessutom kan identifieringsuppgifterna innehålla valfria element.

Identifieringsuppgifterna förs inte in i handelsregistret eller i företags- och samfundsdatasystemet och uppgifterna är således inte allmänt offentliga på motsvarande sätt som uppgifter som gäller de ovannämnda registren. Samtidigt föreskrivs det inte att identifieringsuppgifterna för juridiska personer är sekretessbelagda. Det ska dock noteras att om eIDAS-förordningen eller genomförandeförordningen medför krav som gäller identifieringsuppgifternas offentlighet eller utlämnandet av uppgifterna, ska dessa iakttas.

Patent- och registerstyrelsen får inte i uppgift att tillhandahålla en europeisk digital identitetsplånbok och det föreskrivs inte heller något annat om tillhandahållande av plånböcker i fråga om juridiska personer. Detta blir en uppgift som ska genomföras av privata aktörer. Ett villkor för utfärdande av identifieringsuppgifter är emellertid att den juridiska personen har en plånbok som identifieringsuppgifterna kan kopplas till.

I 2 mom. föreskrivs det om ansökan om identifieringsuppgifter och om de villkor som gäller juridiska personer. Identifieringsuppgifter utfärdas inte å tjänstens vägnar, utan erhållandet förutsätter en ansökan från den juridiska personen. I fråga om ansökan tillämpas bestämmelserna om att företräda en juridisk person, och inte t.ex. vad som i företags- och organisationsdatalagen (244/2001) föreskrivs om att göra anmälan till handelsregistret. När det gäller sökande av ändring i beslut som fattats om ansökan tillämpas vad som föreskrivs i lagen om Patent- och registerstyrelsen (578/2013). För handläggning av ansökan påförs en avgift i enlighet med lagen om avgifter för patent- och registerstyrelsens prestationer (1032/1992).

Identifieringsuppgifter för juridiska personer kan utfärdas endast för juridiska personer som är införda i handelsregistret. När det gäller ett företag eller samfund som är infört i handelsregistret kan det ur registret fås uppgifter bl.a. om dem som har rätt att företräda företaget eller samfundet och om den juridiska personens status, såsom likvidation eller konkurs. Några hundra föreningar och stiftelser är införda i handelsregistret på den grunden att de bedriver näringsverksamhet. I handelsregistret införs emellertid inte föreningars och stiftelsers ansvarspersoner, utan de framgår endast av förenings- och stiftelseregistret. Med hänsyn till att utfärdandet av identifieringsuppgifter i detta skede inte omfattar förenings- och stiftelseregistret utesluts också sådana föreningar och stiftelser från lagens tillämpningsområde som ingår förutom i förenings- och stiftelseregistret även i handelsregistret. Eftersom kravet är att det ska vara fråga om en juridisk person, är det inte möjligt att med en bifirma som är införd i handelsregistret få identifieringsuppgifter, i och med att det är fråga om en utländsk juridisk persons bifirma som inte är en självständig juridisk person. Identifieringsuppgifter ska inte heller utfärdas för utländska juridiska personer. Likaså utesluts privata näringsidkare som inte är juridiska personer från lagens tillämpningsområde. Med hänsyn till hur avgränsade de införda uppgifterna är utfärdas identifieringsuppgifter inte heller till samfund som betraktas som juridiska personer och som är registrerade endast i företags- och organisationsdatasystemet. I företags- och organisationsdatasystemet införs exempelvis inte ansvarspersoner.

Det behövs ingen separat reglering om återkallande av juridiska personers identifieringsuppgifter, utan till den delen tillämpar Patent- och registerstyrelsen vad som föreskrivs i eIDAS-förordningen och genomförandeförordningen (EU) 2024/2977, särskilt i artikel 5.

I 3 mom. föreskrivs det på motsvarande sätt som i 3 § om utfärdande av identifieringsuppgifter för fysiska personer om att Patent- och registerstyrelsen gör en förteckning över alla europeiska digitala identitetsplånböcker som den stöder i egenskap av tillhandahållare av identifieringsuppgifter för juridiska personer.

I 4 mom. föreskrivs det om utlämnande av personuppgifter som framgår av en ansökan om identifieringsuppgifter. Det ska inte anses finnas ett likadant behov för allmän offentlighet för denna typ av personuppgifter som för exempelvis de ansvarspersoner som är införda i det handelsregister som Patent- och registerstyrelsen för. Således föreskrivs det i 4 mom. att Patent- och registerstyrelsen får lämna ut personuppgifter om fysiska personer som framgår av en ansökan som avses i 2 mom. till andra än företrädare för den juridiska personen med iakttagande av vad som i 2 § 2 mom. i handelsregisterlagen (564/2023) föreskrivs om utlämnande av en i handelsregistret införd personbetecknings slutled och en utomlands bosatt fysisk persons hemadress. I 2 § 2 mom. i handelsregisterlagen föreskrivs det att registermyndigheten får lämna ut i handelsregistret införda uppgifter om personbeteckningens slutled och en utomlands bosatt fysisk persons hemadress endast om mottagaren har en sådan grund för behandling av uppgifter som avses i 29 § i dataskyddslagen. Sådana uppgifter får också på det sätt som föreskrivs i 1 mom. lämnas ut elektroniskt i ett krypterat eller på annat sätt skyddat format. En förutsättning är dessutom att den som begär uppgifterna lämnar registermyndigheten en redogörelse för att uppgifterna skyddas på behörigt sätt. När det gäller personuppgifter som framgår av ansökan tillämpas de villkor som anges i 2 § 2 mom. i handelsregisterlagen på alla personuppgifter som framgår av ansökan, inte bara på personbeteckningens slutled eller hemadressen. Företrädare för den juridiska person som har gjort ansökan har emellertid rätt att få uppgifterna utan grund enligt 29 § i dataskyddslagen.

6 §. Registret över identifieringsuppgifter för juridiska personer. Den föreslagna paragrafen motsvarar det som föreslås i 4 § om registret över identifieringsuppgifter för fysiska personer, men Patent- och registerstyrelsen är personuppgiftsansvarig i fråga om identifieringsuppgifterna för juridiska personer. Enligt 1 mom. för Patent- och registerstyrelsen register över de identifieringsuppgifter för juridiska personer som den har utfärdat. I registret införs de uppgifter som behövs för utfärdande, giltighet, uppdatering och återkallande avseende identifieringsuppgifter för juridiska personer med beaktande av artikel 5a i eIDAS-förordningen och de bestämmelser som utfärdats med stöd av den. Sådana uppgifter som ska införas i registret kan i fråga om identifieringsuppgifter för juridiska personer vara exempelvis företagets FO-nummer, den sökande och dennes personbeteckning och ställning, åtgärder som myndigheten vidtagit och individualiseringsuppgifter för plånboken. Även andra nödvändiga uppgifter kan införas i registret. Enligt 2 mom. bevaras identifieringsuppgifter för juridiska personer som införts i registret fem år efter att giltigheten för den juridiska personens identifieringsuppgifter har upphört. Regleringen motsvarar till innehållet det som föreslås om bevarande av identifieringsuppgifter för fysiska personer.

7 §. Tillhandahållande av europeiska digitala identitetsplånböcker. Enligt förslaget föreskrivs det i 1 mom. att Myndigheten för digitalisering och befolkningsdata har till uppgift att tillhandahålla europeiska digitala identitetsplånböcker. Det är fråga om tillhandahållande av en plånbok som används av fysiska personer. Myndigheten för digitalisering och befolkningsdata ska tillämpa kraven i språklagen när den tillhandahåller europeiska digitala identitetsplånböcker och således tillhandahålls plånboken också på svenska. Myndigheten för digitalisering och befolkningsdata åläggs uppgiften att tillhandahålla plånböckerna av den anledningen att en utredning som finansministeriet har låtit göra visar att verksamheten på marknaden för europeiska digitala identitetsplånböcker under de närmaste åren bedöms vara bristfällig. Med detta avses att sedvanlig marknadsverksamhet saknas och att det inte inom utsatt tid kommer att finnas ett utbud på plånböcker som uppfyller kraven enligt den reviderade eIDAS-

förordningen (*marknadsbrist*). I Finland säkerställs det alltså att skyldigheten enligt artikel 5a.1 i den reviderade eIDAS-förordningen att tillhandahålla en nationell europeisk digital identitetsplånbok fullgörs genom att Myndigheten för digitalisering och befolkningsdata i lag åläggs uppgiften att producera en europeisk digital identitetsplånbok. Det är möjligt att följa utvecklingen på marknaden och den fortgående marknadsbristen utifrån information om vilka plånböcker Transport- och kommunikationsverket har anmält till Europeiska kommissionen med stöd av 33 § 2 punkten i den föreslagna eIDAS-lagen. Avsikten med propositionen är inte att avvika från den i 4 a kap. i konkurrenslagen föreskrivna rätten för Konkurrens- och konsumentverket att ingripa i ett förfarande eller en verksamhetsstruktur som tillämpas i den ekonomiska verksamhet som bedrivs av en kommun, en samkommun, ett välfärdsområde, en välfärdssammanslutning eller staten, eller av en enhet som de har bestämmande inflytande över.

I 2 mom. föreskrivs det att också andra aktörer kan producera plånböcker som avses i 1 mom. Enligt paragrafen begränsar bestämmelserna i 1 mom. inte andra myndigheters eller juridiska eller fysiska personers möjligheter att tillhandahålla europeiska digitala identitetsplånböcker. eIDAS-förordningen möjliggör också plånböcker som producerats av andra aktörer. Vid beredningen av propositionen har det bedömts att om aktörer inom den privata sektorn vill tillhandahålla europeiska digitala identitetsplånböcker ska detta inte regleras genom lag på det sätt som avses i 124 § i grundlagen. Grundlagsutskottet har i sin utlåtandepraxis ansett att karaktären av de affärsekonomiska tjänster som avses i autentiseringslagen till den grad har distanserat sig från karakteristika som gäller för offentliga myndighetsuppdrag, att verksamheten inte längre kan betraktas som en offentlig förvaltningsuppgift trots att verktygen för stark elektronisk autentisering och certifiering har betydelse för parternas ställning i olika typer av rättshandlingar (GrUU 16/2009 rd, s. 2). Som det beskrivs ovan under propositionens konsekvenser för konkurrensrätten är funktionerna i den europeiska digitala identitetsplånboken motsvarande som i den starka autentisering och kvalificerade elektroniska underskrift som redan är tillgängliga på marknaden. Om andra aktörer i framtiden tillhandahåller plånböcker ska de uppfylla villkoren i eIDAS-förordningen och den föreslagna eIDAS-lagen.

I 3 mom. föreskrivs det om anmälningsskyldighet för tillhandahållare av europeiska digitala identitetsplånböcker. Med tillhandahållare avses den som tillhandahåller en europeisk digital plånbok i Finland på något av de sätt som avses i artikel 5a.2 i eIDAS-förordningen. Den reviderade eIDAS-förordningen definierar inte tillhandahållare av plånböcker, utan dessa definieras i kommissionens genomförandeförordningar som kompletterar förordningen. En tillhandahållare av en europeisk digital identitetsplånbok ska innan den börjar tillhandahålla plånboken göra en anmälan till Transport- och kommunikationsverket. Anmälningsskyldigheten behövs, eftersom Transport- och kommunikationsverket enligt den föreslagna 33 § 2 punkten informerar Europeiska kommissionen och den samarbetsgrupp som inrättats i enlighet med artikel 46e.1 i den reviderade eIDAS-förordningen om europeiska digitala identitetsplånböcker som i enlighet med artikel 5a tillhandahållits i Finland. Anmälan till Transport- och kommunikationsverket är i praktiken en anmälan om att aktören har för avsikt att börja tillhandahålla en europeisk digital identitetsplånbok. På basis av anmälan kan Transport- och kommunikationsverket innan tillhandahållandet av plånboken inleds säkerställa att tillhandahållaren och plånboken uppfyller kraven i den reviderade eIDAS-förordningen.

De uppgifter som ska anmälas anges detaljerat i 5a.18 b och 5d i eIDAS-förordningen samt i kommissionens genomförandeförordningar (EU) 2024/2980 och (EU) 2025/849 som antagits med stöd av artiklarna. De uppgifter som avses i dessa punkter i förordningen är t.ex. organ som ansvarar för tillhandahållande av europeiska digitala identitetsplånböcker samt certifikat för certifierade europeiska digitala identitetsplånböcker och rapporter om certifieringsbedömning, beskrivningar av det system för elektronisk identifiering där plånboken tillhandahålls samt om det tillsynssystem som tillämpas. I momentet finns emellertid ingen direkt hänvisning till

förordningarna i fråga, eftersom kommissionen har uttryckt att den eventuellt ändrar förordningarna under de närmaste åren. Därför hänvisas det i momentet bara till artiklarna i eIDAS-förordningen och den reglering som antagits med stöd av dem.

Enligt det föreslagna 4 mom. ska tillhandahållaren av en europeisk digital identitetsplånbok utan dröjsmål underrätta Transport- och kommunikationsverket om ändringar i de uppgifter som avses i 3 mom. Transport- och kommunikationsverket får utfärda närmare föreskrifter om hur de uppgifter som avses i 2 och 3 mom. ska lämnas.

8 §. Personuppgiftsansvarig för den europeiska digitala identitetsplånbok som Myndigheten för digitalisering och befolkningsdata tillhandahåller. Enligt förslaget föreskrivs det i paragrafen att Myndigheten för digitalisering och befolkningsdata är personuppgiftsansvarig för den europeiska digitala identitetsplånbok som myndigheten tillhandahåller med stöd av 7 § och för behandlingen av personuppgifter i samband med tillhandahållandet av plånboken. Rättsgrunden för behandlingen av personuppgifter i samband med tillhandahållandet av plånboken är artikel 6.1 c i dataskyddsförordningen, som anger att behandling av personuppgifter i en situation enligt ledet är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Artikel 5a.1 i den reviderade eIDAS-förordningen förutsätter att varje medlemsstat tillhandahåller en plånbok som uppfyller kraven i förordningen. Ovan i 7 § föreskrivs det som komplettering till den reviderade eIDAS-förordningen att Myndigheten för digitalisering och befolkningsdata har till uppgift att tillhandahålla en europeisk digital identitetsplånbok i Finland. Således bildar den reviderade eIDAS-förordningen och den kompletterande nationella lagstiftningen tillsammans en rättslig förpliktelse som åvilar Myndigheten för digitalisering och befolkningsdata.

Myndigheten för digitalisering och befolkningsdata tillhandahåller alltså med stöd av den föreslagna 7 § en plånbok i enlighet med den reviderade eIDAS-förordningen. Tillhandahållandet av plånboken går ut på att erbjuda en applikation som användaren laddar ner på sin mobila enhet samt att genomföra de system och tjänster som tillhandahållandet av applikationen förutsätter. I praktiken leder tillhandahållandet av plånboken till att det vid Myndigheten för digitalisering och befolkningsdata uppkommer flera nya register som innehåller personuppgifter och som förutsätter att dessa behandlas. Myndigheten för digitalisering och befolkningsdata ska exempelvis föra ett register över plånboksenheter som innehåller uppgifter om plånboksinstanserna i den plånbok som myndigheten tillhandahåller.

Det är med stöd av dataskyddsförordningen möjligt att föreskriva om den personuppgiftsansvarige. Med personuppgiftsansvarig avses enligt artikel 4.7 i dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt. I paragrafen föreslås det en uttrycklig bestämmelse om att Myndigheten för digitalisering och befolkningsdata är personuppgiftsansvarig för den europeiska digitala identitetsplånbok som myndigheten tillhandahåller och för registren i anslutning till tillhandahållandet av plånboken. Regleringen behövs för att inget ska bli oklart i fråga om personuppgiftsansvaret när hänsyn tas särskilt till principerna om plånbokens funktioner och till användarens rättigheter.

Ställningen för Myndigheten för digitalisering och befolkningsdata som personuppgiftsansvarig begränsar inte vad som i den reviderade eIDAS-förordningen föreskrivs om plånbokens användares rätt att kontrollera sina uppgifter i plånboken. Avsikten är samtidigt inte heller att

genom den föreslagna regleringen ändra vad den allmänna dataskyddsförordningen föreskriver om den personuppgiftsansvarige och dennes skyldigheter. Den europeiska digitala identitetsplånboken bygger på så kallad egen kontroll över uppgifter. Det handlar om en modell för behandling av personuppgifter där en person själv kan hantera tillhandahållandet av sina personuppgifter från sig själv eller betrodd tredje part till e-tjänster där personuppgifterna behövs.

Egen kontroll över uppgifter framgår av den reviderade eIDAS-förordningen på flera ställen, såsom artikel 5a.4 a, enligt vilken användaren med hjälp av plånböcker på ett säkert sätt ska kunna begära, erhålla, välja, kombinera, lagra, radera, dela och visa, under användarens egen kontroll, uppgifter för personidentifiering och andra uppgifter. Dessutom konstateras det i artikel 5a.14 att användaren ska ha full kontroll över användningen av, och uppgifterna i, sin europeiska digitala identitetsplånbok. Tillhandahållaren av plånboken får inte samla in uppgifter om användningen av plånboken som inte är nödvändiga för tillhandahållandet av tjänsterna i plånboken, och inte kombinera identifieringsuppgifter för personen eller andra personuppgifter som har lagrats i eller som är relaterade till användningen av plånboken med andra personuppgifter som erhållits ur tillhandahållarens tjänster och som inte är nödvändiga för tillhandahållandet av tjänsterna i plånboken.

Den egna kontroll över uppgifterna i den europeiska digitala identitetsplånboken som föreskrivs i den reviderade eIDAS-förordningen påverkar i praktiken hur omfattande personuppgiftsansvar Myndigheten för digitalisering och befolkningsdata har. Exempelvis ansvaret enligt den allmänna dataskyddsförordningen för att personuppgifterna är korrekta hör i regel till den personuppgiftsansvarige, och ansvaret kan inte överföras på någon annan myndighet. I Helsingfors förvaltningsdomstols beslut 8.6.2023 3396/2023 Dnr 26393/03.04.04.04.01/2021 konstaterades i anslutning till detta att domstolarna enligt 6 och 7 § i lagen om justitieförvaltningens nationella informationsresurs (955/2020) ska föra in sina avgöranden eller uppgifter om slutresultatet i Rättsregistercentralens register över avgöranden och meddelanden om avgöranden. I det sammanhanget ska domstolen se till att de uppgifter den för in motsvarar avgörandet och anteckningarna i domstolens egna register, att behövliga anteckningar har gjorts i informationsresursen för att uppgifterna ska överföras på rätt sätt och att anteckningarna har gjorts i enlighet med de tekniska krav som den personuppgiftsansvarige har ställt. Förvaltningsdomstolen ansåg liksom biträdande dataombudsmannen att de skyldigheter som i 7 § i lagen om justitieförvaltningens nationella informationsresurs föreskrivs för domstolarna inte utesluter den personuppgiftsansvariges, dvs. Rättsregistercentralens, skyldighet att sörja för att de personuppgifter som förts in i dess register är korrekta och att vidta alla tänkbara rimliga åtgärder för att säkerställa uppgifternas riktighet.

Det ansvar som Myndigheten för digitalisering och befolkningsdata bär för att uppgifterna är korrekta i relation till den plånbok som myndigheten tillhandahåller och till de anknyttande registren är ändå annorlunda än i det ovan beskrivna fallet. Myndigheten för digitalisering och befolkningsdata är i egenskap av tillhandahållare av den europeiska digitala identitetsplånboken inte på det sätt som beskrivs ovan part när uppgifter överförs till plånboken, utan parter är den som använder plånboken och den aktör som överläter uppgifterna. På motsvarande sätt är Myndigheten för digitalisering och befolkningsdatas personuppgiftsansvar i nuläget begränsat i samband med Suomi.fi-meddelanden. I dataskyddsbeskrivningen för tjänsten Suomi.fi-meddelanden konstateras det att Myndigheten för digitalisering och befolkningsdata inte är en part i elektronisk kommunikation i egenskap av tjänsteproducent för Suomi.fi-meddelanden och myndigheten har i regel inte rätt att läsa meddelanden som anlänt till personer eller företag eller meddelanden som dessa skickat i tjänsten. Kundorganisationerna som använder Suomi.fi-meddelanden är registeransvariga för innehållet i de meddelanden som de skickar. Suomi.fi-meddelanden fungerar endast som en plattform för förmedling av kundorganisationernas

meddelanden. I fråga om genomförandet av plånboken är det fråga om en situation av samma slag med tanke på Myndigheten för digitalisering och befolkningsdatas personuppgiftsansvar.

Som det beskrivits ovan ska uppgifterna i plånboken alltså vara i användarens uteslutande besittning och under dennes egen fulla kontroll. I praktiken är uppgifterna i plånboken personens egna uppgifter, vilket innebär att den som överför uppgifterna inte efter detta har möjlighet att bestämma eller följa var och för vilka ändamål personen visar sina egna uppgifter. Olika uppgifter som gäller användare av en europeisk digital identitetsplånbok tillhandahålls för plånboken i regel som elektroniska attributsintyg, som är en ny betrodd tjänst i enlighet med den reviderade eIDAS-förordningen. Bestämmelser om tillhandahållare av elektroniska attributsintyg och även om de elektroniska attributsintygen finns i den reviderade eIDAS-förordningen. Det är fråga om en tjänst som är separat från plånboken, även om plånboken i praktiken fungerar som användningsplattform för attributsintygen. Tillhandahållaren av ett elektroniskt attributsintyg ansvarar för att uppgifterna i intyget är korrekta.

Myndigheten för digitalisering och befolkningsdata ansvarar i regel endast för att de uppgifter är korrekta som myndigheten själv har överlåtit för personens bruk i den europeiska digitala identitetsplånboken. Det finns emellertid väldigt begränsat med uppgifter av det här slaget när Myndigheten för digitalisering och befolkningsdata har rollen som tillhandahållare av plånboken, och det är främst fråga om uppgifter som av tekniska och praktiska skäl behövs för tillhandahållandet av plånboken. Exempelvis kunde det finnas skäl att i det ovannämnda registret för plånboksenheter föra in vissa personuppgifter, såsom användaruppgifter, med hjälp av vilka användaren kan logga in i den användarportal som Myndigheten för digitalisering och befolkningsdata tillhandahåller och t.ex. återkalla giltigheten för en plånbok i sitt bruk. Myndigheten för digitalisering och befolkningsdata ansvarar också för att de identifieringsuppgifter för fysiska personer som myndigheten har utfärdat för personen enligt den föreslagna 3 § är korrekta, och detsamma gäller uppgifter som myndigheten har tillhandahållit användaren av plånboken som elektroniskt attributsintyg. I dessa situationer har Myndigheten för digitalisering och befolkningsdata emellertid inte rollen som tillhandahållare av plånboken, utan som tillhandahållare av identifieringsuppgifter för fysiska personer samt en betrodd tjänst som tillhandahåller elektroniska attributsintyg.

Omfattningen av det personuppgiftsansvar som beskrivs ovan är i regel motsvarande också när plånboken tillhandahålls av en aktör inom den privata sektorn.

9 §. *Bevaringstid för information om tillhandahållande av europeiska digitala identitetsplånböcker.* Enligt förslaget innehåller paragrafen bestämmelser om bevaringstiden för uppgifter som gäller tillhandahållande av europeiska digitala identitetsplånböcker. Paragrafen gäller både Myndigheten för digitalisering och befolkningsdata när den tillhandahåller en europeisk digital identitetsplånbok med stöd av den föreslagna 7 § och eventuella aktörer inom den privata sektorn när de tillhandahåller en plånbok. I den reviderade eIDAS-förordningen och kommissionens genomförandeförordningar som antagits med stöd av den åläggs aktörer som tillhandahåller plånböcker flera olika skyldigheter, och för att kunna fullgöra dessa krävs det i praktiken att aktörerna för olika register som innehåller också personuppgifter. Den reviderade eIDAS-förordningen fastställer emellertid inte hur länge sådana uppgifter ska bevaras och därför behövs den föreslagna regleringen.

I 1 mom. föreskrivs det att tillhandahållare av en europeisk digital identitetsplånbok ska bevara informationen om plånboken och informationen om tillhandahållandet av den i fem år från det att plånboken upphörde att gälla. Det kan finnas behov av att i efterhand verifiera exempelvis på vilken enhet plånboken har tagits i bruk.

I 2 mom. anges det hur länge transaktionsloggarna över en europeisk digital identitetsplånbok ska finnas tillgängliga. Bestämmelser om transaktionsloggar finns i artikel 5a.4 d i den reviderade eIDAS-förordningen, enligt vilken användare ska kunna få tillgång till en logg över alla transaktioner som utförts genom den europeiska digitala identitetsplånboken via en gemensam instrumentpanel. Enligt artikel 9.6 i kommissionens genomförandeförordning (EU) 2024/2979, som antagits med stöd av artikel 5a i den reviderade eIDAS-förordningen, ska loggarna förbli tillgängliga så länge som krävs enligt unionsrätten eller nationell rätt. Det föreskrivs dock inte om bevarandetiden för uppgifterna i unionsrätten och därför behövs det nationell kompletterande reglering. I transaktionsloggarna finns information om alla transaktioner som utförts genom plånboken och med förlitande parter eller andra europeiska digitala identitetsplånböcker. Det föreslås i momentet att informationen ska finnas tillgänglig i två år från ingången av kalenderåret efter den tidpunkt då informationen registrerades. Användaren kan i efterhand behöva verifiera och få information om transaktioner som utförts via plånboken exempelvis i fall som är relaterade till missbruk av plånboken eller för att tillgodose sina egna rättigheter. Informationsmängden kan emellertid vara betydande, beroende på hur aktivt användaren använder sin plånbok. Av den anledningen förutsätts det inte att informationen finns tillgänglig längre än två år.

10 §. Ibruktagande av en europeisk digital identitetsplånbok för en minderårig. Den reviderade eIDAS-förordningen fastställer inte någon åldersgräns för ibruktagande av en europeisk digital identitetsplånbok, varför saken måste regleras genom nationell lagstiftning och allmänna krav som gäller ibruktagande av plånböcker. Paragrafen föreslås innehålla en uttrycklig bestämmelse om möjligheten för en minderårig att självständigt ta i bruk en plånbok som tillhandahålls i Finland. Den som fyllt tretton år kan ta i bruk en europeisk digital identitetsplånbok utan vårdnadshavarens samtycke.

Det finns nationella bestämmelser i flera olika lagar om vårdnadshavarnas beslutanderätt i ärenden som gäller minderåriga samt om minderårigas rätt att delta i beslutsfattande och sköta ärenden självständigt vid en viss ålder. Enligt 6 § 3 mom. i grundlagen ska barn bemötas som jämlika individer och de ska ha rätt till medinflytande enligt sin utvecklingsnivå i frågor som gäller dem själva. Enligt motiveringen till bestämmelsen vill man genom bestämmelsen bl.a. understryka att barn i förhållande till vuxenbefolkningen ska bemötas som jämlika individer som i princip har lika grundläggande fri- och rättigheter. Samtidigt erkänns det i grundlagen att barn behöver särskilt skydd och särskild omsorg, eftersom de är omyndiga och som grupp svagare än samhällets vuxna befolkning (RP 309/1993, s. 49).

I 5 § i dataskyddslagen föreskrivs det om den åldersgräns som tillämpas när informationssamhällets tjänster erbjuds till barn. Enligt paragrafen är, när personuppgifter behandlas med samtycke enligt artikel 6.1 a i dataskyddsförordningen och det är fråga om informationssamhällets tjänster enligt artikel 4.25 i dataskyddsförordningen som erbjuds direkt till ett barn, behandlingen av barnets personuppgifter lagenlig, om barnet är minst 13 år. Informationssamhällets tjänster är exempelvis mobilapplikationer eller tjänster i sociala medier. En europeisk digital identitetsplånbok är i regel en mobilapplikation, även om också webbläsarversioner av plånboken är möjliga. När aktörer inom den privata sektorn tillhandahåller en plånbok är den anknyttande grunden för behandling av personuppgifter det samtycke som avses i artikel 6.1 a i den allmänna dataskyddsförordningen och som det hänvisas till i paragrafen. Det är alltså fråga om ett samtycke enligt den allmänna dataskyddsförordningen, och inte om ett samtycke som tillämpas som skyddsåtgärd i samband med behandling av personuppgifter. När behandlingsgrunden är samtycke, kan aktörer inom den privata sektorn i regel tillhandahålla en europeisk digital identitetsplånbok för 13-åringar. I fråga om barn som är yngre än så ska en aktör inom den privata sektorn kontrollera att barnet har föräldrarnas samtycke. I samband med att dataskyddslagen stiftades konstaterade

förvaltningsutskottet i fråga om åldersgränsen att genomförandet av dataskyddsförordningen och lagstiftningen är ett slags balanserande mellan att skydda barnet och barnets rätt att delta. Barns och ungas rätt att utnyttja informationssamhällets tjänster och medverka i den digitala kulturen ska ändå inte begränsas i onödan. Samtidigt vill utskottet ytterligare inskräpa betydelsen av andra åtgärder för att inverka på att barn och ungdomar kan agera tryggt i den virtuella världen (FvUB 13/2018 rd s. 30).

Bestämmelser om barns möjlighet att delta i behandlingen av ett förvaltningsärende finns i förvaltningslagens (434/2003) 14 § som gäller omyndigas talan. Enligt 1 mom. förs en omyndigs talan av den omyndigas intressebevakare, vårdnadshavare eller någon annan laglig företrädare. En omyndig har dock rätt att ensam föra sin talan i ärenden som gäller sådan inkomst eller förmögenhet som han eller hon råder över. Enligt 3 mom. har en minderårig som har fyllt femton år och hans eller hennes vårdnadshavare eller någon annan laglig företrädare rätt att var för sig föra talan i ett ärende som gäller den minderårigas person eller personliga fördel eller rätt. En minderårig som har fyllt 15 år kan alltså agera självständigt vid sidan av sin vårdnadshavare eller en annan laglig företrädare. När Myndigheten för digitalisering och befolkningsdata tillhandahåller en europeisk digital identitetsplånbok är den anknytande grunden för behandling av personuppgifter artikel 6.1 c i dataskyddsförordningen, där det anges att behandling av personuppgifter är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. På en plånbok som tillhandahålls av Myndigheten för digitalisering och befolkningsdata tillämpas således inte åldersgränsen på 13 år enligt 5 § i dataskyddslagen. Däremot tillämpar Myndigheten för digitalisering och befolkningsdata vid ibruktagande av plånboken regleringen i förvaltningslagen och den ovan beskrivna åldersgränsen på 15 år. Det är alltså på denna grund möjligt för en minderårig som har fyllt 15 år att självständigt ta i bruk en plånbok som Myndigheten för digitalisering och befolkningsdata tillhandahåller.

Regleringen i paragrafen behövs för att personer i samma ålder ska kunna ta i bruk plånboken självständigt oavsett om plånboken tillhandahålls av Myndigheten för digitalisering och befolkningsdata eller av en aktör inom den privata sektorn. Utan den föreslagna regleringen förutsätter självständigt ibruktagande av den plånbok som Myndigheten för digitalisering och befolkningsdata tillhandahåller en högre ålder än ibruktagande av en plånbok som tillhandahålls inom den privata sektorn. Eftersom plånboken ändå till sina funktioner och krav är likadan oavsett tillhandahållaren är det inte motiverat att det ska vara möjligt att ta en plånbok i bruk självständigt vid olika ålder beroende på vilken tillhandahållaren är.

När det i regel är fråga om informationssamhällets tjänster som avses i dataskyddslagen är det motiverat att vid självständigt ibruktagande tillämpa åldersgränsen på 13 år i enlighet med dataskyddslagen. Detta ökar konsekvensen med tanke på regleringen av den digitala miljön. Trots att fallen av missbruk och brott som sker på nätet har ökat kan det ändå antas att en 13-åring inte ens på elektronisk väg kan utföra rättshandlingar med betydande förmögenhetsvärde. Ändå kan en 13-åring ha svårigheter att förstå eller gestalta konsekvenserna av sina förbindelser och ansvaren i anslutning till användningen av tjänsten. Det bör emellertid noteras att propositionen inte innehåller något förslag om att utvidga 13-åringars rättigheter att utföra rättshandlingar, utan denna rätt fastställs också i fortsättningen med stöd av annan lagstiftning. Däremot främjar en åldersgräns på 13 år minderårigas likvärdiga möjligheter att sköta ärenden och styrka sin identitet elektroniskt. Exempelvis inom social- och hälsovården är det möjligt för en 13-åring att sköta ärenden självständigt utan vårdnadshavare, och för dessa situationer behövs det en självständig möjlighet för 13-åringar att styrka identiteten och göra elektroniska underskrifter.

Dessutom bör det noteras att den ålder på 13 år som föreslås i paragrafen gäller endast ibruktagande av en europeisk digital identitetsplånbok i en minderårigs mobila enhet. I praktiken är det fråga om att ladda ned en applikation för en europeisk digital identitetsplånbok på användarens tekniska utrustning samt att ta i bruk identifieringsuppgifter för personen. För varje elektroniskt attributsintyg tillämpas emellertid den reglering som gäller intyget och dess tillhandahållare. Också plånbokens förlitande parter ska själv bedöma om en minderårig i varje enskilt fall kan sköta ärendet självständigt eller om ärendet kräver separat samtycke av vårdnadshavaren. Att plånboken laddas ned i den minderårigas mobila enhet innebär således inte nödvändigtvis att den minderåriga med hjälp av plånboken kan sköta ärenden självständigt i varje situation, utan detta fastställs enligt annan reglering.

Samtidigt har den europeiska digitala identitetsplånboken också ansetts möjliggöra bättre skydd för minderåriga vid elektronisk kommunikation. Diskussionen om skydd för minderåriga i elektroniska tjänster har under den senaste tiden blivit allt viktigare i och med att olika plattformar för sociala medier samt användningen av videospel ökar. Med hjälp av plånboken är det möjligt att styrka användarens ålder på ett tillförlitligt sätt, vilket kan möjliggöra övervakning av åldersgränser i anslutning till olika elektroniska tjänster och kanaler på sociala medier. Dessutom kan minderåriga med plånboken styrka sin egen identitet på motsvarande sätt som med de nuvarande verktygen för stark autentisering. I den regeringsproposition som stiftandet av autentiseringslagen stödde sig på konstaterades det att stark autentisering är säkrare att använda än svag autentisering såväl för användaren som för tjänsteleverantören. Metoderna för stark autentisering är bättre än metoderna för svag autentisering t.ex. när det gäller att bekämpa identitetsstöld (RP 36/2009 rd, s. 10). Vid svag autentisering kan en person själv skapa sig eller ges flera elektroniska s.k. identiteter, som också kan avvika från personens faktiska egenskaper. Personen kan uppge felaktiga uppgifter om t.ex. sin ålder eller sitt kön (RP 36/2009 rd, s. 8). Den föreslagna åldersgränsen främjar alltså också i detta avseende möjligheterna för yngre personer än tidigare att använda ett säkert sätt för att styrka sin identitet elektroniskt.

Om en person som är under 13 år vill ta i bruk en europeisk digital identitetsplånbok kräver det vårdnadshavarens samtycke. Enligt 5 § 1 mom. i lagen angående vårdnad om barn och umgängesrätt (361/1983) ansvarar barnets vårdnadshavare gemensamt för de uppgifter som hör till vårdnaden om barnet och fattar gemensamt beslut som gäller barnet, om inte annorlunda är stadgat eller bestämt. Enligt den föreslagna paragrafen räcker emellertid samtycke från en vårdnadshavare för ibruktagande av plånboken. Tillhandahållaren av plånboken ska bedöma på vilket sätt vårdnadshavarens samtycke inhämtas. Vårdnadshavarens samtycke till ibruktagande av plånboken ska ges senast i samband med att identifieringsuppgifterna för personen tas i bruk.

11 §. Utlämnande av källkoder för europeiska digitala identitetsplånböcker. I paragrafen föreslås det bestämmelser om utnyttjande av nationellt handlingsutrymme i fråga om utlämnande av källkoder för applikationer för europeiska digitala identitetsplånböcker. Bestämmelser om nationellt handlingsutrymme finns i artikel 5a.3 i den reviderade eIDAS-förordningen. Innehållet i handlingsutrymmet beskrivs närmare i avsnitt 2.2.1. Enligt paragrafen behöver en tillhandahållare av en europeisk digital identitetsplånbok inte lämna ut en källkod för en plånboks komponenter som inte har installerats på den tekniska utrustningen av en användare för den europeiska digitala identitetsplånboken, om det föreligger vederbörligen motiverade skäl för detta. Det är alltså möjligt att begränsa utlämnandet av källkoden i fråga om olika bakomliggande system, såsom de bibliotek och kommunikationskanaler som används.

Enligt formuleringen i paragrafen behöver tillhandahållaren av plånboken inte överlåta källkoden för den europeiska digitala identitetsplånboken om det finns vederbörligen motiverade skäl för att låta bli att överlåta källkoden. Det är således fråga om möjliggörande

reglering så att tillhandahållaren av plånboken ändå alltid enligt sitt övervägande kan låta bli att tillämpa de föreslagna bestämmelserna och överlåta källkoden för plånboken. När det nationella handlingsutrymmet utnyttjas är det fråga om ett undantag. Därmed ska förekomsten av ett vederbörligen motiverat skäl tolkas snävt. Tillhandahållaren av plånboken ska bedöma om det finns ett vederbörligen motiverat skäl som gör att källkoden för plånboken inte behöver överlåtas. Myndigheten för digitalisering och befolkningsdata ska också vid tillhandahållande av en europeisk digital identitetsplånbok följa lagen om offentlighet i myndigheternas verksamhet (621/1999, nedan *offentlighetslagen*). Källkoden för plånboken kan anses vara en myndighetshandling som avses i 5 § i offentlighetslagen. I 24 § i offentlighetslagen föreskrivs det om sekretessbelagda myndighetshandlingar, och i 1 mom. uppräknas olika grunder för sekretessen. Offentlighetslagen stiftades med medverkan av grundlagsutskottet och godtagbarheten av grunderna för sekretess i förhållande till offentlighetspresumtionen samt till andra grundläggande fri- och rättigheter bedömdes i lagens förarbeten (RP 30/1998 rd). Det är inte ändamålsenligt att i detta sammanhang avvika från de framförda bedömningarna, och som sådana vederbörligen motiverade skäl som avses i paragrafen kan alltså i regel betraktas grunderna för sekretess enligt 24 § i offentlighetslagen. Myndigheten för digitalisering och befolkningsdata kan således låta bli att lämna ut källkoden för den plånbok som myndigheten tillhandahåller i fråga om sådana komponenter som inte har lagrats på användarens utrustning när någon av grunderna för sekretess enligt 24 § i offentlighetslagen råder.

Offentlighetslagen tillämpas inte på privata tjänstetillhandahållares handlingar. Därmed kan ett vederbörligen motiverat skäl inte på motsvarande sätt direkt härledas ur grunderna för sekretess enligt 24 § 1 mom. i offentlighetslagen när en europeisk digital identitetsplånbok tillhandahålls av en privat tjänstetillhandahållare. Vid bedömningen av ett vederbörligen motiverat skäl kan det ändå vara möjligt att hämta stöd i grunderna för sekretess enligt offentlighetslagen, t.ex. i grunden för sekretess i relation till privata affärshemligheter enligt 24 § 1 mom. 20 punkten. Vid bedömningen ska det dessutom läggas vikt vid de aspekter som eftersträvas genom öppenhet hos källkoden för plånböckerna. Enligt skäl 33 i den reviderade eIDAS-förordningen är avsikten med öppenheten hos källkoden att främja det samhälleliga förtroendet för plånböckerna och plånböckernas godkännande bland användarna. Dessutom är avsikten att säkerställa att plånboken fungerar så transparent som möjligt i synnerhet med tanke på behandlingen av personuppgifter. Med öppenheten hos källkoden för plånböckerna vill man också säkerställa deras säkerhet.

12 §. Avgifter för kvalificerade elektroniska underskrifter i europeiska digitala identitetsplånböcker. I paragrafen föreslås det bestämmelser om utnyttjande av nationellt handlingsutrymme i fråga om avgifter för elektroniska underskrifter. Bestämmelser om det nationella handlingsutrymmet finns i artikel 5a.5 andra delen i den reviderade eIDAS-förordningen. Innehållet i handlingsutrymmet beskrivs närmare i avsnitt 2.2.1. Om det nationella handlingsutrymmet inte utnyttjas är elektronisk underskrift med hjälp av plånboken alltid avgiftsfri för fysiska personer. En kvalificerad elektronisk underskrift är emellertid en betrodd tjänst enligt eIDAS-förordningen som i nuläget vanligen tillhandahålls mot avgift av leverantörer av betrodda tjänster inom EU. Också enligt artikel 3.16 i den reviderade eIDAS-förordningen avses med betrodda tjänster elektroniska tjänster som i allmänhet tillhandahålls mot vederlag. Att det föreskrivs att tjänsten ska vara avgiftsfri innebär alltså redan i sig ett undantag från att tjänster i allmänhet är avgiftsbelagda. Syftet med att utnyttja det nationella handlingsutrymmet är att minska de negativa konsekvenserna för verksamheten hos de leverantörer av betrodda tjänster som tillhandahåller kvalificerade elektroniska underskrifter. Avsikten är ändå inte att genom bestämmelsen begränsa eller på annat sätt ta ställning till för vilka användningsändamål elektronisk underskrift som görs med en europeisk digital identitetsplånbok kan eller inte kan användas. Avsikten med bestämmelsen är endast att göra

det möjligt att ta ut en avgift när elektronisk underskrift görs för undertecknarens yrkesmässiga ändamål.

Enligt paragrafen kan en tillhandahållare av en europeisk digital identitetsplånbok eller en kvalificerad betrodd tjänst som producerar en kvalificerad underskrift för plånboken ta ut en avgift för kvalificerad elektronisk underskrift som görs med plånboken när de villkor som avses i paragrafen uppfylls. Med tanke på det praktiska genomförandet kan kvalificerad underskrift produceras för plånboken av en annan aktör än den som tillhandahåller den egentliga plånboken. Av denna anledning kan rätten att besluta om avgiften höra också till den kvalificerade tillhandahållare av den betrodda tjänsten som producerar funktionen i fråga.

Enligt paragrafen kan avgift tas ut i första hand när det går att tillförlitligt verifiera att den som använder plånboken är kopplad till en organisation. I praktiken innehåller en europeisk digital identitetsplånbok en anordning för att skapa en kvalificerad elektronisk underskrift. Alternativt går det att med hjälp av plånboken använda en extern kvalificerad anordning för att skapa en elektronisk underskrift. När plånboken används av en fysisk person är anordningen för att skapa en kvalificerad elektronisk underskrift i regel personlig. Därför kan man i regel i en sådan situation inte sluta sig till att den fysiska personen har en koppling till en organisation, vilket krävs t.ex. för underskrift i tjänsteuppdrag. Då är användningen av elektronisk underskrift i regel jämförbar med den nuvarande användningen av underskriftscertifikat som finns i identitetskort. Det ska emellertid vara möjligt att påvisa en tillförlitlig koppling till en organisation t.ex. genom användning av Suomi.fi-fullmakter, med ett separat elektroniskt attributsintyg eller med kvalificerad elektronisk stämpel. Avsikten är emellertid att bestämmelsen ska vara teknikneutral och därför anges där inte det tekniska sättet för genomförandet av kopplingen.

En tillförlitlig koppling till en organisation kan styrkas också genom utveckling av sådana europeiska digitala identitetsplånböcker vars användare är fysiska personer som sköter ärenden för en organisations räkning. Då kan genom en kvalificerad underskrift som gjorts med plånboken utöver undertecknarens identitet också kopplingen till organisationen verifieras tillförlitligt. Detta tillvägagångssätt är i någon mån jämförbart med elektronisk underskrift med underskriftscertifikat som finns i de nuvarande organisationskort. Verifieringen av organisationskopplingen bör göras samtidigt som personen beviljas det underskriftscertifikat som behövs för att göra underskrift. Organisationskopplingen kan verifieras antingen av certifierarens bakomliggande system t.ex. mot ett externt register eller alternativt så att undertecknaren styrker de uppgifter som behövs för verifiering av organisationskopplingen genom sin egen plånbok, t.ex. med hjälp av ett elektroniskt attributsintyg.

Enligt paragrafen kan en avgift tas ut förutom för elektronisk underskrift med plånboken också i situationer där man tillförlitligt kan verifiera att underskriften är kopplad till ett yrkesmässigt ändamål. Det är möjligt att påvisa kopplingen exempelvis med ett separat elektroniskt attributsintyg. Alternativt kan kopplingen och avgiften bygga på samlad information i informationssystemet för den part som begär underskriften. Det kan vara fråga om ett yrkesmässigt ändamål t.ex. om underskriften görs som en del av näringsverksamheten för användaren av den europeiska digitala identitetsplånboken. I den gällande lagstiftningen har i allmänhet yrkesmässighet och kontinuitet betraktats som kännetecken för näringsverksamhet. Icke-yrkesmässig verksamhet har däremot ansetts vara förknippad med en viss slumpmässighet. Det är emellertid möjligt att det också finns situationer där yrkesmässigheten är småskalig, men kontinuerlig, såsom vid företagande som bisyssla.

13 §. Skyldigheter för tillhandahållare av europeiska digitala identitetsplånböcker i situationer med säkerhetsincidenter. Paragrafen föreslås innehålla bestämmelser om skyldigheterna för tillhandahållare av europeiska digitala identitetsplånböcker i situationer där plånboken, de

valideringsmekanismer som avses i artikel 5a.8 eller det system för elektronisk identifiering där plånboken tillhandahålls är föremål för en säkerhetsincident eller deras säkerhet delvis har äventyrats. Regleringen behövs för att förtydliga vilken aktör som ansvarar för fullgörandet av de skyldigheter som åläggs medlemsstaterna i den reviderade eIDAS-förordningens artikel 5e, som gäller säkerhetsincidenter med europeiska digitala identitetsplånböcker (se närmare om skyldigheternas innehåll i avsnitt 2.2.1).

I 1 mom. anges det att tillhandahållaren av en europeisk digital identitetsplånbok i fråga om den plånbok som denne tillhandahåller svarar för att medlemsstatens skyldigheter enligt artikel 5e i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den artikeln fullgörs. Tillhandahållaren av plånboken har de bästa förutsättningarna att observera och hantera säkerhetsincidenter i fråga om den plånbok den tillhandahåller samt att vidta de åtgärder som avses i artikel 5e. Av denna anledning är det ändamålsenligt att den som tillhandahåller en europeisk digital identitetsplånbok svarar för skyldigheterna enligt artikeln i fråga om den plånbok som den tillhandahåller. Medlemsstaternas skyldigheter preciseras i kommissionens genomförandeförordning (EU) 2025/847. I genomförandeförordningen föreskrivs det exempelvis om kriterierna för bedömning av en säkerhetsincident eller äventyrande samt om upphävande av tillhandahållandet och användningen av plånboken och om andra åtgärder samt om återupprättande av användningen. I momentet finns dock ingen direkt hänvisning till förordningen i fråga, eftersom kommissionen har uttryckt att den eventuellt ändrar förordningen under de närmaste åren, och därför hänvisas det i momentet bara till eIDAS-förordningen och den reglering som antagits med stöd av den.

I 2 mom. föreskrivs det om situationer där en tillhandahållare av en europeisk digital identitetsplånbok av tekniska skäl inte kan fullgöra medlemsstatens skyldighet att anmäla säkerhetsincidenter. Då görs anmälan av Transport- och kommunikationsverket. Enligt artikel 10 i kommissionens genomförandeförordning (EU) 2025/847 ska anmälningarna göras via systemet för analys och rapportering av cyberincidenter, (Cyber Incident Reporting and Analysis System, CIRAS) som drivs av Enisa, eller ett likvärdigt system som överenskommit av medlemsstaterna och kommissionen. I regel är det inte möjligt för någon annan än en aktör inom den offentliga sektorn att göra anmälningar via CIRAS-systemet. I praktiken innebär detta att när plånboken tillhandahålls av en aktör inom den privata sektorn, är det inte möjligt för aktören att fullgöra medlemsstaternas anmälningsskyldigheter i situationer som avses i artikel 5e. Av denna anledning behövs det reglering om att anmälan i dessa situationer görs av Transport- och kommunikationsverket. Tillhandahållaren av plånboken har en skyldighet att utan obefogat dröjsmål lämna alla behövliga uppgifter till Transport- och kommunikationsverket. När det gäller att lämna uppgifter ska de tidsfrister för anmälan som avses i kommissionens genomförandeförordningen (EU) 2025/847 beaktas och det ska säkerställas att Transport- och kommunikationsverket ges en rimlig tid för att göra anmälan.

14 §. Skyldigheter för användare av europeiska digitala identitetsplånböcker. Det föreslås att paragrafen innehåller bestämmelser om skyldigheterna för användaren av en europeisk digital identitetsplånbok när det gäller förvaring och användning av plånboken. I artikel 3.5a i den reviderade eIDAS-förordningen definieras användare, som avser en fysisk eller juridisk person, eller en fysisk person som företräder en annan fysisk person eller en juridisk person, som använder betrodda tjänster eller medel för elektronisk identifiering som tillhandahålls i enlighet med eIDAS-förordningen. Dessutom definieras användare i kommissionens genomförandeförordningar som utfärdats med stöd av den reviderade eIDAS-förordningen och med termen avses en användare som innehar en plånboksenhet.

Den reviderade eIDAS-förordningen reglerar inte det ansvar som användaren av en europeisk digital identitetsplånbok har, varför saken ska regleras enligt nationellt övervägande. Enligt 1

mom. ska användaren av en europeisk digital identitetsplånbok använda plånboken omsorgsfullt. Skyldigheten att använda plånboken omsorgsfullt gäller särskilt de individualiserande uppgifter med vilka plånboken kan användas, så som PIN-kod eller annan motsvarande kod eller identifieringskod. Vid bedömning av hurdana försiktighetsåtgärder det är rimligt att förutsätta av användaren ska det beaktas att plånboken i många fall ingår i personens mobila enhet som han eller hon använder ofta och bär på sig. Till rimliga försiktighetsåtgärder hör exempelvis att på det sätt som omständigheterna förutsätter hålla reda på den enhet där plånboken finns. Hur omsorgsfulla försiktighetsåtgärderna är bedöms som helhet. Skyldigheten att använda plånboken omsorgsfullt börjar när plånboken har tagits i bruk. Med användning av plånboken avses användning av vilken som helst av funktionerna i plånboken. Skyldigheten att vara omsorgsfull gäller således elektronisk identifiering med hjälp av plånboken och elektronisk underskrift samt användning av elektroniska attributsintyg. Om användaren alltså gör en elektronisk underskrift eller sätter en stämpel med hjälp av plånboken tillämpas på detta inte de skyldigheter som föreskrivs i den föreslagna 16 §.

I 1 mom. föreskrivs det dessutom om förbud mot att överlåta den europeiska digitala identitetsplånboken för att användas av någon annan. Plånboken är avsedd endast för att styrka identiteten för den person som är kopplad till plånboken och den personens fastställda uppgifter. Regleringen behövs med tanke på fastställandet av det ansvar som användaren av plånboken har, och motsvarande bestämmelse ingår i 23 § 2 mom. i autentiseringslagen. Plånboken gör det möjligt för användaren att identifiera sig elektroniskt och även att använda andra uppgifter som är kopplade till personen själv. För att e-tjänster ska kunna lita på den identifiering som bygger på plånboken och på de uppgifter som styrks med plånboken är det nödvändigt att plånboken och de ärenden som sköts med dess hjälp med säkerhet gäller bara en person. Avsikten med regleringen är dessutom att göra det tydligt för användaren att även om den europeiska digitala identitetsplånboken i regel är en applikation som fungerar i en mobil enhet, vilket i nuläget är ett rätt vardagligt fenomen, är den avsedd att användas enbart av användaren själv. Att bestämmelserna överensstämmer med autentiseringslagen stöder målet i den föreslagna regleringen att förtydliga för användarna att den europeiska digitala plånboken och användningen av den är förknippad med motsvarande skyldighet att ta hand om plånboken som den skyldighet som gäller de nuvarande identifieringsverktygen för stark autentisering.

Det föreslagna 1 mom. innehåller ingen uttrycklig bestämmelse om att förbudet mot att överlåta den europeiska digitala identitetsplånboken för att användas av någon annan inte gäller situationer där användaren behöver hjälp av en personlig assistent för att använda plånboken. Enligt artikel 5a.21 i den reviderade eIDAS-förordningen ska europeiska digitala identitetsplånböcker emellertid göras tillgängliga för användning av personer med funktionsnedsättning, på samma villkor som andra användare, i enlighet med Europaparlamentets och rådets direktiv (EU) 2019/882. Det föreslagna 1 mom. begränsar inte detta krav enligt eIDAS-förordningen. Med tillgänglighet avses att hinder för användning av produkter och tjänster undanröjs och uppkomsten av hinder förebyggs. Tillgänglighet innebär att personer med funktionsnedsättning kan observera, använda och förstå produkter och tjänster på samma villkor som andra. Enligt 15 § i diskrimineringslagen (1325/2014) ska myndigheter och de som tillhandahåller varor eller tjänster göra sådana ändamålsenliga och rimliga anpassningar som behövs i det enskilda fallet för att göra det möjligt för personer med funktionsnedsättning att på lika villkor som andra använda myndigheters tjänster samt få varor och tjänster som tillhandahålls allmänheten. När anpassningarnas rimlighet bedöms beaktas utöver behoven hos en människa med funktionsnedsättning också aktörens storlek och ekonomiska ställning, verksamhetens art och omfattning samt de uppskattade kostnaderna för anpassningarna och det stöd som finns att få för anpassningarna.

I enlighet med kundens behov kan tänkbara anpassningsformer vara bland annat redigering av handlingar i punktskrift, tillhandahållande av nyckeltal i elektronisk form, identifiering med fingeravtryck eller tillåtande av att personlig assistent används. När en plånbok tillhandahålls måste det emellertid bedömas hurdana anpassningar som är möjliga inom ramen för eIDAS-förordningen och reglering som antagits med stöd av den samt den nationella certifieringsordningen, för att en person med funktionsnedsättning på lika villkor som andra ska kunna använda en europeisk digital identitetsplånbok. Om det vid tillhandahållande av en plånbok har gjorts anpassningar som möjliggör användning av plånboken på lika villkor möjliggjort exempelvis anlitande av personlig assistent ska dessa anpassningar beaktas när man bedömer om användaren har överlåtits plånboken för att användas av någon annan. Det är t.ex. i regel inte fråga om överlåtande av plånboken för att användas av någon annan om det som en rimlig anpassning har gjorts möjligt att anlita personlig assistent. Den föreslagna regleringens förhållande till jämlikhet behandlas närmare i avsnitt 12.1.

I 2 mom. föreskrivs det om skyldigheten för den som använder en europeisk digital identitetsplånbok att göra en anmälan om att den tekniska utrustningen obehörigen har kommit i någon annans besittning eller om obehörig användning av plånboken. Anmälan ska göras till tillhandahållaren av plånboken utan obefogat dröjsmål när användaren har noterat saken. Ansvar för användaren av plånboken för obehörig användning upphör efter att anmälan har gjorts. Huruvida användaren har gjort anmälan utan obefogat dröjsmål bedöms från fall till fall med hänsyn till omständigheterna. Ingen fastställd form anges för anmälan.

15 §. Användarens ansvar för obehörig användning av en europeisk digital identitetsplånbok. Enligt förslaget föreskrivs det i paragrafen om ansvaret för användaren av en europeisk digital identitetsplånbok i situationer där en annan person använder eller har använt plånboken obehörigen. Paragrafen tillämpas exempelvis när en mobil enhet där den europeiska digitala identitetsplånboken har tagits i bruk har förkommit eller blivit stulen och den person som hittat eller stulit plånboken lyckas använda den och de uppgifter den innehåller. Autentiseringslagens gällande 27 § innehåller motsvarande bestämmelser om vilket ansvar innehavaren av ett identifieringsverktyg har för obehörig användning av verktyget. På motsvarande sätt innehåller betaltjänstlagen (290/2010) bestämmelser om vilket ansvar användaren av en betaltjänst har för obehörig användning av betalningsmedlet och 7 kap. 40 § i konsumentskyddslagen bestämmelser om vilket ansvar konsumenten har för obehörig användning av ett kreditkort eller annan kod som berättigar till användning av kredit.

I 1 mom. föreskrivs det uttömmande om de situationer där användaren av en europeisk digital identitetsplånbok ansvarar för obehörig användning av plånboken. Med användning av plånboken avses användning av vilken som helst av funktionerna i plånboken. Skyldigheten att vara omsorgsfull gäller således stark autentisering med hjälp av plånboken och elektronisk underskrift samt användning av elektroniska attributsintyg. Om elektronisk underskrift eller stämpling inte görs med plånboken tillämpas på detta alltså inte det ansvar som föreskrivs i 15 §. Användaren kan enligt 1 mom. bli ansvarig för sådan obehörig användning som beror på att användaren av den europeiska digitala identitetsplånboken själv har överlåtits plånboken för att användas av någon annan. Det handlar om sådan överlåtelse som avses i bestämmelsen när användaren av plånboken medvetet och frivilligt överlåter besittningen av plånboken till någon annan. Bestämmelsen gäller således t.ex. inte situationer där användaren av plånboken tillfälligt överlåter den mobila enhet där plånboken har tagits i bruk till någon annan för förvaring. Tillämpningen av bestämmelsen förutsätter att uppgifter som behövs för hantering av plånboken har överlåtits, t.ex. den sifferkod eller någon annan kod som behövs för att applikationen ska kunna användas.

Vid bedömning av om personen själv har överlåtit plånboken för att användas av någon annan ska det emellertid på det sätt som beskrivs ovan i 14 § tas hänsyn till om det vid tillhandahållande av plånboken har gjorts anpassningar som möjliggör användning av plånboken på lika villkor och t.ex. gjorts möjligt att anlita personliga assistent. Det är i regel inte fråga om överlåtande av plånboken för att användas av någon annan om det som en rimlig anpassning har gjorts möjligt att anlita personlig assistent. Den föreslagna regleringens förhållande till jämlikhet behandlas närmare i avsnitt 12.1.

Enligt 2 *punkten* kan användaren bli ansvarig för obehörig användning av plånboken om den obehöriga användningen beror på användarens oaktsamhet som inte är lindrig. Enligt 3 *punkten* kan användaren därtill bli ansvarig för obehörig användning av plånboken om han eller hon har försummat sin skyldighet enligt den föreslagna 14 § att utan obefogat dröjsmål anmäla till tillhandahållaren av plånboken att den tekniska utrustningen obehörigen har kommit i någon annans besittning eller om obehörig användning av plånboken.

I 2 *mom.* föreskrivs det om situationer där användaren av en europeisk digital identitetsplånbok dock inte ansvarar för obehörig användning av plånboken, trots att någon av grunderna för ansvar enligt 1 *mom.* uppfylls. Enligt 1 *punkten* ansvarar användaren inte för obehörig användning av plånboken till den del plånboken har använts efter att användaren har gjort en anmälan enligt 14 §. Enligt 2 *punkten* ansvarar användaren inte heller för användningen av plånboken om han eller hon inte har kunnat göra anmälan enligt den föreslagna 14 § på grund av att tillhandahållaren av plånboken har försummat att sörja för att det är möjligt att göra anmälan.

I 3 *mom.* föreskrivs det om ansvarsregleringens tvingande natur till skydd för konsumenten. Motsvarande bestämmelse finns i 3 § i autentiseringslagen.

16 §. Nationellt register över europeiska digitala identitetsplånböckers förlitande parter. Enligt förslaget föreskrivs det i 1 *mom.* att Transport- och kommunikationsverket ska inrätta och vara personuppgiftsansvarig för det nationella register över europeiska digitala identitetsplånböckers förlitande parter som avses i artikel 5b i den reviderade eIDAS-förordningen. Regleringen behövs eftersom den reviderade eIDAS-förordningen föreskriver om en skyldighet för förlitande parter att registrera sig i den medlemsstat där de är etablerade. Dessutom förutsätts det i artikel 3.1 i kommissionens genomförandeförordning (EU) 2025/843, som antagits med stöd av artikel 5b, att varje medlemsstat inrättar minst ett nationellt register för plånböckers förlitande parter. Paragrafen innehåller ändå inte någon uttrycklig hänvisning till kommissionens genomförandeförordning, eftersom kommissionen har meddelat att den kommer att ändra genomförandeförordningarna i anslutning till genomförandet av den europeiska digitala identitetsplånboken. Enligt artikel 5b i den reviderade eIDAS-förordningen eller kommissionens genomförandeförordning som antagits med stöd av den är det ändå inte klart vilken aktör i Finland som ska säkerställa att denna skyldighet fullgörs. Av den anledningen behövs det nationell kompletterande reglering.

I 1 *mom.* föreskrivs det dessutom att Transport- och kommunikationsverket är personuppgiftsansvarig i fråga om registrering av förlitande parter. Förlitande parter är i regel juridiska personer, men de kan också vara fysiska personer och registret över förlitande parter kan vara förknippat med behandling av personuppgifter. Rättsgrunden för behandlingen av personuppgifter är artikel 6.1 c i den allmänna dataskyddsförordningen, som anger att behandling av personuppgifter i en situation enligt ledet är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Kommissionens genomförandeförordning (EU) 2025/848, som antagits med stöd av artikel 5b i den reviderade eIDAS-förordningen förutsätter att varje medlemsstat utser minst en personuppgiftsansvarig för att administrera och

inrätta ett nationellt register över plånbokens förlitande parter. I paragrafen föreskrivs det alltså som komplettering till den reviderade eIDAS-förordningen att Transport- och kommunikationsverket har till uppgift att inrätta och vara personuppgiftsansvarig för ett register i Finland över förlitande parter. Således bildar den reviderade eIDAS-förordningen och den kompletterande nationella lagstiftningen tillsammans en rättslig förpliktelse som åvilar Transport- och kommunikationsverket.

Det är ändamålsenligt att Transport- och kommunikationsverket anvisas uppgiften, eftersom ämbetsverket är tillsynsmyndighet i fråga om europeiska digitala identitetsplånböcker och det enligt 46a.4 led f i den reviderade eIDAS-förordningen hör till Transport- och kommunikationsverkets uppgifter som tillsynsmyndighet att i vissa situationer registrera förlitande parter eller tillfälligt eller permanent upphäva registreringen och inkluderingen av förlitande parter i den gemensamma mekanism som avses i 5b.7 För att Transport- och kommunikationsverket ska kunna utföra också dessa uppgifter effektivt är det ändamålsenligt att ämbetsverket inrättar ett register över förlitande parter.

I 2 mom. föreskrivs det att Transport- och kommunikationsverket svarar för medlemsstatens skyldigheter i Finland enligt artikel 5b i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den. I kommissionens genomförandeförordning (EU) 2025/848 föreskrivs det att medlemsstaten ska göra informationen om registrerade förlitande parter allmänt tillgänglig online. Dessutom ska medlemsstaterna säkerställa att de inrättade nationella registren över plånböckernas förlitande parter är förenliga med relevanta gemensamma registreringsprinciper. Transport- och kommunikationsverket har som personuppgiftsansvarig de bästa förutsättningarna att fullgöra medlemsstatens föreskrivna skyldigheter och därför föreskrivs det att det nationella genomförandet är en uppgift för ämbetsverket.

I 3 mom. föreskrivs det om ett nytt bemyndigande för Transport- och kommunikationsverket att utfärda närmare föreskrifter om genomförandet av förlitandepartcertifikat och förlitandepartregistreringscertifikat för en europeisk digital identitetsplånbok samt om certifikatspolicy och certifieringspraxis för dem, med iakttagande av de bestämmelser som utfärdats med stöd av artikel 5b i eIDAS-förordningen. I kommissionens genomförandeförordning (EU) 2025/848 föreskrivs det om grundläggande krav som gäller båda de ovannämnda certifikaten. Medlemsstaterna ges emellertid i uppgift att verkställa den certifikatsrelaterade certifikatspolicyn och fastställa vissa relaterade krav. Certifikaten i fråga är nära anknutna till inrättandet av det nationella registret över plånböckernas förlitande parter.

17 §. Valideringsmekanismer för ramverket för den europeiska digitala identitetsplånboken. Enligt förslaget innehåller paragrafen bestämmelser om genomförandet i Finland av valideringsmekanismerna enligt artikel 5a.8 i den reviderade eIDAS-förordningen. De valideringsmekanismer som föreskrivs i paragrafen ska tillhandahållas avgiftsfritt. I 1 mom. föreskrivs det om skyldigheten för Myndigheten för digitalisering och befolkningsdata att tillhandahålla den valideringsmekanism som säkerställer att europeiska digitala identitetsplånböckers äkthet och giltighet kan kontrolleras.

I 2 mom. föreskrivs det om Transport- och kommunikationsverkets skyldighet att tillhandahålla den valideringsmekanism enligt artikel 5a.8 b i den reviderade eIDAS-förordningen som gör det möjligt för användare att kontrollera äkthet och giltighet för identiteten hos de förlitande parter som registrerats i enlighet med artikel 5b. I den föreslagna 16 § föreskrivs det att Transport- och kommunikationsverket ska inrätta och vara personuppgiftsansvarig för det nationella registret över europeiska digitala identitetsplånböckers förlitande parter. Transport- och kommunikationsverket genomför den valideringsmekanism som avses i momentet som en del av det nationella registret över plånbokens förlitande parter genom att upprätta ett offentligt

gränssnitt där vem som helst kan göra förfrågningar till det nationella registret över förlitande parter. Detta offentliga gränssnitt erbjuder både maskin- och människoläsbara gränssnitt där det går att kontrollera äkthet och giltighet för identiteten hos de förlitande parterna.

18 §. Identitetsmatchning. Det föreslås att paragrafen innehåller bestämmelser om genomförande av identitetsmatchning i Finland. Identitetsmatchning beskrivs närmare i avsnitt 2.2.2. Artikel 11a i den reviderade eIDAS-förordningen förutsätter att medlemsstaterna säkerställer otvetydig identitetsmatchning för fysiska personer som använder anmälda medel för elektronisk identifiering eller europeiska digitala identitetsplånböcker. Det är ändå inte på grundval av bestämmelserna i den reviderade eIDAS-förordningen klart hur skyldigheten ska fullgöras eller vilken eller vilka aktörer i Finland som ska göra det. Därför behövs nationell kompletterande reglering.

Enligt 1 mom. genomförs identitetsmatchning i Finland centraliserat av Myndigheten för digitalisering och befolkningsdata. Den reviderade eIDAS-förordningen gör det möjligt att fullgöra skyldigheten också decentraliserat så att varje förlitande part själv sörjer för att fullgöra skyldigheten. I Finland genomförs identitetsmatchningen emellertid som en centraliserad lösning där Myndigheten för digitalisering och befolkningsdata genomför identitetsmatchningen för alla de e-tjänster som omfattas av skyldigheten. Vid beredningen av propositionen bedömdes en centraliserad lösning vara den mest kostnadseffektiva och ändamålsenliga lösningen för att genomföra identitetsmatchning i Finland. Identitetsmatchning tillhandahålls enligt 1 mom. både myndigheter och andra som sköter offentliga förvaltningsuppgifter, eftersom artikel 11a förutsätter identitetsmatchning i situationer där en medlemsstat är förlitande part.

I praktiken genomför Myndigheten för digitalisering och befolkningsdata informationstjänsten för identitetsmatchning, där e-tjänsten ska registrera sig. Identifieringstjänsten Suomi.fi är en e-tjänst som utnyttjar identitetsmatchning och svarar därmed för att begära att informationstjänsten gör identitetsmatchningen för de e-tjänster som använder identifieringstjänsten Suomi.fi. Informationstjänsten för identitetsmatchning försöker göra identitetsmatchningen i förhållande till de uppgifter som finns i befolkningsdatasystemet. För att identitetsmatchningen ska kunna göras förutsätts därmed att personen är registrerad i befolkningsdatasystemet. Vid identitetsmatchning skapas inga nya registeridentiteter i befolkningsdatasystemet, utan den gällande regleringen ska också i fortsättningen tillämpas vid registrering av personer i befolkningsdatasystemet.

Myndigheten för digitalisering och befolkningsdata ska genomföra identitetsmatchningen med iakttagande av artikel 11a i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den. Kommissionen har antagit en genomförandeförordning (EU) 2025/846 om tillämpningsreglerna vid gränsoverskridande identitetsmatchning för fysiska personer. I genomförandeförordningen fastställs de allmänna kraven på processen i fråga om såväl skyldigheterna för förlitande parter eller ett centraliserat system som dessa använder i anslutning till matchningsprocessens olika slutresultat. Dessutom föreskrivs det om den processrelaterade matchningsloggen. Bestämmelsen innehåller emellertid ingen uttrycklig hänvisning till genomförandeförordningen i fråga, eftersom kommissionen har uttryckt att den eventuellt kommer att ändra de genomförandeförordningar som den redan antagit.

Enligt det föreslagna 2 mom. ska Myndigheten för digitalisering och befolkningsdata bevara sådana uppgifter i identitetsmatchningsprocessen som avses i bestämmelser som utfärdats med stöd av artikel 11a i eIDAS-förordningen i högst två år från ingången av kalenderåret efter den tidpunkt då uppgifterna registrerades.

I 3 mom. föreskrivs det om rätten för aktörer inom den privata sektorn att använda identitetsmatchning som tillhandahålls av Myndigheten för digitalisering och befolkningsdata. Enligt kommissionens ovannämnda genomförandeförordning (EU) 2025/846 kan medlemsstaterna om de så vill möjliggöra identitetsmatchning också till e-tjänster inom den privata sektorn. I e-tjänster inom den privata sektorn är det på motsvarande sätt viktigt att identitetsmatchning av dem som sköter ärenden från andra medlemsstater kan göras med uppgifter som redan finns om dem. Identitetsmatchningen är viktig i synnerhet för sådana sammanslutningar och företag som har verksamhet som överskrider medlemsstaternas gränser. Enligt bestämmelsen får privata sammanslutningar, stiftelser och näringsidkare använda identitetsmatchning som tillhandahålls av Myndigheten för digitalisering och befolkningsdata. I praktiken förutsätter detta att de registrerar sig som användare av informationstjänsten för identitetsmatchning. Myndigheten för digitalisering och befolkningsdata kan av aktörer inom den privata sektorn ta ut en avgift för användningsrätt till eller användning av informationstjänsten för identitetsmatchning. Paragrafens 3 mom. tillämpas enligt den föreslagna ikraftträdandebestämmelsen först fr.o.m. den 1 januari 2028.

19 §. Nationell nod. Enligt förslaget föreskrivs det i paragrafen att den nationella noden upprätthålls av Myndigheten för digitalisering och befolkningsdata. Bestämmelsen motsvarar den tidigare 42 c § i autentiseringslagen. Den reviderade eIDAS-förordningen påverkade inte nämnvärt det interoperabilitetsramverk som föreskrivs i artikel 12 i förordningen och i vilket den nationella noden ingår. Det behövs således fortfarande reglering i den nationella kompletterande lagstiftningen om Myndigheten för digitalisering och befolkningsdatas uppgift att upprätthålla den nationella noden.

3 kap. Betrodda tjänster

Kapitlets 20–22 § motsvarar 4 a kap., dvs. 39–41 § i den gällande autentiseringslagen. I fortsättningen ingår all reglering som kompletterar eIDAS-förordningen, inklusive den kompletterande regleringen om betrodda tjänster, i den nya eIDAS-lag som nu föreslås. Den reviderade eIDAS-förordningen kräver inga ändringar i dessa bestämmelser i den kompletterande nationella lagstiftningen om betrodda tjänster. De överförs därmed nästan som sådana från autentiseringslagen. Det görs endast små terminologiska preciseringar i bestämmelserna. I fråga om 20–22 § i den föreslagna eIDAS-lagen gäller det som i specialmotiveringen i den ursprungliga regeringspropositionen om autentiseringslagen (RP 36/2009 rd) samt i regeringspropositionen om ändring av autentiseringslagen (RP 74/2016 rd) konstaterades om 39–41 § i autentiseringslagen.

23 §. Myndigheten för digitalisering och befolkningsdatas anvisningar för kontroll av attribut mot autentiska källor. Enligt förslaget föreskrivs det i paragrafen att Myndigheten för digitalisering och befolkningsdata har till uppgift att utarbeta anvisningar om de elektroniska medel som kvalificerade leverantörer av betrodda tjänster kan använda när de vill kontrollera de attribut som avses i bilaga VI till eIDAS-förordningen mot autentiska källor i Finland. Genom regleringen genomförs skyldigheten enligt artikel 45 e i den reviderade eIDAS-förordningen, enligt vilken medlemsstaterna för de attribut som avses i bilaga VI kan säkerställa att åtgärder vidtas för att göra det möjligt för kvalificerade leverantörer av betrodda tjänster för elektroniska attributsintyg att på användarens begäran på elektronisk väg kontrollera dessa attribut, om attributen i fråga grundar sig på register som förs inom den offentliga sektorn. Kommissionen har antagit en genomförandeförordning (EU) 2025/1569 som kompletterar artikeln, där medlemsstaterna enligt artikel 9.1 ska inrätta mekanismer som möjliggör den kontroll som avses i artikel 45 e i den reviderade eIDAS-förordningen. Enligt samma artikel får medlemsstaterna tillgängliggöra gemensamma kontrollpunkter.

I 1 mom. fastställs en skyldighet för Myndigheten för digitalisering och befolkningsdata att utarbeta anvisningar. I Finland tillgängliggörs således inte någon gemensam kontrollpunkt där kvalificerade leverantörer av betrodda tjänster kan kontrollera alla attribut som avses i bilaga VI. Däremot har den mekanism som inrättas i Finland formen av anvisningar som styr kvalificerade leverantörer av betrodda tjänster till det relevanta offentliga registret för varje attribut och den kvalificerade tillhandahållaren av betrodda tjänster avtalar direkt med registret i fråga om hur det är möjligt att kontrollera uppgifterna i registret. Vid beredningen av propositionen har det bedömts att det inte är ändamålsenligt att inrätta en gemensam kontrollpunkt, eftersom registren inom den offentliga sektorn i Finland redan i stor utsträckning är i elektronisk form och det finns elektroniska gränssnitt till dem, genom vilka den skyldighet som avses i artikel 45 e i den reviderade eIDAS-förordningen kan fullgöras. Hur attributen kontrolleras fastställs alltså för varje attribut enligt förfarandena, de tekniska gränssnitten och regleringen för det befintliga registret.

I 2 mom. finns det närmare bestämmelser om vad de anvisningar som Myndigheten för digitalisering och befolkningsdata utarbetar ska innehålla. Anvisningarna ska åtminstone innehålla en beskrivning av de autentiska källorna i Finland för de attribut som avses i bilaga VI till eIDAS-förordningen samt en beskrivning av de tekniska gränssnitt som är tillgängliga för de autentiska källorna. Syftet är att en kvalificerad leverantör av betrodda tjänster genom anvisningarna ska kunna få tillräcklig information om i vilket register vart och ett av de attribut som avses i bilaga VI finns i Finland samt om de grundläggande tekniska förutsättningarna för att kontrollera attributen. En kvalificerad leverantör av betrodda tjänster kan på grundval av anvisningarna bedöma vilka dess förutsättningar i praktiken är att kontrollera attributen t.ex. i förhållande till det tekniska genomförandet av dess befintliga tjänster.

4 kap. Bedömning av överensstämmelse

24 §. Bedömning av överensstämmelse av den nationella noden. Paragrafen innehåller bestämmelser om bedömning av överensstämmelse av den nationella noden. Enligt den föreslagna 19 § har Myndigheten för digitalisering och befolkningsdata till uppgift att upprätthålla den nationella noden.

I artikel 10.1 i kommissionens genomförandeförordning (EU) 2015/1501 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden konstateras att nodoperatörer som tillhandahåller autentisering ska visa att noden, vad gäller dess deltagande i interoperabilitetsramverket, uppfyller kraven för standarden ISO/IEC 27001 genom certifiering, eller genom en likvärdig bedömningsmetod, eller genom att följa nationell lagstiftning.

Enligt 1 mom. i paragrafen ska Myndigheten för digitalisering och befolkningsdata genom en bedömning som görs av ett godkänt bedömningsorgan för informationssäkerhet som avses i lagen om bedömningsorgan för informationssäkerhet (1405/2011), av ett organ för bedömning av överensstämmelse eller av Transport- och kommunikationsverket visa att den nationella nod som myndigheten upprätthåller med stöd av 19 § uppfyller kraven enligt eIDAS-förordningen och bestämmelser som utfärdats med stöd av den. Myndigheten för digitalisering och befolkningsdata ska också skaffa en bedömningsrapport över bedömningen och lämna den till Transport- och kommunikationsverket, om bedömningen görs av ett bedömningsorgan för informationssäkerhet eller ett organ för bedömning av överensstämmelse.

Nodens verksamhet är kritisk med tanke på gränsöverskridande elektronisk identifiering. Med stöd av 3 § i lagen om bedömning av informationssäkerheten i myndigheternas

informationssystem och datakommunikation (1406/2011) får statsförvaltningsmyndigheterna för bedömning av informationssäkerheten i sina informationssystem och sin datakommunikation bara använda sig av Transport- och kommunikationsverkets tjänster eller av ett sådant bedömningsorgan som har godkänts av Kommunikationsverket enligt lagen om bedömningsorgan. I motiveringen till bestämmelsen (RP 45/2011 rd, s. 11) konstateras det att avsikten är att säkerställa att statsförvaltningsmyndigheterna anlitar bara tillförlitliga externa tjänster för bedömning av informationssäkerheten och att bestämmelsen behövs för att informationssäkerheten inom statsförvaltningen ska utvecklas på ett enhetligt sätt och utan kostnader vars grund är osaklig. Av dessa skäl föreslås det att som nationellt förfarande i Finland när det gäller påvisande av överensstämmelse av noden betraktas en bedömning som görs av ett godkänt bedömningsorgan för informationssäkerhet, av ett organ för bedömning av överensstämmelse (som utsetts och anmälts för bedömning av uppfyllelse av kraven enligt eIDAS-förordningen) eller av Transport- och kommunikationsverket.

I 2 mom. föreskrivs det om Transport- och kommunikationsverkets befogenhet att utfärda närmare föreskrifter om bedömningsgrunderna för bedömning av överensstämmelse av den nationella noden med iakttagande av vad som föreskrivs i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den. Bemyndigandet att meddela föreskrifter motsvarar gällande 30 § 2 mom. i autentiseringslagen.

25 §. Nationell certifieringsordning för europeiska digitala identitetsplånböcker. I artikel 3 i den förordning om certifiering av plånböcker som utfärdats med stöd av artikel 5c i eIDAS-förordningen förutsätts att en ägare till den nationella certifieringsordningen ska utses. I 1 mom. föreslås det att den nationella certifieringsordning för en europeisk digital identitetsplånbok som avses i artikel 5c i eIDAS-förordningen och i bestämmelser som utfärdats med stöd av den i Finland ägs av Transport- och kommunikationsverket. Det kan anses vara ändamålsenligt att uppgiften åläggs Transport- och kommunikationsverket, eftersom verket har kompetens inom och erfarenhet av tillsynen över och bedömningen av överensstämmelse av aktörer för elektronisk identifiering.

Enligt artikel 7.2 i förordningen om certifiering av plånböcker får systemägarna lägga ut hela eller delar av sina uppgifter på en tredje part. Systemägarna ska förbli ansvariga för all verksamhet som läggs ut på entreprenad och som utförs av deras underleverantörer. Av dessa skäl föreskrivs det i 2 mom. om Transport- och kommunikationsverkets rätt att i anslutning till sin uppgift enligt 1 mom. samt i anslutning till utseendet av ett organ för bedömning av överensstämmelse anförtro en biträdande uppgift till en underleverantör som har tillräckliga tekniska förutsättningar och tillräcklig kompetens för uppgiften och som uppfyller vad som föreskrivs i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den samt i denna lag och föreskrifter som utfärdats med stöd av den. Den föreslagna 32 § innehåller bestämmelser om underleverantörers straffrättsliga tjänsteansvar. Underleverantörerna utför sin uppgift på uppdrag av Transport- och kommunikationsverket, vilket innebär att de omfattas av det som i offentlighetslagen föreskrivs om den som utför ett myndighetsuppdrag.

Enligt 3 mom. får Transport- och kommunikationsverket utfärda närmare föreskrifter om den nationella certifieringsordningen för en europeisk digital identitetsplånbok samt om bedömningsgrunderna för bedömning av överensstämmelse av plånboken och om det förfarande som ska iaktas vid bedömning av överensstämmelse, med iakttagande av vad som föreskrivs i eIDAS-förordningen och bestämmelser som har utfärdats med stöd av den. Bemyndigandet att utfärda föreskrifter behövs, eftersom förordningen om certifiering av plånböcker innehåller mycket detaljerade bestämmelser om vilka krav i fråga om olika aktörer och tjänster som ska ingå i den nationella certifieringsordningen. I genomförandeförordningen upprepas delvis kraven enligt standarderna för bedömning av överensstämmelse. Det är

ändamålsenligt att certifieringsordningen som regel beskrivs (t.ex. genom hänvisningar till relevanta bestämmelser och standarder) genom lagstiftning på lägre nivå. Det hör till Transport- och kommunikationsverket att bedöma om och i vilken utsträckning en förpliktande föreskrift ska utfärdas om de ovannämnda frågorna eller huruvida det räcker med en anvisning som beskriver de förfaranden som ska följas och som hänvisar till bestämmelser och standarder som gäller dessa förfaranden. Det föreskrivs om bemyndiganden att utfärda föreskrifter som gäller ett organ för bedömning av överensstämmelse i 26 § 4 mom.

26 §. Utseende och anmälan av organ för bedömning av överensstämmelse. Enligt 1 mom. har Transport- och kommunikationsverket till uppgift att på ansökan av ett organ för bedömning av överensstämmelse utse och till Europeiska kommissionen anmäla ett i Finland etablerat organ för bedömning av överensstämmelse i enlighet med eIDAS-förordningen och bestämmelser som utfärdats med stöd av den. Bestämmelser om utseende och anmälan av organ finns i artiklarna 5c, 12a och 20 i eIDAS-förordningen.

Enligt 2 mom. är en förutsättning för utseende och anmälan att organet för bedömning av överensstämmelse uppfyller de krav som föreskrivs i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den samt i denna lag och föreskrifter som utfärdats med stöd av den och att det har beviljats ett ackrediteringsintyg utfärdat av Säkerhets- och kemikalieverkets ackrediteringsenhet (ackrediteringstjänsten FINAS) eller en utländsk ackrediteringsenhet, enligt vilket organet för bedömning av överensstämmelse inom sitt behörighetsområde uppfyller de angivna kraven. Bestämmelser om de krav som ställs på organ för bedömning av överensstämmelse finns i eIDAS-förordningen och bl.a. i förordningen om certifiering av plånböcker samt i kommissionens genomförandeförordning (EU) 2025/2162 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller ackreditering av organ för bedömning av överensstämmelse som utför bedömning av kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller, rapporten om bedömning av överensstämmelse och systemet för bedömning av överensstämmelse.

Bestämmelser om förutsättningarna för ackreditering finns förutom i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den även i lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (920/2005) samt i förordningen om ackreditering, dvs. Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93.

I de ovannämnda genomförandeförordningarna föreskrivs det om möjligheten för organ för bedömning av överensstämmelse att anlita en underleverantör. Av denna anledning kan ett organ för bedömning av överensstämmelse enligt 3 mom. i sitt uppdrag anlita en underleverantör för vars arbete organet ansvarar som för sitt eget. Underleverantören ska ha tillräckliga tekniska förutsättningar och tillräcklig kompetens för uppgiften och uppfylla de krav för uppgiften som föreskrivs i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den samt i denna lag och föreskrifter som utfärdats med stöd av den. I 32 § föreskrivs det om straffrättsligt tjänsteansvar för anställda hos underleverantörer och personer verksamma i beslutande organ hos underleverantörer. Bestämmelser om hur offentlighetslagen ska tillämpas på verksamheten finns i 31 §.

Enligt 4 mom. får Transport- och kommunikationsverket utfärda närmare föreskrifter om förutsättningarna för att utse ett organ för bedömning av överensstämmelse och de uppgifter som ska ingå i en ansökan om utseende av ett organ för bedömning av överensstämmelse och inlämnandet av uppgifterna till Transport- och kommunikationsverket. Dessutom får Transport-

och kommunikationsverket utfärda föreskrifter om grunderna för bedömning av överensstämmelse i fråga om system för elektronisk identifiering och betrodda tjänster och förfarandet vid bedömning av överensstämmelse. Föreskrifterna ska utfärdas med iakttagande av eIDAS-förordningen och bestämmelser som utfärdats med stöd av den. Kommissionen har genom genomförandeakter fastställt att vissa krav och standarder ska följas vid ackreditering och utseende av organ för bedömning av överensstämmelse. Det kan dock delvis finnas behov av kompletterande föreskrifter av Transport- och kommunikationsverket.

27 §. Tillsyn över organ för bedömning av överensstämmelse. Enligt 1 mom. övervakar Transport- och kommunikationsverket att ett av verket utsett och anmält organ för bedömning av överensstämmelse i sin verksamhet uppfyller de förutsättningar för utseende som avses i 26 § och på behörigt sätt utför de uppgifter som föreskrivs i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den samt i denna lag och föreskrifter som utfärdats med stöd av den.

Enligt 2 mom. ska ett organ för bedömning av överensstämmelse underrätta Transport- och kommunikationsverket om varje ändring som kan ha betydelse för uppfyllandet av villkoren för att utses. Ackrediteringen av organ för bedömning av överensstämmelse är också förknippad med en tillsynsmekanism, utifrån vilken det t.ex. är möjligt att återkalla ett ackrediteringsintyg, varvid bedömningsorganet inte längre uppfyller villkoren för att utses.

Enligt 3 mom. ska Transport- och kommunikationsverket, om inte något annat följer av vad som föreskrivs i eller med stöd av eIDAS-förordningen, ålägga organet för bedömning av överensstämmelse att avhjälpa sina fel eller försummelser inom en skälig tid. Om bestämmelser om ett annat förfarande utfärdas med stöd av eIDAS-förordningen ska dessa följas i stället för denna lag.

I 4 mom. konstateras det att om organet för bedömning av överensstämmelse inte korregerar sin verksamhet inom utsatt tid och ett fel eller en försummelse är väsentlig ska Transport- och kommunikationsverket, om inte något annat följer av vad som föreskrivs i eller med stöd av eIDAS-förordningen, återkalla utseendet av organet för bedömning av överensstämmelse och till Europeiska kommissionen anmäla att organet inte längre uppfyller kraven för anmälan.

28 §. Certifierare av anordningar för skapande av elektroniska underskrifter och elektroniska stämplat. I denna paragraf föreskrivs det om de certifierare av anordningar för skapande av elektroniska underskrifter och elektroniska stämplat som avses i artiklarna 30 och 39 i eIDAS-förordningen. Bestämmelserna i 1 och 2 mom. motsvarar gällande 36 § i autentiseringslagen. I 3 mom. konstateras det att på tillsynen över certifierare och den certifiering som de utför tillämpas vad som i 27, 29 och 30 § föreskrivs om tillsynen över organ för bedömning av överensstämmelse, organets tillsynsuppgifter och tillsynsmetoder samt återkallande av intyg om överensstämmelse. Om något annat föreskrivs om tillsynen över certifierare eller certifieringen med stöd av eIDAS-förordningen ska de bestämmelserna tillämpas i stället för denna lag.

Bemyndigandet att utfärda föreskrifter i 4 mom. motsvarar gällande 42 § 8 punkten i autentiseringslagen. Transport- och kommunikationsverket har med stöd av den gällande lagen meddelat en föreskrift om elektroniska identifieringstjänster och betrodda tjänster (M72 B/2022). I 8 kap. i föreskriften, som gäller certifiering av kvalificerade anordningar för skapande av elektroniska underskrifter och stämplat, konstateras det att för att kraven enligt 36 § i autentiseringslagen ska kunna uppfyllas, krävs tillräcklig kompetens och resurser i fråga om den anordning som certifieras för verifiering av kraven som ställs i eIDAS-förordningen och kommissionens genomförandebeslut (EU) 2016/650 eller ett beslut som ersätter det. Att certifieringsorganet uppfyller kraven kan visas genom en ackreditering eller någon annan oberoende utredning. Ett bevis på kompetens kan också vara att visa att organen omfattas av

SOGIS-MRA-avtalet mellan vissa certifieringsorgan i EU-medlemsstater eller i medlemsstater i EES-området (Senior Officers Group for Information Systems, Mutual Recognition Agreement).

29 §. Tillsynsuppgift och tillsynsmetoder för organ för bedömning av överensstämmelse. Den föreslagna paragrafen innehåller nya bestämmelser, som följer av artikel 16 i förordningen om certifiering av plånböcker. Enligt denna artikel ska de nationella certifieringsordningarna innehålla krav på att organen för bedömning av överensstämmelse (i genomförandeförordningen i fråga "certifieringsorganen") genomför viss kontrollverksamhet, som regleras närmare i förordningen, i fråga om innehavare av ett intyg om överensstämmelse. Kraven på kontrollverksamhet ingår i allmänhet i standarderna för bedömning av överensstämmelse och certifiering, men med stöd av eIDAS-förordningen har ovannämnda genomförandeförordning antagits, och den kan av nationella konstitutionella skäl inte genomföras t.ex. genom att rätten för organet för bedömning av överensstämmelse att få och kontrollera uppgifter fastställs i en föreskrift om ett nationellt certifieringssystem som Transport- och kommunikationsverket utfärdat med stöd av 25 § 3 mom. eller genom anvisningar.

Enligt 1 mom. ska ett organ för bedömning av överensstämmelse utöva tillsyn över att en innehavare av ett intyg om överensstämmelse uppfyller villkoren för erhållande av intyget. Momentet innehåller en definition av innehavare av intyg om överensstämmelse. Med innehavare av intyg om överensstämmelse avses den som ett organ för bedömning av överensstämmelse har beviljat ett intyg om överensstämmelse, dvs. i praktiken en innehavare av intyg om överensstämmelse som avses i Europeiska kommissionens genomförandeakter som antagits med stöd av eIDAS-förordningen. I förordningen om certifiering av plånböcker föreskrivs om innehavaren av ett intyg om överensstämmelse samt om de krav som gäller innehavaren och som ska ingå i den nationella certifieringsordningen. I kommissionens genomförandeförordning (EU) 2025/2162 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller ackreditering av organ för bedömning av överensstämmelse som utför bedömning av kvalificerade tillhandahållare av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller, rapporten om bedömning av överensstämmelse och systemet för bedömning av överensstämmelse avses med intyg om överensstämmelse en handling med vilken ett organ för bedömning av överensstämmelse verifierar ett certifieringsbeslut, där det fastställs att en viss kvalificerad tillhandahållare av betrodda tjänster och de kvalificerade tjänster som denna tillhandahåller uppfyller de krav som anges i eIDAS-förordningen och som är förenliga med artikel 21 i NIS 2-direktivet. I praktiken är innehavare av intyg om överensstämmelse tillhandahållare av europeiska digitala identitetsplånböcker, tillhandahållare av kvalificerade betrodda tjänster samt aktörer som tillhandahåller anordningar för skapande av elektroniska underskrifter eller elektroniska stämplat.

I 2 mom. föreskrivs det på det sätt som förutsätts i förordningen om certifiering av plånböcker om rätten för organ för bedömning av överensstämmelse att få uppgifter. Innehavaren av ett intyg om överensstämmelse ska underrätta organet för bedömning av överensstämmelse om varje ändring som kan ha betydelse för uppfyllandet av villkoren för erhållande av intyget.

Enligt 3 mom. har ett organ för bedömning av överensstämmelse för fullgörande av sin tillsynsuppgift enligt 1 mom. rätt att utföra inspektion av innehavaren av ett intyg om överensstämmelse och av den produkt eller tjänst som innehavaren tillhandahåller och som är föremål för bedömningen.

30 §. Återkallande av intyg om överensstämmelse. På samma sätt som 29 § innehåller också 30 § nya bestämmelser, som följer av artikel 17 i förordningen om certifiering av plånböcker. Enligt den artikeln ska de nationella certifieringsordningarna fastställa konsekvenserna av att en certifierad plånbokslösning och det system för elektronisk identifiering inom ramen för vilket den tillhandahålls inte uppfyller kraven i denna förordning. Kraven på återkallande av certifiering ingår i allmänhet i standarderna för bedömning av överensstämmelse och certifiering, men med stöd av eIDAS-förordningen har ovannämnda genomförandeförordning antagits, och den kan av nationella konstitutionella skäl inte genomföras t.ex. genom att rätten för organet för bedömning av överensstämmelse att förplikta en innehavare av intyg om överensstämmelse eller att återkalla ett intyg om överensstämmelse fastställs i en föreskrift om ett nationellt certifieringssystem som Transport- och kommunikationsverket utfärdat med stöd av 25 § 3 mom.

I 1 mom. föreskrivs det att ett organ för bedömning av överensstämmelse ska ge en uppmaning om att avhjälpa brister, om det konstaterar att innehavaren av ett intyg om överensstämmelse eller den produkt eller tjänst som bedömningen gäller inte uppfyller villkoren för erhållande av intyget om överensstämmelse eller att intyget annars inte borde ha utfärdats.

Enligt 2 mom. ska organet för bedömning av överensstämmelse återkalla intyget om överensstämmelse för viss tid eller helt och hållet eller utfärda det med begränsningar, om inte innehavaren av intyget om överensstämmelse avhjälper bristerna inom utsatt tid.

Om det med stöd av eIDAS-förordningen föreskrivs om något annat förfarande för bedömning av överensstämmelse ska det tillämpas i stället för 1 och 2 mom.

Enligt 3 mom. ska ett organ för bedömning av överensstämmelse underrätta Transport- och kommunikationsverket om de tillsynsåtgärder som avses i 1 och 2 mom. Rapporteringsskyldigheten grundar sig förutom på den ovannämnda genomförandeförordningen även på att Transport- och kommunikationsverket har till uppgift att övervaka innehavare av intyg om överensstämmelse, dvs. exempelvis tillhandahållare av europeiska digitala identitetsplånböcker och tillhandahållare av kvalificerade betrodda tjänster.

31 §. Tillämpning av lagstiftningen om offentlighet samt utlämnande av uppgifter vid bedömning av överensstämmelse. I artikel 20 i förordningen om certifiering av plånböcker konstateras det att enligt de nationella certifieringsordningarna ska alla personer eller organisationer som beviljas tillgång till information vid utförandet av verksamhet inom ramen för den nationella certifieringsordningen vara skyldiga att säkerställa säkerheten för och skyddet av företagshemligheter och annan konfidentiell information, samt att bevara immateriella rättigheter, och vidta nödvändiga och lämpliga tekniska och organisatoriska åtgärder för att säkerställa denna konfidentialitet. Enligt 4 § 2 mom. i offentlighetslagen gäller vad som sägs om en myndighet även sammanslutningar, inrättningar, stiftelser och enskilda personer som utövar offentlig makt och som enligt en lag, en bestämmelse eller en föreskrift som meddelats med stöd av en lag eller en förordning utför ett offentligt uppdrag.

Enligt 1 mom. tillämpas offentlighetslagen på sådana organ för bedömning av informationssäkerhet som avses i 24 §, på organ för bedömning av överensstämmelse och av dem använda underleverantörer samt på certifierare, också när det inte är fråga om utövning av offentlig makt. Offentlighetslagen tillämpas på dessa i fråga om uppgifter i anslutning till verkställigheten av eIDAS-förordningen och bestämmelser som utfärdats med stöd av den samt av denna lag och föreskrifter som utfärdats med stöd av denna lag. Momentet innehåller dessutom en informativ allmän hänvisning till andra allmänna förvaltningslagars lämplighet på det sätt som föreskrivs särskilt i dessa lagar.

I 2 mom. konstateras det att på tystnadsplikten och förbudet mot att utnyttja uppgifter för en person som är anställd hos en i 1 mom. avsedd aktör eller verksam i aktörens beslutande organ och som behandlar sekretessbelagda uppgifter som hänför sig till bedömningsverksamheten tillämpas vad som i 23 § i lagen om offentlighet i myndigheternas verksamhet föreskrivs om tystnadsplikt och förbud mot utnyttjande för den som är anställd hos en myndighet.

Enligt 3 mom. har en i 1 mom. avsedd aktör trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter rätt att på eget initiativ lämna ut handlingar som aktören fått eller upprättat i samband med skötseln av sina uppgifter enligt det momentet samt att röja sekretessbelagd information för Transport- och kommunikationsverket för skötseln av uppgifter som föreskrivs i eIDAS-förordningen eller bestämmelser som utfärdats med stöd av den eller i eIDAS-lagen. Momentet innehåller dessutom en informativ hänvisning till 35 § om Transport- och kommunikationsverkets rätt att få information.

32 §. Straffrättsligt tjänsteansvar vid bedömning av överensstämmelse. I 1 mom. föreskrivs det på det sätt som förutsätts i grundlagen att bestämmelserna om straffrättsligt tjänsteansvar för tjänstemän tillämpas på anställda hos aktörer som sköter en offentlig förvaltningsuppgift och personer verksamma i beslutande organ hos dessa, när de sköter uppgifter som föreskrivs i eIDAS-förordningen eller bestämmelser som utfärdats med stöd av den eller i den föreslagna eIDAS-lagen.

I 2 mom. ingår en informativ hänvisning till skadeståndslagen (412/1974).

5 kap. Tillsyn

33 §. Transport- och kommunikationsverkets uppgifter. I paragrafen föreskrivs det om Transport- och kommunikationsverkets uppgifter i anslutning till eIDAS-förordningen och kompletterande nationell lagstiftning, till den del det inte föreskrivs om dessa ovan i den föreslagna eIDAS-lagen. En del av uppgifterna regleras redan i 42 a § i autentiseringslagen som komplement till den ursprungliga eIDAS-förordningen. Vissa uppgifter är nya, och det är nödvändigt att föreskriva om dessa för att skyldigheterna enligt den reviderade eIDAS-förordningen ska uppfyllas.

En ny uppgift är för det första att utöva tillsyn över efterlevnaden av den föreslagna lagen, vilket det föreskrivs om i den första meningen i paragrafen. Denna bestämmelse ger Transport- och kommunikationsverket behörighet att övervaka att kraven enligt den nationella kompletterande lagstiftningen iakttas.

I 1 punkten åläggs Transport- och kommunikationsverket den nya uppgiften att informera Europeiska kommissionen om de uppgifter som avses i artikel 5a.18 och de bestämmelser som utfärdats med stöd av den artikeln i eIDAS-förordningen. Enligt artikel 5a.18 i den reviderade eIDAS-förordningen förutsätts medlemsstaterna informera kommissionen om det organ som ansvarar för att upprätta och underhålla förteckningen över registrerade förlitande parter som förlitar sig på de europeiska digitala identitetsplånböckerna, de organ som ansvarar för tillhandahållandet av de europeiska digitala identitetsplånböckerna, de organ som ansvarar för att säkerställa att uppgifterna för personidentifiering är kopplade till den europeiska digitala identitetsplånboken, den mekanism som gör det möjligt att validera uppgifter för personidentifiering och de förlitande parternas identitet samt mekanismen för validering av de europeiska digitala identitetsplånböckernas äkthet och giltighet. I kommissionens genomförandeförordning (EU) 2024/2980 preciseras vilka uppgifter som ska lämnas. Paragrafen innehåller dock ingen hänvisning till genomförandeförordningen i fråga, eftersom

det är möjligt att genomförandeförordningarna revideras under de närmaste åren. För att Transport- och kommunikationsverket ska kunna lämna de uppgifter som krävs föreskrivs det i 7 § 3 mom. i eIDAS-lagen om skyldigheten för dem som tillhandahåller plånböcker att lämna uppgifterna i fråga till Transport- och kommunikationsverket.

I 2 *punkten* föreskrivs det också om en ny uppgift för Transport- och kommunikationsverket att informera Europeiska kommissionen och den samarbetsgrupp som avses i artikel 46e.1 om de uppgifter som avses i artikel 5d i den reviderade eIDAS-förordningen och i bestämmelser som utfärdats med stöd av den artikeln. I artikel 5d.2 i den reviderade eIDAS-förordningen föreskrivs det om den information som medlemsstaterna ska lämna. Som exempel kan nämnas certifikatet och rapporten om certifieringsbedömningen för den certifierade europeiska digitala identitetsplånboken, en beskrivning av det system för elektronisk identifiering inom ramen för vilket den europeiska digitala identitetsplånboken tillhandahålls och det tillämpliga tillsynssystemet. I kommissionens genomförandeförordning (EU) 2025/849 preciseras vilka uppgifter som ska lämnas. Paragrafen innehåller dock ingen hänvisning till genomförandeförordningen i fråga, eftersom det är möjligt att genomförandeförordningarna revideras under de närmaste åren. Uppgifterna måste lämnas för att kommissionen ska kunna upprätta en förteckning över alla EU-certifierade plånböcker. Förteckningen och de uppgifter som förs in i den är av avgörande betydelse för att säkerställa förtroendet, öppenheten och enhetligheten i det europeiska plånboksekosystemet som helhet.

För att Transport- och kommunikationsverket ska kunna lämna de uppgifter som krävs föreskrivs det i 7 § i den föreslagna lagen om skyldigheten för dem som tillhandahåller plånböcker att lämna uppgifterna i fråga till Transport- och kommunikationsverket. En tillhandahållare kan inte tillhandahålla sin plånbok som en europeisk digital identitetsplånbok förrän Transport- och kommunikationsverket har lämnat den information som avses i den föreslagna 33 § 2 punkten. När informationen lämnas är det således samtidigt fråga om ett nationellt erkännande av en plånbok. Genom skyldigheten att lämna information får Transport- och kommunikationsverket reda på vilka plånböcker som kommer att tillhandahållas i Finland, och dessutom kan verket göra tillhandahållaren och den plånbok som denna tillhandahåller föremål för tillsynsverksamhet på förhand på det sätt som krävs i artikel 46a i den reviderade eIDAS-förordningen.

Andra nya uppgifter är uppgiften enligt 6 *punkten* att vara tillsynsorgan enligt artikel 46a i den reviderade eIDAS-förordningen och uppgiften enligt 7 *punkten* att vara den gemensamma kontaktpunkt som avses i artikel 46c i den reviderade eIDAS-förordningen. I artikel 46a i den reviderade eIDAS-förordningen föreskrivs det om tillsynen över ramverket för den europeiska digitala identitetsplånboken, och i artikel 46a.1 åläggs medlemsstaterna att utse ett eller flera tillsynsorgan som är etablerade på deras territorium. Tillsynen över ramverket för den europeiska digitala identitetsplånboken går i första hand ut på att övervaka plånböckerna och deras tillhandahållare, men tillsynsorganet har t.ex. också uppgifter som gäller tillsynen över förlitande parter. I artikel 46c i den reviderade eIDAS-förordningen föreskrivs det om gemensamma kontaktpunkter, och i artikel 46a.1 åläggs medlemsstaterna att utse en gemensam kontaktpunkt. De gemensamma kontaktpunkterna ska underlätta gränsöverskridande samarbete och kontakter.

I 8 *punkten* föreskrivs det också om en ny uppgift för Transport- och kommunikationsverket att offentliggöra och till Europeiska kommissionen lämna uppgifter som avses i artikel 48a.2 i eIDAS-förordningen med iakttagande av artikel 48a.3 och 48a.4 i förordningen. Artikel 48a.2 i den reviderade eIDAS-förordningen gäller medlemsstaternas rapporteringskrav och förutsätter att medlemsstaterna varje år lämnar en rapport till kommissionen med de uppgifter som anges i artikeln. Transport- och kommunikationsverket har till uppgift att offentliggöra och lämna

uppgifterna i fråga till kommissionen. Transport- och kommunikationsverket begär med stöd av den rätt att få uppgifter som fastställs i 35 § de uppgifter som ska rapporteras av de aktörer som har uppgifterna i fråga. I regel fås de uppgifter som avses i artikel 48a hos andra myndigheter och hos Transport- och kommunikationsverket själva.

Till Transport- och kommunikationsverkets uppgifter hör redan nu de uppgifter som avses i *punkterna 3–5* samt den i 6 punkten avsedda uppgiften att vara det tillsynsorgan som avses i artikel 46b i den reviderade eIDAS-förordningen. I den artikeln föreskrivs det om tillsyn över betrodda tjänster och artikeln motsvarar i stort sett artikel 17 i den ursprungliga eIDAS-förordningen, med stöd av vilken Transport- och kommunikationsverkets nuvarande uppgift att övervaka betrodda tjänster regleras i 42 b § i autentiseringslagen. Som det beskrivits ovan i avsnitt 4.1 kommer i fortsättningen alla bestämmelser som kompletterar eIDAS-förordningen att ingå i den nya eIDAS-lagen som föreslås. Av denna anledning överförs Transport- och kommunikationsverkets befintliga uppgifter i anslutning till eIDAS-förordningen från autentiseringslagen till den nya lag som föreslås i propositionen.

34 §. Prioritetsordning för Transport- och kommunikationsverkets uppgifter och lämnande av ett ärende utan prövning. I 1 mom. föreskrivs det om Transport- och kommunikationsverkets rätt att ställa sina uppgifter enligt den föreslagna eIDAS-lagen i viktighetsordning i enlighet med uppgiftens betydelse för fullgörandet av de skyldigheter som föreskrivs i den föreslagna eIDAS-lagen eller eIDAS-förordningen eller i bestämmelser eller föreskrifter som utfärdats med stöd av dem. Det är fråga om en procedurbestämmelse, enligt vilken prioritetsordningen fastställs utifrån hur viktiga ärendena är. Ju viktigare ett ärende är, desto högre prioritet har det.

Enligt 2 mom. får Transport- och kommunikationsverket lämna ett ärende utan prövning, om ärendet trots en misstanke om fel eller försummelser endast har en ringa betydelse. Transport- och kommunikationsverket ska dock sträva efter att finna en lösning i ärendet t.ex. genom rådgivning. Transport- och kommunikationsverket ska genast när det är möjligt fatta beslut om att inte ta upp ett ärende till prövning. I många fall kan man redan i ett tidigt skede efter att ett ärende blivit anhängigt bedöma om ärendet har ringa betydelse och på denna grund ska lämnas utan prövning. Det är emellertid också möjligt att fatta ett beslut om att inte ta upp ärendet till prövning senare, oberoende av om ärendet redan har utretts en längre tid.

Syftet med paragrafen är att Transport- och kommunikationsverket ska kunna rikta sina resurser på sådana ärenden som är av störst betydelse för att uppnå målen för den föreslagna eIDAS-lagen eller eIDAS-förordningen. Motsvarande prioriteringsbestämmelser finns i 313 § i lagen om tjänster inom elektronisk kommunikation, 27 § i cybersäkerhetslagen, 12 § i lagen om tillsyn över förvaltningen och delningen av data samt 7 § i lagen om Konkurrens- och konsumentverket.

35 §. Rätt att få information. Paragrafen innehåller bestämmelser om Transport- och kommunikationsverkets rätt att få information. Enligt paragrafen har Transport- och kommunikationsverket trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att av andra myndigheter, tillhandahållare av en europeisk digital identitetsplånbok och plånbokens användare, förlitande parter, tillhandahållare av en betrodd tjänst och användare av tjänsten, organ för bedömning av överensstämmelse, certifierare, tillhandahållare av system för elektronisk identifiering och av dem som handlar för deras räkning få de uppgifter som är nödvändiga för att verket ska kunna utföra sina uppgifter enligt denna lag och eIDAS-förordningen samt bestämmelser som utfärdats med stöd av dem.

Den föreslagna regleringen är nödvändig för att Transport- och kommunikationsverket ska kunna utföra de uppgifter som det åläggs i den föreslagna eIDAS-lagen och den reviderade

eIDAS-förordningen. Enligt artikel 46a.4 b i den reviderade eIDAS-förordningen hör det till tillsynsorganets uppgifter att begära information som är nödvändig för att övervaka efterlevnaden av den förordningen. Dessutom förutsätts det i artikel 24.2 andra stycket i den reviderade eIDAS-förordningen att tillsynsorganet ska få begära även andra uppgifter än de som avses i artikel 24.2 första stycket. Vidare har Transport- och kommunikationsverket enligt den föreslagna 33 § flera uppgifter som hänför sig till lämnande av information, och rätten att få information har också samband med fullgörandet av dessa uppgifter. Syftet med regleringen är också att mer allmänt säkerställa att tillsynsmyndigheten på det sätt som avses i artiklarna 46a och 46b i den reviderade eIDAS-förordningen har de befogenheter som krävs för att utföra sina uppgifter.

Det är inte möjligt att på förhand fastställa eller ge en uttömmande förteckning över den information som krävs för utförandet av uppgifterna. Följaktligen är rätten att få information i denna paragraf bunden vid att den information som rätten gäller är nödvändig för skötseln av uppgifterna i enlighet med grundlagsutskottets utlåtandepraxis (bl.a. GrUU 13/2023 rd, GrUU 17/2016 rd). Rätten att få information gäller också sekretessbelagd information, om denna är nödvändig för skötseln av uppgifterna.

36 §. Rätt att lämna ut sekretessbelagd information. Enligt paragrafen har Transport- och kommunikationsverket rätt att trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att lämna ut information till vissa andra myndigheter samt att själv behandla den i vissa uppgifter enligt andra lagar och EU-bestämmelser. Den föreslagna regleringen behövs för att Transport- och kommunikationsverket ska kunna fullgöra de skyldigheter som i artiklarna 46a–46d i eIDAS-förordningen åläggs den gemensamma kontaktpunkten och tillsynsmyndigheten. Det är i praktiken nödvändigt att säkerställa ett smidigt samarbete mellan myndigheterna i form av utlämnande eller användning av information, eftersom dataombudsmannen och Transport- och kommunikationsverket i egenskap av tillsynsmyndighet enligt NIS 2-direktivet, dvs. cybersäkerhetslagen, och myndighet för cybersäkerhetscertifiering inom ramen för sin behörighet övervakar samma tillhandahållare av tjänster. Olika störningar och säkerhetsincidenter kan gälla ärenden som övervakas av flera olika myndigheter. Utlämnandet och användningen av uppgifterna begränsas till de uppgifter som är nödvändiga för respektive behörig myndighets uppgifter.

Enligt *1 mom. 1 punkten* har Transport- och kommunikationsverket trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att på eget initiativ eller på begäran lämna ut handlingar som verket fått eller upprättat i samband med skötseln av sina uppgifter enligt den föreslagna eIDAS-lagen och eIDAS-förordningen samt att röja sekretessbelagd information till dataombudsmannen, om det är nödvändigt för skötseln av dennes lagstadgade tillsynsuppgifter. När det gäller att på det sätt som avses i artikel 46a.4 g och artikel 46b.4 f i eIDAS-förordningen informera en behörig myndighet som inrättats enligt artikel 51 i dataskyddsförordningen ska denna information i en situation där en omständighet observeras i samband med tillsyn som sker i Finland lämnas till dataombudsmannen, även om den tillsynsmyndighet som i situationen i fråga är behörig med stöd av den allmänna dataskyddsförordningen är etablerad i en annan EU-medlemsstat. Dataombudsmannen överväger med stöd av den allmänna dataskyddsförordningen och dataskyddslagen de åtgärder som behövs i situationen. Tillsynsmyndighetens skyldighet att informera dataombudsmannen påverkar dock inte aktörernas skyldigheter och uppfyller således inte t.ex. den personuppgiftsansvariges skyldighet att anmäla personuppgiftsincidenter.

Enligt *1 mom. 2 punkten* har Transport- och kommunikationsverket motsvarande rätt att lämna ut information till tillsynsmyndigheter i andra medlemsstater i Europeiska unionen som avses i artiklarna 46a och 46b i eIDAS-förordningen och gemensamma kontaktpunkter i andra

medlemsstater i Europeiska unionen som avses i artikel 46c i den förordningen, om det är nödvändigt för skötseln av de uppgifter som föreskrivs i eIDAS-förordningen.

Enligt 2 mom. har Transport- och kommunikationsverket i den utsträckning det är nödvändigt rätt att använda sekretessbelagda handlingar och uppgifter som verket upprättat och fått i samband med skötseln av sina uppgifter enligt denna lag och eIDAS-förordningen för skötseln av de uppgifter som tillhör verket som tillsynsmyndighet enligt 26 § i cybersäkerhetslagen (124/2025), som CSIRT-enhet enligt 19 § i den lagen och som gemensam kontaktpunkt enligt 18 § i den lagen samt som myndighet för cybersäkerhetscertifiering enligt 21 § i lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering. Regeringens proposition till riksdagen med förslag till lagstiftning om genomförande av cyberresiliensförordningen (RP 179/2025 rd) har överlämnats till riksdagen. I propositionen föreslås det att det stiftas en ny lag om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering, där det föreskrivs bl.a. om Transport- och kommunikationsverkets uppgifter i egenskap av myndighet för cybersäkerhetscertifiering enligt cybersäkerhetsakten (EU) 2019/881.

37 §. Rätt att utföra inspektioner. I paragrafen föreskrivs det om Transport- och kommunikationsverkets inspektionsrätt. Bestämmelserna motsvarar till stor del den rätt som Transport- och kommunikationsverket enligt 46 § i autentiseringslagen har att utföra inspektioner i anslutning till tillsynen över leverantörer av identifieringstjänster och tillhandahållare av betrodda tjänster. Bestämmelserna behövs också i denna lag för att Transport- och kommunikationsverket ska kunna genomföra inspektioner på det sätt som avses i artikel 46a.4 d och artikel 46b.4 e i den reviderade eIDAS-förordningen.

Enligt 1 mom. har Transport- och kommunikationsverket rätt att utföra inspektioner av en tillhandahållare av en europeisk digital identitetsplånbok och en plånbok som denne tillhandahåller, av ett organ för bedömning av överensstämmelse eller av en certifierare och deras verksamhet, av en tillhandahållare av betrodda tjänster och den betrodda tjänst som denne tillhandahåller samt av dem som handlar för deras räkning. Inspektioner kan utföras för att övervaka att skyldigheterna enligt denna lag eller föreskrifter som utfärdats med stöd av den eller enligt eIDAS-förordningen eller bestämmelser som utfärdats med stöd av den iakttas. Med bestämmelser som utfärdats med stöd av eIDAS-förordningen avses kommissionens genomförandeförordningar.

Enligt 2 mom. förordnar Transport- och kommunikationsverket en inspektör att utföra inspektionen. Inspektören ska vara en tjänsteperson vid Transport- och kommunikationsverket. Inspektioner kan utföras i aktörens lokaler eller informationssystem. En inspektion av ett informationssystem kan t.ex. gå ut på att fastställa informationssäkerheten och tillförlitligheten hos system, produkter eller programvaror. En inspektion av aktörens lokaler kan omfatta t.ex. en inspektion på grundval av skriftligt material, såsom granskning av anvisningar som aktören utarbetat eller beskrivningar av administrativa förfaranden eller kontroll av överensstämmelse i anslutning till lokalsäkerheten. Inspektioner får dock inte förrättas i utrymmen som är avsedda för boende av permanent natur. För att bestämmelserna ska vara tydliga finns det en uttrycklig bestämmelse i momentet om att den som utför en inspektion trots sekretessbestämmelserna eller andra begränsningar i fråga om utlämnande av uppgifter har rätt att få granska sådana uppgifter som är nödvändiga för tillsynsuppgiften. Uttryckliga bestämmelser om Transport- och kommunikationsverkets rätt att få information finns i 35 §.

I 3 mom. finns en materiell hänvisning enligt vilken det som i förvaltningslagen föreskrivs om inspektion också ska iakttas vid sådan inspektion som avses i paragrafen.

38 §. Anmärkning och tillsynsbeslut. I 1 mom. föreskrivs det om Transport- och kommunikationsverkets behörighet att uppmärksamma en aktör som verket utövar tillsyn över med stöd av eIDAS-lagen på brister eller ålägga aktören att inom skälig tid avhjälpa brister i iakttagandet av skyldigheterna enligt denna lag eller föreskrifter som utfärdats med stöd av den eller enligt eIDAS-förordningen eller bestämmelser som utfärdats med stöd av dem. Bestämmelserna motsvarar Transport- och kommunikationsverkets gällande befogenheter enligt 45 § i autentiseringslagen i anslutning till tillsynen över leverantörer av identifieringstjänster och tillhandahållare av betrodda tjänster. Bestämmelserna behövs också i denna lag för att säkerställa att Transport- och kommunikationsverket kan utföra de tillsynsuppgifter som avses i eIDAS-förordningen.

Enligt paragrafen kan Transport- och kommunikationsverket uppmärksamma en aktör på brister i iakttagandet av de skyldigheter som anges i den föreslagna eIDAS-lagen eller eIDAS-förordningen eller i bestämmelser som utfärdats med stöd av dem. Med aktör avses vilken aktör som helst som Transport- och kommunikationsverket övervakar i enlighet med den föreslagna 33 §. I praktiken är det alltså fråga om en aktör som tillhandahåller tjänster enligt eIDAS-lagen eller eIDAS-förordningen eller som bedriver verksamhet enligt dem eller på annat sätt fullgör de skyldigheter som anges i denna lag eller eIDAS-förordningen. Det kan handla om bl.a. en tillhandahållare av europeiska digitala identitetsplånböcker, en förlitande part eller en kvalificerad tillhandahållare av betrodda tjänster. Med bestämmelser som utfärdats med stöd av eIDAS-förordningen avses kommissionens genomförandeförordningar som antagits med stöd av förordningen.

En anmärkning kan ges t.ex. i sådana fall där det inte finns skäl att vidta strängare åtgärder eller när det är fråga om en brist av så ringa betydelse när det gäller iakttagandet av skyldigheterna att det inte är nödvändigt att i efterhand övervaka att verksamheten korrigeras eller att det inte är nödvändigt att särskilt i efterhand anvisa Transport- och kommunikationsverket att avhjälpa bristen. En anmärkning blir således aktuell särskilt vid kortvariga och obetydliga överträdelser av bestämmelserna. Transport- och kommunikationsverket fattar dock också ett tillsynsbeslut om anmärkningen, i vilket ändring kan sökas på det sätt som föreskrivs i 52 § i lagen.

Utöver anmärkningar kan Transport- och kommunikationsverket genom beslut ålägga den som bryter mot eller försummar sina skyldigheter enligt den lagstiftning som avses i paragrafen att inom en skälig tid rätta till sin verksamhet. Bestämmelserna behövs för att Transport- och kommunikationsverket på det sätt som avses i artikel 46a.4 e i den reviderade eIDAS-förordningen ska kunna kräva att tillhandahållare av europeiska digitala identitetsplånböcker ska avhjälpa eventuella brister i uppfyllandet av kraven enligt den förordningen och på det sätt som avses i artikel 46b.4 j ska kunna kräva att tillhandahållare av betrodda tjänster ska avhjälpa eventuella brister i uppfyllandet av kraven enligt den förordningen. Om Transport- och kommunikationsverket således upptäcker fel, försummelser eller andra brister i iakttagandet av skyldigheterna, kan det således ålägga aktören att rätta till sin verksamhet inom utsatt tid. Transport- och kommunikationsverket kan ålägga aktören att avhjälpa konstaterade brister eller försummelser eller att upphöra med verksamhet som strider mot skyldigheterna och att avstå från motsvarande verksamhet i framtiden.

I 2 mom. föreskrivs det om Transport- och kommunikationsverkets behörighet att ålägga aktören att avbryta eller upphöra med tillhandahållandet av tjänsten eller i fråga om kvalificerade betrodda tjänster återkalla tjänstetillhandahållarens eller den av tjänstetillhandahållaren tillhandahållna tjänstens kvalificerade status. Bestämmelserna behövs för att Transport- och kommunikationsverket på det sätt som avses i artikel 46a.5 i den reviderade eIDAS-förordningen ska kunna ålägga tillhandahållaren att tillfälligt eller permanent upphöra med tillhandahållandet av den europeiska digitala identitetsplånboken och på det sätt som avses i

artikel 46b.4 g ska kunna återkalla status som kvalificerad tillhandahållare av betrodda tjänster och till de tjänster som de tillhandahåller. Innan Transport- och kommunikationsverket fattar ett beslut som avses i momentet ska verket ålägga aktören att inom en skälig tid rätta till sin verksamhet genom ett beslut enligt 1 mom., och endast om tjänstetillhandahållaren inte iakttar beslutet i fråga kan Transport- och kommunikationsverket överväga att meddela ett föreläggande om avbrytande eller avslutande av tillhandahållandet av tjänsten. Transport- och kommunikationsverket ska särskilt beakta överträdelsens omfattning, varaktighet och konsekvenser. Ett föreläggande om att avbryta eller avsluta tillhandahållandet av en tjänst eller återkalla kvalificerad status är endast tillämpligt om det föreligger betydande och långvariga brister i iakttagandet av de skyldigheter som följer av bestämmelserna.

Paragrafens 3 mom. gäller endast kvalificerade tillhandahållare av betrodda tjänster och kvalificerade betrodda tjänster som tillhandahålls av dem. I momentet konstateras det att om en behörig myndighet som utsetts eller inrättats med stöd av Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (*NIS 2-direktivet*) eller ett övervakningsorgan som utsetts eller inrättats med stöd av den allmänna dataskyddsförordningen gör en anmälan till Transport- och kommunikationsverket om att en tjänstetillhandahållare eller en tjänst som denna tillhandahåller inte uppfyller de krav som anges i NIS 2-direktivet eller i den allmänna dataskyddsförordningen, får Transport- och kommunikationsverket återkalla statusen som kvalificerad för den kvalificerade tillhandahållaren av betrodda tjänster eller för den berörda tillhandahållna tjänsten. Bestämmelserna behövs för att Transport- och kommunikationsverket ska kunna vidta de åtgärder som avses i artikel 20.3 a och 20.3 b i den reviderade eIDAS-förordningen. I båda fallen ska hänsyn tas till omfattningen, varaktigheten och konsekvenserna av underlåtenheten att uppfylla de föreskrivna kraven. Återkallande av kvalificerad status är endast tillämpligt om det är fråga om betydande och långvarig underlåtenhet att uppfylla kraven.

39 §. *Interimistiska beslut.* I paragrafen föreskrivs det om Transport- och kommunikationsverkets behörighet att fatta interimistiska beslut. Bestämmelserna motsvarar vad som i 45 a § i autentiseringslagen föreskrivs om Transport- och kommunikationsverkets behörighet att fatta interimistiska beslut. Bestämmelserna behövs, eftersom tillhandahållandet av europeiska digitala identitetsplånböcker, elektroniska identifieringssystem och betrodda tjänster kan vara förknippat med överträdelser och störningar som får så allvarliga konsekvenser att tillsynsmyndigheten behöver fatta beslut om interimistiska åtgärder. Det är fråga om sådana överträdelser av skyldigheter som leder till de mest betydande konsekvenserna eller som är allvarligare än överträdelser som är föremål för en anmärkning eller ett tillsynsbeslut enligt 38 §, eftersom Transport- och kommunikationsverket som en interimistisk åtgärd direkt kan förbjuda eller avbryta tillhandahållandet av en viss tjänst utan uppmaning att vidta korrigerande åtgärder. Paragrafen gör det också möjligt att delvis förbjuda eller avbryta tillhandahållandet av en tjänst.

Bestämmelserna behövs också för att säkerställa att medlemsstaternas skyldigheter enligt artikel 5e i den reviderade eIDAS-förordningen och kommissionens genomförandeförordning som utfärdats med stöd av den fullgörs. I 13 § föreskrivs det att tillhandahållaren av en europeisk digital identitetsplånbok i regel ansvarar för medlemsstatens skyldigheter enligt artikel 5e, t.ex. att avbryta användningen och tillhandahållandet av en europeisk digital identitetsplånbok. Transport- och kommunikationsverket kan dock vid behov genom ett interimistiskt beslut säkerställa att de åtgärder som avses i artikel 5e och artikel 10 i den reviderade eIDAS-förordningen vidtas, om tillhandahållaren av plånboken eller systemet för elektronisk identifiering inte vidtar de åtgärder som förordningen förutsätter.

40 §. *Vite, hot om tvångsutförande och hot om avbrytande.* I paragrafen föreskrivs det om Transport- och kommunikationsverkets möjlighet att förena ett beslut med vite, hot om tvångsutförande eller hot om avbrytande. Bestämmelser om föreläggande och verkställande av administrativa sanktioner finns i viteslagen (1113/1990).

41 §. *Avgifter till Transport- och kommunikationsverket.* Paragrafen föreslås innehålla bestämmelser om avgifter till Transport- och kommunikationsverket. De tillsynsavgifter som föreslås i paragrafen täcker de kostnader som Transport- och kommunikationsverket orsakas för skötseln av de tillsynsuppgifter som anges i eIDAS-förordningen, bestämmelser som utfärdats med stöd av den och den föreslagna eIDAS-lagen. Med stöd av eIDAS-förordningen utfärdas flera genomförandeakter som påverkar myndigheternas uppgifter. Bestämmelserna i paragrafen motsvarar delvis 47 § i den gällande autentiseringslagen och har ett nära samband med de ändringar som i det andra lagförslaget föreslås i 47 § i autentiseringslagen. Paragrafen behövs för det första av den orsaken att alla bestämmelser som kompletterar eIDAS-förordningen i framtiden kommer att finnas i den nya eIDAS-lagen. Därför föreslås det att avgifterna i anslutning till betrodda tjänster enligt 47 § i den gällande autentiseringslagen, de organ som ska bedöma deras överensstämmelse och certifieringsorganet (certifierare i den föreslagna eIDAS-lagen) upphävs i autentiseringslagen och överförs till den nya eIDAS-lagen. I eIDAS-lagen föreskrivs det dock inte om avgifter för nationella identifieringstjänster, utan dessa regleras alltså i 47 § i autentiseringslagen. För det andra innehåller paragrafen också bestämmelser om en helt ny avgift, dvs. en avgift för tillhandahållare av europeiska digitala identitetsplånböcker.

I 1 mom. föreskrivs det att en tillhandahållare av europeiska digitala identitetsplånböcker ska betala Transport- och kommunikationsverket en årlig tillsynsavgift på 17 000 euro. Det är fråga om en nationell bestämmelse som motsvarar 47 § 1 mom. i autentiseringslagen, där det föreskrivs om en tillsynsavgift för leverantörer av identifieringstjänster. Den föreslagna avgiften motsvarar också till sin storlek den tillsynsavgift som föreslås för leverantörer av identifieringstjänster i 47 § 1 mom. i det andra lagförslaget. Tillsynsavgiften betraktas konstitutionellt sett som skatt, vilket innebär att det ska föreskrivas om den i lag. Utöver den årliga tillsynsavgiften kan Transport- och kommunikationsverket för behandlingen av en anmälan som lämnats av en plånbokstillhandahållare enligt det föreslagna 7 § 3 mom. i eIDAS-lagen ta ut en avgift för behandling av anmälan enligt lagen om grunderna för avgifter till staten. Det föreslås att avgiftens storlek fastställs på förordningsnivå, dvs. i förordningen om avgifter för elektronisk kommunikation. Vid behandlingen av anmälan är det fråga om att tillsynsmyndigheten bedömer erkännandet av en tillhandahållare av en europeisk digital identitetsplånbok och meddelar bedömningen vidare till Europeiska kommissionen, dvs. en prestation. Bestämmelser om de allmänna grunderna för när statens prestationer ska vara avgiftsbelagda och för storleken av avgifterna finns i lagen om grunderna för avgifter till staten. Förhållandet mellan skatter och avgifter behandlas mer ingående i avsnitt 12.6 om lagstiftningsordningen.

Det föreslås att bestämmelserna om tillsynsavgifter för kvalificerade tillhandahållare av betrodda tjänster i 47 § 2 mom. i den gällande autentiseringslagen flyttas till 2 mom. Tillsynsavgiftens storlek höjs på motsvarande sätt som andra avgifter för identifieringstjänster och betrodda tjänster som redan är i kraft i enlighet med ökningen av kostnadsnivån, och språkliga korrigeringar görs i bestämmelserna. En kvalificerad tillhandahållare av betrodda tjänster ska betala Transport- och kommunikationsverket en årlig tillsynsavgift på 17 000 euro (nu 14 000 euro) för den första kvalificerade betrodda tjänst som den tillhandahåller och en årlig tillsynsavgift på 11 000 euro (nu 9 000 euro) för varje därpå följande kvalificerade betrodda tjänst som den tillhandahåller. Höjningarna baserar sig på Transport- och kommunikationsverkets beräkningar, som bygger på Statistikcentralens prisindex för offentliga

utgifter. När man räknar med en höjning enligt delindexet för löner och andra personalkostnader i prisindexet för offentliga utgifter från 2016 års nivå till 2024 års nivå och en liten avrundning blir den tillsynsavgift som ska betalas för den första tjänsten 17 000 euro om den införs vid utgången av 2026, när lagen ska träda i kraft. Höjningen kan därför anses vara rimlig och motiverad på grundval av den allmänna ökningen av kostnadsnivån och de faktiska kostnader som Transport- och kommunikationsverket orsakas av tillsynen. Utöver tillsynsavgiften tar Transport- och kommunikationsverket ut en ansökningsavgift för behandlingen av en anmälan om inledande av tillhandahållande av tjänster, vars storlek i framtiden bestäms med stöd av förordningen om avgifter för elektronisk kommunikation. I nuläget föreskrivs det om denna avgift i 47 § 2 mom. i autentiseringslagen, där den kallas för registreringsavgift, men det föreslås att bestämmelsen upphävs på lagnivå, eftersom det anses vara fråga om en prestation, dvs. konstitutionellt sett en avgift.

Enligt 3 mom. ska ett organ för bedömning av överensstämmelse betala Transport- och kommunikationsverket en årlig tillsynsavgift på 18 000 euro. Bestämmelsen grundar sig på 47 § 3 mom. i den gällande autentiseringslagen och motsvarar 47 § 2 mom. som föreslås bli ändrat i det andra lagförslaget. Konstitutionellt sett är det fråga om en skatt som ska regleras på lagnivå. Tillsynsavgiftens storlek (nu 15 000 euro) höjs med 3 000 euro, vilket motsvarar den allmänna ökningen av kostnadsnivån.

Enligt 4 mom. ska också en certifierare som utsetts enligt den föreslagna eIDAS-lagen betala Transport- och kommunikationsverket en årlig tillsynsavgift på 18 000 euro. Bestämmelsen grundar sig på 47 § 3 mom. i den gällande autentiseringslagen. Den nuvarande tillsynsavgiften på 15 000 euro höjs med 3 000 euro, vilket motsvarar ökningen av kostnadsnivån. I fortsättningen kan en avgift för behandling av ansökan enligt lagen om grunderna för avgifter till staten tas ut för utseende av ett organ för bedömning av överensstämmelse och en certifierare, och avgiftens storlek fastställs i förordningen om avgifter för elektronisk kommunikation. Därför föreskrivs det inte om dessa i den föreslagna lagen.

I 5 mom. föreskrivs det på motsvarande sätt som i 47 § i autentiseringslagen om vissa detaljer i anslutning till skyldigheten att betala tillsynsavgift. Tillsynsavgiften ska betalas till fullt belopp också under det första verksamhetsåret, även om verksamheten inleds senare under året. Tillsynsavgiften återbetalas inte även om tjänsteleverantören upphör med sin verksamhet under året.

I 6 mom. föreskrivs det om vissa förfaranden i anslutning till tillsynsavgiften. Tillsynsavgiften påförs av Transport- och kommunikationsverket och avgiften är direkt utsökbar. Momentet innehåller också för tydlighetens skull en informativ hänvisning till paragrafen om sökande av ändring. En motsvarande bestämmelse föreslås ingå i 47 § i autentiseringslagen.

I 7 mom. föreslås en informativ hänvisning till lagen om verkställighet av skatter och avgifter (706/2007), som tillämpas på indrivning av tillsynsavgifter. Momentet innehåller dessutom en bestämmelse om dröjsmålsränta. En motsvarande bestämmelse föreslås ingå i 47 § i autentiseringslagen.

Slutligen föreslås i 8 mom. en informativ hänvisning enligt vilken bestämmelser om avgifter för vissa i momentet särskilt angivna prestationer finns i lagen om grunderna för avgifter till staten. Denna informativa hänvisning ansågs vid beredningen vara nödvändig, eftersom syftet är att förtydliga att utöver de tillsynsavgifter som det föreskrivs om i paragrafen kan även andra avgifter som hänför sig till tillhandahållandet av tjänster enligt den reviderade eIDAS-förordningen, såsom avgifter för behandling av anmälan eller ansökan eller registrering av förtroendevalda parter, tas ut i enlighet med lagen om grunderna för avgifter till staten.

Avgifternas storlek fastställs i förordningen om avgifter för elektronisk kommunikation enligt kostnadsmotsvarighetsprincipen, som ingår i lagen om grunderna för avgifter till staten, dvs. avgiftens storlek motsvarar de totala kostnader som utförandet av prestationen orsakar staten. I fråga om avgifter som tas ut för prestationer som gäller identifieringsuppgifter för juridiska personer innehåller momentet en informativ hänvisning till lagen om avgifter för patent- och registerstyrelsens prestationer (1032/1992). Avgifterna kan gälla både ansökningsavgifter, årsavgifter och andra prestationer som hänför sig till identifieringsuppgifter för juridiska personer.

6 kap. Påföljdsavgifter

I 42–46 § föreskrivs det om överträdelser och försummelser av skyldigheterna i den reviderade eIDAS-förordningen som kan leda till att den behöriga myndigheten påför tillhandahållare av betrodda tjänster en påföljdsavgift. Dessa påföljder anknyter till genomförandet av artikel 16.2 i den reviderade eIDAS-förordningen. Enligt den artikeln ska medlemsstaterna säkerställa att överträdelser av denna förordning som begås av kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster medför administrativa sanktionsavgifter.

Transport- och kommunikationsverkets behörighet att påföra påföljdsavgifter. I 42–46 § finns bestämmelser om Transport- och kommunikationsverkets behörighet att påföra tillhandahållare av betrodda tjänster påföljdsavgifter. Transport- och kommunikationsverket har varit och är även i fortsättningen den myndighet som övervakar kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster och har därmed sakkunskap och kompetens om dessa. Därför är det lämpligast att verket ges behörighet att påföra påföljdsavgifter. Enligt 7 a § i lagen om Transport- och kommunikationsverket (935/2018) har Transport- och kommunikationsverket ett påföljdskollegium som har till uppgift att påföra påföljdsavgifter som omfattas av verkets behörighet i sådana fall när påföljdsavgiften överstiger 100 000 euro. Den föreslagna regleringen om Transport- och kommunikationsverkets behörighet att påföra påföljdsavgifter enligt paragrafen behövs emellertid, eftersom den ovannämnda paragrafen inte innehåller bestämmelser om behörigheten att påföra påföljdsavgifter, utan det ska föreskrivas om detta annanstans i lag.

42 §. Påföljdsavgifter för tillhandahållare av betrodda tjänster. Paragrafen innehåller en påföljdsavgift för de artiklar som varje tillhandahållare av betrodda tjänster kan bryta mot. Med tanke på tillämpningen av paragrafen är det således inte relevant om den som tillhandahåller betrodda tjänster är kvalificerad eller inte, eller vilken betrodd tjänst denna tillhandahåller. Enligt *paragrafen* kan en tillhandahållare av betrodda tjänster påföras en påföljdsavgift om tillhandahållaren bryter mot eller försummar den i artikel 15 i den reviderade eIDAS-förordningen föreskrivna skyldigheten att tillhandahålla sina tjänster på ett klart och begripligt språk i enlighet med Förenta nationernas konvention om rättigheter för personer med funktionsnedsättning (FödrS 27/2016) och tillgänglighetskraven i Europaparlamentets och rådets direktiv (EU) 2019/882 (tillgänglighetsdirektivet). Det är fråga om viktiga skyldigheter med tanke på användarna av tjänsterna. Kraven på tillgänglighet enligt artikel 15 främjar en bred tillgång till betrodda tjänster, vilket i sin tur bidrar till att olika elektroniska processer och förfaranden används i olika tjänster.

43 §. Påföljdsavgifter för icke-kvalificerade tillhandahållare av betrodda tjänster. Paragrafen innehåller en påföljdsavgift för de artiklar som icke-kvalificerade tillhandahållare av betrodda tjänster kan bryta mot och som är tillräckligt tydligt formulerade och avgränsade samt väsentliga med tanke på målen i den reviderade eIDAS-förordningen. Bestämmelser om krav som gäller icke-kvalificerade tillhandahållare av betrodda tjänster finns i artikel 19a i den reviderade eIDAS-förordningen, och i denna paragraf föreskrivs det om påförande av påföljdsavgift för

överträdelse av den i artikel 19 a föreskrivna skyldigheten för icke-kvalificerade tillhandahållare av betrodda tjänster att underrätta olika parter om säkerhetsincidenter eller störningar vid tillhandahållandet av tjänsten eller vid genomförandet av de åtgärder som avses i artikel 19a.1. Det är fråga om skyldigheter som är viktiga både för tillhandahållandet av tjänster och ur tillsynsmyndighetens synvinkel. Enligt artikel 46b.3 b övervakar tillsynsmyndigheterna icke-kvalificerade tillhandahållare av betrodda tjänster genom tillsynsverksamhet endast i efterhand, om de tar del av påståenden att dessa icke-kvalificerade tillhandahållare av betrodda tjänster eller de betrodda tjänster som de tillhandahåller inte uppfyller kraven i denna förordning. Skyldigheten att rapportera om säkerhetsincidenter eller störningar i tjänsterna eller i de åtgärder som avses i punkt 1 i den artikeln bidrar till att säkerställa att tillsynsmyndigheten kan vidta tillsynsåtgärder mot en tjänstetillhandahållare för att säkerställa att denna har handlat i enlighet med de krav som ställs på tjänstetillhandahållare och eventuellt kräva korrigerande åtgärder för att undvika framtida säkerhetsincidenter. Det är också viktigt att andra berörda parter informeras om säkerhetsincidenter, så att de genom sina egna åtgärder kan sträva efter att minimera konsekvenserna av incidenterna.

44 §. Påföljdsavgifter för kvalificerade tillhandahållare av betrodda tjänster. Paragrafen innehåller en påföljdsavgift för de artiklar som kvalificerade tillhandahållare av betrodda tjänster kan bryta mot och som är tillräckligt tydligt formulerade och avgränsade samt väsentliga med tanke på målen i den reviderade eIDAS-förordningen. I *1 punkten* föreskrivs det om påförande av påföljdsavgift för överträdelse av skyldigheten enligt artikel 20.1 att lämna in en rapport om bedömning av överensstämmelse till tillsynsorganet eller skyldigheten enligt artikel 20.1a att informera tillsynsorganet om en planerad revision. Det är fråga om skyldigheter som är viktiga ur tillsynsmyndighetens synvinkel. Rapporten om bedömning av överensstämmelse beskriver den kvalificerade betrodda tjänstens överensstämmelse och är därför ett viktigt dokument när tillsynsmyndigheten beviljar en tillhandahållare av betrodda tjänster statusen kvalificerad eller bedömer upprätthållandet av statusen.

I *2 punkten* föreskrivs det om påförande av påföljdsavgift för överträdelse av skyldigheten enligt artikel 21.1 att informera tillsynsorganet om sin avsikt att börja tillhandahålla en kvalificerad betrodd tjänst och samtidigt lämna in en rapport om bedömning av överensstämmelse. Det är fråga om skyldigheter som är viktiga ur tillsynsmyndighetens synvinkel. Enligt artikel 46b.3 a i den reviderade eIDAS-förordningen ska tillsynsmyndigheten genom tillsynsverksamhet på förhand och i efterhand säkerställa att de kvalificerade tillhandahållarna av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i den reviderade eIDAS-förordningen. Om de kvalificerade tillhandahållarna av betrodda tjänster inte på förhand informerar om att de har för avsikt att börja tillhandahålla tjänsten kan tillsynsmyndigheten inte utöva sådan tillsynsverksamhet på förhand som krävs enligt förordningen.

I *3 punkten* föreskrivs det om påförande av påföljdsavgift för överträdelse av skyldigheten enligt artikel 23.2 att se till att en länk till den relevanta förteckningen över betrodda tjänsteleverantörer finns på dess webbplats, när tillhandahållaren av betrodda tjänster använder EU-förtroendemärket. Det är fråga om viktiga skyldigheter med tanke på tjänstens tillförlitlighet. Enligt artikel 23.1 i den reviderade eIDAS-förordningen får kvalificerade tillhandahållare av betrodda tjänster använda sig av EU-förtroendemärket för att på ett enkelt, igenkännligt och tydligt sätt ange de kvalificerade betrodda tjänster som de tillhandahåller. EU-förtroendemärket bör inte användas på villkor som direkt eller indirekt leder till uppfattningen att icke-kvalificerade betrodda tjänster som tillhandahålls av dessa tillhandahållare är kvalificerade. Länken till den relevanta förteckningen över betrodda tjänsteleverantörer anger att EU-förtroendemärket används korrekt, dvs. för att påvisa att tjänsten har statusen kvalificerad.

I 4 punkten föreskrivs det om påförande av påföljdsavgift för överträdelse av skyldigheterna enligt artikel 24.2 ledvis. För det första föreskrivs det om påförande av påföljdsavgift för överträdelse av skyldigheten för en kvalificerad tillhandahållare av betrodda tjänster att informera tillsynsorganet innan en ändring av tillhandahållandet av dess kvalificerade betrodda tjänster genomförs eller dess verksamhet upphör. Dessutom föreskrivs det om påförande av påföljdsavgift för överträdelse av tillhandahållarens skyldighet att innan ett avtalsförhållande ingås informera om de exakta villkoren och förutsättningarna för användningen av den kvalificerade betrodda tjänsten samt att använda tillförlitliga system för att lagra uppgifter som har lämnats till den. Det är fråga om viktiga skyldigheter både ur tillsynsmyndighetens och användarens perspektiv och med tanke på dataskyddet. Enligt artikel 46b.3 a i den reviderade eIDAS-förordningen ska tillsynsmyndigheten genom tillsynsverksamhet på förhand och i efterhand säkerställa att de kvalificerade tillhandahållarna av betrodda tjänster och de kvalificerade betrodda tjänster som de tillhandahåller uppfyller kraven i den reviderade eIDAS-förordningen. Om en tillhandahållare av betrodda tjänster genomför ändringar i sina tjänster kan detta inverka på tjänsternas överensstämmelse, vilket tillsynsmyndigheten ska kontrollera. Ur användarens synvinkel är det viktigt att i samband med att tjänsten tas i bruk ha en tydlig uppfattning om villkoren och förutsättningarna för användningen av tjänsten, så att användaren kan agera enligt dessa.

Vidare föreskrivs det om påförande av påföljdsavgift för överträdelse av skyldigheten enligt artikel 24.2 f b att anmäla incidenter eller störningar vid tillhandahållandet av tjänsten eller genomförandet av de åtgärder som avses i artikel 24.2 f a till tillsynsorganet, de identifierbara berörda personerna, vid behov andra relevanta behöriga organ och, på begäran av tillsynsorganet, allmänheten om det ligger i allmänt intresse. Det är fråga om skyldigheter som är viktiga både för tillhandahållandet av tjänster och ur tillsynsmyndighetens synvinkel. Skyldigheten att anmäla incidenter eller störningar i genomförandet av de åtgärder som avses i artikel 24.2 f a bidrar till att säkerställa att tillsynsmyndigheten kan vidta tillsynsåtgärder mot en tjänstetillhandahållare för att säkerställa att denna har handlat i enlighet med de krav som ställs på tjänstetillhandahållare och eventuellt kräva korrigerande åtgärder för att undvika framtida säkerhetsincidenter. Det är också viktigt att andra berörda parter informeras om säkerhetsincidenter, så att de genom sina egna åtgärder kan sträva efter att minimera konsekvenserna av incidenterna.

Dessutom föreskrivs det om påförande av påföljdsavgift för överträdelse av skyldigheten att registrera och tillgänglighålla all relevant information om uppgifter som den kvalificerade tillhandahållaren av betrodda tjänster har utfärdat och tagit emot. Slutligen föreskrivs det om påförande av påföljdsavgift för överträdelse av skyldigheten enligt artikel 24.2 i att ha en uppdaterad plan för verksamhetens upphörande. Det är fråga om skyldigheter som är viktiga med tanke på dataskyddet och tjänstens allmänna tillförlitlighet. Det är viktigt att alla uppgifter som en tillhandahållare av betrodda tjänster samlat in registreras, eftersom betrodda tjänster kan vara av sådan karaktär att åtgärder som genomförts med hjälp av betrodda tjänster måste kunna verifieras även efter flera år och t.ex. i situationer där tillhandahållandet av tjänsten har upphört. En uppdaterad plan för verksamhetens upphörande gör det möjligt att vid behov avsluta tillhandahållandet av betrodda tjänster som en kontrollerad åtgärd. Betrodda tjänster kan vara kritiska för många användares affärsverksamhet, och med tanke på det är det viktigt att användarna ges möjlighet att vidta åtgärder om en tillhandahållare av betrodda tjänster upphör med sin verksamhet.

45 §. Påföljdsavgift för kvalificerade tillhandahållare av betrodda tjänster som tillhandahåller kvalificerade certifikat. Paragrafen innehåller en påföljdsavgift för de artiklar som kvalificerade tillhandahållare av betrodda tjänster som tillhandahåller kvalificerade certifikat kan bryta mot och som är tillräckligt tydligt formulerade och avgränsade samt väsentliga med tanke på målen

i den reviderade eIDAS-förordningen. I paragrafen föreskrivs det om påförande av påföljdsavgift för överträdelse av den i artikel 24.1 föreskrivna skyldigheten att kontrollera identiteten och eventuella andra attribut för den fysiska eller juridiska person för vilken det kvalificerade certifikatet utfärdas. Dessutom föreskrivs det om påförande av påföljdsavgift för överträdelse av skyldigheten enligt artikel 24.2 k att upprätta och uppdatera en certifikatdatabas, skyldigheten enligt artikel 24.3 att registrera ett återkallande av certifikat i sin certifikatdatabas och offentliggöra återkallandet eller skyldigheten enligt artikel 24.4 att informera om giltigheten eller statusen som återkallad hos kvalificerade certifikat. Det är fråga om skyldigheter som är viktiga med tanke på hanteringen av livscykeln för kvalificerade certifikat och användningen av certifikat. Den tillförlitliga användningen av ett certifikat äventyras om det inte informeras i rätt tid om certifikatets giltighet eller eventuella status som återkallad. Med andra ord, om dessa uppgifter inte finns tillgängliga i rätt tid, kan det äventyra såväl certifikatanvändarens intressen och rättigheter som intressen hos dem som utnyttjar certifikaten i sina tjänster. Den som utnyttjar certifikat i sina tjänster ska dessutom kunna lita på att certifikatet har utfärdats uttryckligen till den fysiska eller juridiska person vars uppgifter förmedlas med certifikatet.

46 §. Påföljdsavgift för kvalificerade tillhandahållare av betrodda tjänster som tillhandahåller kvalificerade elektroniska attributsintyg. Paragrafen innehåller en påföljdsavgift för de artiklar som kvalificerade tillhandahållare av betrodda tjänster som tillhandahåller kvalificerade elektroniska attributsintyg kan bryta mot och som är tillräckligt tydligt formulerade och avgränsade samt väsentliga med tanke på målen i den reviderade eIDAS-förordningen. I paragrafen föreskrivs det om påförande av påföljdsavgift för överträdelse av den i artikel 24.1 föreskrivna skyldigheten att kontrollera identiteten och eventuella andra attribut för den fysiska eller juridiska person till vilken ett kvalificerat elektroniskt attributsintyg utfärdas. Dessutom föreskrivs det om påförande av påföljdsavgift för överträdelse av den i artikel 24.4a föreskrivna skyldigheten att iakttä kraven i artikel 24.3 och 24.4 vid återkallelse av kvalificerade elektroniska attributsintyg. Tillhandahållare av ett elektroniskt attributsintyg som kvalificerats med stöd av artikel 24.4a ska i rätt tid registrera en återkallelse av det kvalificerade elektroniska attributsintyget och offentliggöra statusen återkallad för intyget. När det gäller sådana elektroniska attributsintyg som endast gäller en viss tid ska det i regel anses att ett beslut om återkallande som avses i artikeln inte ska fattas, utan att intyget ska upphöra att gälla efter att tidsfristen löpt ut. Tillhandahållare av ett elektroniskt attributsintyg som kvalificerats med stöd av artikel 24.4a ska dessutom informera alla förlitande parter om giltigheten eller statusen som återkallad hos de kvalificerade elektroniska attributsintyg som de utfärdat.

Det är fråga om skyldigheter som är viktiga med tanke på hanteringen av livscykeln för kvalificerade elektroniska attributsintyg och användningen av elektroniska attributsintyg. Den tillförlitliga användningen av ett elektroniskt attributsintyg äventyras om det inte informeras i rätt tid om det elektroniska attributsintygets giltighet eller eventuella status som återkallad. Med andra ord, om dessa uppgifter inte finns tillgängliga i rätt tid, kan det äventyra såväl attributsintygsanvändarens intressen och rättigheter som intressen hos dem som utnyttjar elektroniska attributsintyg i sina tjänster. Den som utnyttjar elektroniska attributsintyg i sina tjänster ska kunna lita på att intyget har utfärdats uttryckligen till den fysiska eller juridiska person vars uppgifter förmedlas med det elektroniska attributsintyget.

47 §. Påföljdsavgiftens storlek. I paragrafen föreskrivs det om påförande av påföljdsavgift och bedömning av påföljdsavgiftens storlek i enskilda fall. Enligt *1 mom.* grundar sig påförandet av påföljdsavgift och påföljdsavgiftens belopp på en helhetsbedömning, och alla väsentliga omständigheter ska beaktas i bedömningen av påföljdsavgiftens storlek. I skäl 44 i den reviderade eIDAS-förordningen konstateras det att vid fastställandet av sanktionerna bör vederbörlig hänsyn tas till de berörda enheternas storlek, deras affärsmodeller och överträdelsernas allvar. Enligt paragrafen ska dessutom andra omständigheter beaktas i

helhetsbedömningen, såsom det allmänintresse som eftersträvas med påföljden, de åtgärder som tillhandahållaren av betrodda tjänster vidtagit för att lindra eller avhjälpa den skada som överträdelsen orsakat samt eventuella tidigare överträdelser. Det är motiverat att beakta denna typ av omständigheter för att säkerställa att påföljdsavgiften står i proportion till gärningen eller försummelsen. Även i andra EU-förordningar som gäller samhällstjänster och som i viss mån kan jämföras med tillhandahållare av betrodda tjänster har det förutsatts att motsvarande omständigheter ska beaktas. Som exempel kan nämnas Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster) och Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen). Frågan om huruvida en överträdelse eller försummelse är klandervärd ska särskilt bedömas mot bakgrund av de rättsobjekt som den föreslagna lagen och den reviderade eIDAS-förordningen syftar till att skydda.

I vilket fall som helst baserar sig påföljdsavgiften alltid på en helhetsbedömning, där den ska användas i sista hand i förhållande till mindre påföljder eller andra tillsynsåtgärder. I synnerhet i inledningsskedet ska rådgivning och handledning från tillsynsmyndigheten vara det främsta sättet att ingripa i överträdelser av förordningen. Detta gäller särskilt i fråga om mindre tillhandahållare av betrodda tjänster, vars juridiska kompetens och resurser vanligtvis är mer begränsade än hos större tillhandahållare av betrodda tjänster.

Enligt 2 mom. är den påföljdsavgift som påförs en tillhandahållare av betrodda tjänster minst 1 000 euro om påföljdsavgiften påförs en fysisk person, och i annat fall minst 10 000 euro. För att påföljden ska ha en tillräcklig förebyggande effekt ska avgiften vara tillräckligt stor. Den högsta påföljdsavgiften är det lägsta tillåtna maximibeloppet enligt den nivå som förutsätts i artikel 16.2 i den reviderade eIDAS-förordningen. I fråga om fysiska personer fastställs maximibeloppet som ett belopp i euro och i fråga om juridiska personer antingen som ett belopp i euro eller som en procentuell andel av omsättningen, beroende på vilket belopp som är högst. Eftersom påföljdsavgifter av straffkaraktär till sin stränghet kan jämföras med bötesstraff, föreslås det att ingen dröjsmålsränta eller annan dröjsmålspåföljd ska tas ut.

Med omsättning avses enligt 3 mom. omsättning enligt 4 kap. 1 § i bokföringslagen (1336/1997). Med motsvarande omsättning avses i sin tur en omsättning som bedöms på grundval av någon annan utredning. Bestämmelsen gäller eventuella situationer där bokslutet ännu inte är färdigt i samband med fastställandet av påföljdsavgiften eller där ett bokslut ännu inte finns att tillgå, på grund av att affärsverksamheten nyligen har inletts. Vidare gäller bestämmelsen situationer där en administrativ påföljd påförs en myndighet som tillhandahåller betrodda tjänster. Myndigheter har inte en sådan omsättning som avses i bokföringslagen, vilket innebär att när en påföljdsavgift ska fastställas enligt det maximibelopp som anges i paragrafen ska storleken på en procent bestämmas på basis av en avkastning som motsvarar omsättning.

48 §. Avstående från påförande av påföljdsavgift. Paragrafen innehåller bestämmelser om situationer där ingen påföljdsavgift ska påföras en tillhandahållare av betrodda tjänster. Grundlagsutskottet har i sin praxis förutsatt att myndighetens prövning vid beslut om att inte påföra påföljdsavgift ska vara bunden till prövning på ett sådant sätt att påföljdsavgift inte påförs om de villkor som anges i lag är uppfyllda.

Enligt 1 mom. 1 punkten påförs påföljdsavgift inte om överträdelsen av en skyldighet ska anses vara ringa. En överträdelse eller underlåtenhet kan anses vara ringa t.ex. om en aktör på eget initiativ eller omedelbart efter att ha upptäckt sin överträdelse eller underlåtenhet har vidtagit

åtgärder för att korrigera sitt förfarande och de slutliga konsekvenserna därmed förblivit obetydliga. Det kan också vara fråga om en mindre överträdelse eller underlåtenhet om det rör sig om en engångsöverträdelse och det inte handlar om ett kontinuerligt eller återkommande tillvägagångssätt för en tillhandahållare av betrodda tjänster.

Enligt *1 mom. 2 punkten* ska påföljdsavgift inte heller påföras om det ska anses vara uppenbart oskäligt. Det är fråga om en övergripande bedömning där hänsyn kan tas exempelvis till orsakerna till och konsekvenserna av det felaktiga förfarandet, aktörens individuella omständigheter samt frågan huruvida aktören är en fysisk person.

I *2 mom.* föreskrivs det om situationer där överträdelser av förordningen samtidigt uppfyller brottsrekvisiten. För sådana situationer är det nödvändigt att föreskriva att påföljdsavgift inte kan påföras den som misstänks för samma gärning i en förundersökning, en åtalsprövning eller ett brottmål som behandlas i domstol eller den som för samma gärning redan har meddelats en lagakraftvunnen dom. Bestämmelsen motsvarar den s.k. *ne bis in idem*-principen, förbudet mot att påföra flera påföljder av straffkaraktär för samma gärning. Bestämmelsen behövs eftersom påföljdsavgiften till sin storlek kan vara av straffkaraktär.

I *3 mom.* finns det bestämmelser om preskribering av rätten att påföra en påföljdsavgift. Rätten att påföra påföljdsavgift preskriberas om mer än fem år har förflutit sedan överträdelsen eller försummelsen inträffade. Om överträdelsen eller försummelsen har varit fortlöpande räknas preskriptionstiden från det att överträdelsen eller försummelsen upphörde.

49 §. Verkställighet av påföljdsavgift. Enligt paragrafen verkställs en administrativ påföljdsavgift som påförts med stöd av den föreslagna eIDAS-lagen med iakttagande av lagen om verkställighet av böter (672/2002). Rättsregistercentralen ansvarar för verkställigheten av påföljdsavgiften. Den gällande lagen om verkställighet av böter innehåller en allmän bestämmelse om när en administrativ påföljd av straffkaraktär förfaller, och därför är det inte nödvändigt att i denna lag separat föreskriva om när en påföljdsavgift förfaller. Även bestämmelser om den myndighet som tar emot påföljdsavgiften finns i fortsättningen i lagen om verkställighet av böter.

7 kap. Särskilda bestämmelser

50 §. Avvikelse från förvaltningslagens procedurbestämmelser. Enligt 43 § i förvaltningslagen ska förvaltningsbeslut ges skriftligen. Enligt 47 § i förvaltningslagen ska besväransvisning fogas till ett beslut som får överklagas genom besvär. Om det enligt en särskild bestämmelse är förbjudet att anföra besvär eller om beslutet inte är överklagbart, ska enligt lagens 48 § den bestämmelse som ligger till grund för detta anges i beslutet. I 46 § i förvaltningslagen föreskrivs det om skyldigheten att ge anvisningar om hur man begär omprövning. I paragrafen föreskrivs det om de beslut om utfärdande av identifieringsuppgifter för en person och tillhandahållande av betrodda tjänster i fråga om vilka Patent- och registerstyrelsen och Myndigheten för digitalisering och befolkningsdata inte behöver meddela ett separat förvaltningsbeslut, anvisningar om hur man begär omprövning eller upplysning om besvärsförbud. Denna bestämmelse motsvarar vad som i 13 och 14 § i det tredje lagförslaget föreskrivs om beviljande och indragning av e-legitimation på ansökan. Det är inte heller möjligt att söka ändring i eller begära omprövning av de beslut som avses i paragrafen. Bestämmelser om detta finns i de föreslagna 51 och 52 §.

Enligt *1 mom.* ges inte något förvaltningsbeslut eller några anvisningar om hur man begär omprövning eller någon upplysning om besvärsförbud när identifieringsuppgifter för fysiska och juridiska personer enligt 3 och 5 § i denna lag utfärdas eller återkallas i enlighet med

ansökan. Utfärdandet av identifieringsuppgifter för fysiska personer beskrivs ovan i motiveringen till den föreslagna 3 § och utfärdandet av identifieringsuppgifter för juridiska personer i motiveringen till den föreslagna 5 §.

Enligt 2 mom. ges inte något förvaltningsbeslut eller några anvisningar om hur man begär omprövning eller någon upplysning om besvärshöjning i fråga om tillhandahållande av betrodda tjänster för en europeisk digital identitetsplånbok eller avbrytande eller avslutande av tillhandahållandet i enlighet med tjänstemottagarens ansökan. I enlighet med artikel 3.16 i eIDAS-förordningen avses med betrodda tjänster t.ex. skapande och validering av elektroniska underskrifter och elektroniska stämplat. Myndigheten för digitalisering och befolkningsdata tillhandahåller för plånboken en tjänst för skapande och validering av en kvalificerad elektronisk underskrift. Med hjälp av plånboken ska det vara möjligt att genomföra en kvalificerad elektronisk underskrift som uppfyller kraven i eIDAS-förordningen och genomförandeförordningarna.

Identifieringsuppgifter och betrodda tjänster tillhandahålls på begäran av användaren. I de flesta fall återkallas också uppgifter och tjänster på begäran. Dessa situationer innebär inte ett sådant avgörande i ett förvaltningsärende som skulle kräva ett förvaltningsbeslut eller möjlighet att söka ändring. Av denna anledning föreskrivs det i lagen, avvikande från förvaltningslagen, att sökanden i dessa ärenden inte ska ges något förvaltningsbeslut eller några anvisningar om hur man begär omprövning eller någon upplysning om besvärshöjning, om identifieringsuppgifter utfärdas eller återkallas i enlighet med ansökan eller om betrodda tjänster tillhandahålls eller tillhandahållandet av dessa tjänster upphör i enlighet med ansökan. Den föreslagna regleringens förhållande till rättsskyddet behandlas närmare i avsnitt 12.3 nedan. Eftersom det i 68 § i BDS-lagen föreskrivs att beslut om utfärdande av sådana certifikat som Myndigheten för digitalisering och befolkningsdata producerar får undertecknas maskinellt, finns det i den föreslagna bestämmelsen ett behov av att avvika från den paragrafen, eftersom det enligt förslaget inte ska ges något förvaltningsbeslut om betrodda tjänster (t.ex. certifikat) som beviljats för plånboken i enlighet med ansökan.

Enligt 34 § 2 mom. 5 punkten i förvaltningslagen får ett ärende avgöras utan att en part hörs, om ett yrkande som inte rör någon annan part godkänns eller om hörandet av någon annan orsak är uppenbart onödigt. I praktiken behöver en part inte heller höras i dessa fall, där inget förvaltningsbeslut ges. Ett undantag utgör utfärdandet av identifieringsuppgifter för personer under 13 år, vilket kräver vårdnadshavarens samtycke.

51 §. Begäran om omprövning. I paragrafen föreskrivs det om begäran om omprövning i ärenden där det är ändamålsenligt att föreskriva att omprövningsförfarande ska vara det första steget vid sökande av ändring.

Enligt 1 mom. får omprövning begäras av andra avgöranden som Myndigheten för digitalisering och befolkningsdata och Patent- och registerstyrelsen har meddelat med stöd av eIDAS-lagen än sådana som avses i 50 §. Ovannämnda myndigheter ska med stöd av lagen avgöra ärenden som gäller erhållande av identifieringsuppgifter för en person. Dessutom ska Myndigheten för digitalisering och befolkningsdata avgöra andra frågor som gäller tjänster som ska fogas till plånboken. Dessa frågor kan avgöras genom massbeslut och delvis automatiserat. Enligt 53 f § 1 mom. i förvaltningslagen är en förutsättning för automatiserade avgöranden att den fysiska person som avgörandet avser avgiftsfritt till alla delar får begära omprövning av avgörandet genom en omprövningsbegäran enligt 7 a kap. eller ett jämförbart rättsmedel som behandlas hos den myndighet som har fattat beslutet eller hos en myndighet som hör till samma personuppgiftsansvarige som den beslutande myndigheten. Även av denna anledning finns det skäl att föreskriva om möjligheten att begära omprövning av dessa avgöranden. Omprövning

får inte begäras när det gäller avgöranden som Myndigheten för digitalisering och befolkningsdata och Patent- och registerstyrelsen fattar med stöd av 50 § – dvs. beslut i enlighet med ansökan där det enligt den paragrafen inte ska ges något förvaltningsbeslut eller några anvisningar om hur man begär omprövning eller någon upplysning om besvärshöjning. Enligt 53 f § 2 mom. i förvaltningslagen tillämpas möjligheten att begära omprövning när det gäller rättsmedel vid automatiserade avgöranden dock inte, om en parts yrkande, som inte rör någon annan part, godkänns genom ett automatiserat avgörande. Således kan även dessa avgöranden i enlighet med sökandens ansökan vid behov automatiseras.

Enligt 2 mom. får omprövning begäras av ett beslut av Transport- och kommunikationsverket som gäller en avgift som ska betalas till Transport- och kommunikationsverket. Transport- och kommunikationsverkets avgiftsbeslut fattas utan att parterna hörs enligt de grunder för avgifterna som fastställs i lag. Om det uppstår ett fel i ett sådant beslut är omprövningsförfarande det lämpligaste sättet att avhjälpa det.

I paragrafen föreslås det inte att omprövning får begäras i Transport- och kommunikationsverkets övriga beslut, såsom anmärkningar eller tillsynsbeslut. Tillsynsbeslut är ofta komplexa helheter som kräver en lång utredningsprocess. Vid beredningen av tillsynsbeslut ska parterna alltid höras under beredningen av beslutet och vid behov separat ges tillfälle att yttra sig. Om omprövning föreskrivs vara det primära rättsmedlet när det gäller tillsynsbeslut kan detta i onödan fördröja tillgodoseendet av rättsskyddet för den som är föremål för tillsynsbeslutet, eftersom ändring i beslutet inte får sökas genom besvär. Eftersom förvaltningslagen, särskilt dess 6 kap., iakttas vid beredningen av tillsynsbeslut, och parterna ges tillfälle att bli hörda innan beslutet meddelas i enlighet med 34 § i förvaltningslagen, är det osannolikt att sådana fel uppstår i beslutet som kan avhjälpas genom begäran om omprövning.

Enligt 3 mom. ska omprövningsförfarande vara det första steget vid sökande av ändring i ett beslut som fattats av ett organ för bedömning av överensstämmelse eller av en aktör som utför certifieringar av anordningar för skapande av elektroniska underskrifter och elektroniska stämplat, dvs. certifierare. Omprövning av ett beslut som fattats med stöd av eIDAS-lagen eller eIDAS-förordningen eller bestämmelser som utfärdats med stöd av den får begäras hos Transport- och kommunikationsverket. När ett organ för bedömning av överensstämmelse eller en aktör som utför certifieringar av anordningar för skapande av elektroniska underskrifter och elektroniska stämplat fattar ett beslut om överensstämmelse, är avgörandet av betydelse med tanke på rättsskyddet för den som är föremål för bedömningen. Enligt 2 § 3 mom. i förvaltningslagen tillämpas lagen, inklusive bestämmelserna om meddelande av förvaltningsbeslut, också på enskilda då de sköter offentliga förvaltningsuppgifter.

Enligt 49 d § i förvaltningslagen ska en begäran om omprövning göras skriftligen hos den myndighet som fattat beslutet eller hos den som sköter en offentlig förvaltningsuppgift och som fattat beslutet. Det föreslagna 3 mom. är alltså en specialbestämmelse i förhållande till förvaltningslagen, eftersom ändring ska sökas hos någon annan än den som fattat beslutet. Enligt specialmotiveringen till 49 d § i förvaltningslagen kan det exempelvis i situationer där ett förvaltningsbeslut meddelas av en privat förening vara ändamålsenligt att omprövningsbegäran i stället för av denna förening avgörs av den myndighet som övervakar eller styr föreningen i fråga (RP 230/2014 rd, s. 58). Beslut som fattas av ett organ för bedömning av överensstämmelse eller av en certifierare kan i praktiken gälla t.ex. återkallande av certifiering. Om en certifiering återkallas kan detta i sin tur leda till att t.ex. tillhandahållandet av en europeisk digital identitetsplånbok eller en kvalificerad betrodd tjänst avbryts genom ett beslut av Transport- och kommunikationsverket. Det är därför sannolikt att återkallandet av certifieringen i vilket fall som helst kommer att behandlas av ämbetsverket, och således är det

ändamålsenligt att tillsynsmyndigheten i detta fall behandlar och avgör begäran om omprövning.

Paragrafens 4 mom. innehåller en informativ hänvisning till 7 a kap. i förvaltningslagen, där det föreskrivs om förfarandet för begäran om omprövning.

52 §. Besvärsförbud och sökande av ändring i myndighetsbeslut. I paragrafen föreskrivs det om besvärsförbud i fråga om vissa myndighetsbeslut. Vidare föreskrivs det om Transport- och kommunikationsverkets möjlighet att bestämma att vissa beslut som verket fattar är verkställbara innan de har vunnit laga kraft. Till övriga delar innehåller paragrafen informativa hänvisningar till relevanta bestämmelser om sökande av ändring.

Paragrafens 1 mom. innehåller en informativ hänvisning till bestämmelserna om sökande av ändring, dvs. till lagen om rättegång i förvaltningsärenden och till viteslagen.

Enligt 2 mom. får ändring i avgöranden som avses i 50 § och som fattats av Myndigheten för digitalisering och befolkningsdata eller av Patent- och registerstyrelsen inte sökas genom besvär. På grundval av ovannämnda avgöranden kan identifieringsuppgifter för en person och betrodda tjänster tillhandahållas eller återkallas i enlighet med sökandens begäran. Dessa situationer är inte förknippade med ett sådant behov av rättsskydd som skulle kräva ett förvaltningsbeslut eller möjlighet att söka ändring. Av denna anledning föreskrivs det i lagen, avvikande från lagen om rättegång i förvaltningsärenden (808/2019), att ändring inte får sökas i ett avgörande, om identifieringsuppgifter utfärdas eller återkallas i enlighet med ansökan eller om betrodda tjänster tillhandahålls eller tillhandahållandet av dessa tjänster upphör i enlighet med ansökan. I fråga om andra avgöranden som Myndigheten för digitalisering och befolkningsdata och Patent- och registerstyrelsen har meddelat och som inte avses i denna bestämmelse får omprövning begäras i enlighet med 51 §.

Det föreslagna 3 mom. innehåller en informativ hänvisning till lagen om Patent- och registerstyrelsen, i vars 7 § det föreskrivs om sökande av ändring i Patent- och registerstyrelsens beslut i andra ärenden än sådana som gäller industriellt rättsskydd och handelsregisterärenden, om vilka det föreskrivs om ändringssökande i 6 § i den lagen.

Enligt 4 mom. får Transport- och kommunikationsverket i sitt tillsynsbeslut eller interimistiska beslut bestämma att beslutet ska iakttas innan det har vunnit laga kraft. Enligt 123 § i lagen om rättegång i förvaltningsärenden kan förvaltningsdomstolen under den tid ett besvärssärende är anhängigt förbjuda att beslutet verkställs, förordna att verkställigheten ska avbrytas eller förordna om något annat som gäller verkställigheten av beslutet. Ett sådant förordnande som avser verkställigheten kan också gälla en del av beslutet.

53 §. Ikraftträdande. Paragrafen innehåller en ikraftträdandebestämmelse och övergångsbestämmelser. En närmare motivering till lagens ikraftträdande och övergångsbestämmelserna finns i avsnitt 9 (Ikraftträdande).

7.2 Lagen om stark autentisering och betrodda elektroniska tjänster

1 §. Tillämpningsområde. Tillämpningsområdet för autentiseringslagen ändras så att lagen i fortsättningen endast gäller nationella leverantörer av elektroniska identifieringstjänster och nationella elektroniska identifieringstjänster. I fortsättningen ingår de bestämmelser som kompletterar eIDAS-förordningen i den föreslagna eIDAS-lagen. Syftet med ändringen av tillämpningsområdet är dock inte att ändra utgångspunkten att kraven på nationella

identifieringstjänster är förenliga med de krav som eIDAS-förordningen ställer på identifieringsmetoder på tillitsnivån väsentlig.

I det gällande 2 mom. stryks bestämmelsen om att lagen innehåller bestämmelser om tillsynen över efterlevnaden av eIDAS-förordningen och bestämmelser som kompletterar den förordningen. I den senare meningen i momentet stryks hänvisningen till betrodda tjänster, och meningen flyttas i ändrad form till 1 mom. I momentet görs också några lagtekniska korrigeringar. Paragrafens gällande 3 mom. flyttas med oförändrat innehåll men med vissa lagtekniska korrigeringar och blir ett nytt 2 mom.

I 3 mom. finns i fortsättningen en informativ hänvisning till den föreslagna eIDAS-lagen. Hänvisningen behövs eftersom det är fråga om en betydande ändring av lagens tillämpningsområde och den informativa hänvisningen utgör en tydlig indikation till intressentgrupperna att tillämpningsområdet ändras.

2 §. Definitioner. Paragrafen ändras så att definitionerna i 1 mom. 1 och 2 punkten preciseras och så att en definition läggs till som en ny 12 punkt. I definitionen i 1 och 2 punkten förkortas i hänvisningen till EU:s förordning om elektronisk identifiering namnet på förordningen till eIDAS-förordningen. Förkortningen överensstämmer med den nya föreslagna eIDAS-lagen, där förkortningen eIDAS-förordningen används om förordningen. I den nya 12 punkten definieras termen europeisk digital identitetsplånbok. Det är fråga om den europeiska digitala identitetsplånbok som avses i artikel 3.42 i eIDAS-förordningen och som har tillhandahållits i Finland.

Paragrafens 2 mom. upphävs. I momentet stryks hänvisningen till elektroniska underskrifter, betrodda tjänster och avancerad elektronisk underskrift. De bestämmelser som kompletterar eIDAS-förordningen och därmed också de kompletterande bestämmelserna om betrodda tjänster ingår i fortsättningen i den föreslagna eIDAS-lagen. Definitionerna av system för elektronisk identifiering och förlitande part flyttas till 1 mom. och blir nya punkter 13 och 14. Till definitionerna av system för elektronisk identifiering och förlitande part fogas en mer exakt hänvisning till artikel 3.4 och 3.6 i eIDAS-förordningen. Dessutom ändras i hänvisningen till EU:s förordning om elektronisk identifiering namnet på förordningen till eIDAS-förordningen.

7 b §. Information om giltighet för pass, identitetskort eller e-legitimation. E-legitimation jämförs i framtiden med en identitetshandling som utfärdats av en myndighet, t.ex. pass och identitetskort, och kan också användas vid inledande identifiering av en fysisk person. Till 1 mom. fogas en rätt för leverantörer av identifieringstjänster att få information om giltigheten av ett kvalificerat elektroniskt attributsintyg som innehåller uppgifter om e-legitimation. Information om giltigheten fås ur Myndigheten för digitalisering och befolkningsdatas informationssystem, vilket i praktiken innebär att attributsintygets giltighet kontrolleras i en statusförteckning som förs av Myndigheten för digitalisering och befolkningsdata och som Myndigheten för digitalisering och befolkningsdata genomför som en del av tillhandahållandet av elektroniska attributsintyg. Giltigheten för pass och identitetskort kontrolleras alltså i polisens informationssystem. Paragrafrubriken ändras så att den motsvarar innehållet.

Till paragrafen fogas ett nytt 2 mom. om skyldigheten för leverantörer av identifieringsverktyg att se till att pass, identitetskort eller e-legitimation som används vid inledande identifiering är giltiga. I praktiken gäller skyldigheten endast situationer där den inledande identifieringen grundar sig på en finsk identitetshandling. Enligt 17 § i autentiseringslagen kan inledande identifiering också grunda sig på officiella identitetshandlingar som utfärdats av myndigheter i vissa andra länder, men det är inte möjligt att kontrollera giltigheten av dessa handlingar elektroniskt. Skyldigheten att säkerställa att en handling som används vid inledande

identifiering är giltig gäller endast sådana situationer av inledande identifiering som avses i 17 §, dvs. situationer där identiteten hos den som ansöker om ett verktyg för stark autentisering verifieras i samband med att det nya identifieringsverktyget utfärdas. Giltigheten ska i första hand kontrolleras innan identifieringsverktyget utfärdas och överläts till sökanden. Om det dock inte är möjligt att kontrollera giltigheten vid en inledande identifiering, t.ex. på grund av störningar i datatrafiken eller något annat avbrott i användningen, kan den även kontrolleras i efterhand. Leverantören av identifieringsverktyget ska emellertid säkerställa att identifieringsverktyget inte kan användas förrän giltigheten har kontrollerats. Ett identifieringsverktyg kan således överlämnas till sökanden innan giltighetskontrollen har genomförts, men då ska verktyget aktiveras för användning först senare.

Möjligheten att i polisens informationssystem kontrollera giltigheten för pass eller identitetskort som används vid inledande identifiering har funnits alltsedan 2017, men den har sällan utnyttjats av leverantörer av identifieringsverktyg. Regleringen har därför inte lett till någon förbättring av säkerheten vid utfärdande av identifieringsverktyg, utan giltighetskontrollen har varit beroende av identifieringstjänstens egen riskbedömning. Kommunikationsutskottet har ansett att det är viktigt att försöka förhindra missbruk i samband med utfärdande och förnyande av identitetsverktyg för stark autentisering med alla till buds stående medel och att eventuella lagstiftningsbehov som dessa orsakar bör bevakas (KoUB 6/2021 rd). Skyldigheten för leverantörer av identifieringsverktyg att med hjälp av uppgifter från polisens informationssystem kontrollera handlingarnas giltighet kan leda till att säkerheten vid utfärdandet av identifieringsverktyg förbättras i och med att giltigheten i fortsättningen alltid kontrolleras. Kontrollen av giltigheten för pass eller identitetskort i polisens informationssystem är inte en avgiftsbelagd tjänst men kan kräva att leverantören av identifieringsverktyget inrättar en anslutningsserver för den nationella servicekanalen.

12 e §. Förmedling av identifieringstransaktioner baserade på en europeisk digital identitetsplånbok. Paragrafen är ny, och den gäller leverantörer av tjänster för identifieringsförmedling. Enligt paragrafen kan leverantörer av tjänster för identifieringsförmedling förmedla identifieringstransaktioner som baserar sig på en europeisk digital identitetsplånbok till en part som förlitar sig på elektronisk identifiering, trots att bestämmelserna i autentiseringslagen inte tillämpas på plånböcker eller deras tillhandahållare.

Syftet med regleringen är att främja fullgörandet av den skyldighet som anges i artikel 5f.2 i den reviderade eIDAS-förordningen (en mer detaljerad beskrivning av innehållet i denna skyldighet finns i avsnitt 2.2.1). I nuläget köper e-tjänsterna stark autentisering för sina tjänster centraliserat via förtroendenätet (se närmare avsnitt 3.1.1). De tekniska gränssnitt och andra förutsättningar som behövs för förmedling av identifieringstransaktioner till e-tjänster har sålunda byggts i och kring förtroendenätet. Ur de privata e-tjänsternas synvinkel är det sannolikt tydligast och enklast att skyldigheten fullgörs så att identifiering av användare på grundval av plånboken kan ske med hjälp av samma tekniska gränssnitt som den nuvarande starka autentiseringen. Syftet med regleringen är dessutom att generellt stödja omfattande möjligheter att använda plånboken inom samhällets tjänster, även när det inte finns någon skyldighet enligt lag att erbjuda detta.

Regleringen behövs, eftersom det i 12 a § i autentiseringslagen konstateras att endast de leverantörer av identifieringstjänster som har gjort en anmälan enligt lagens 10 § ansluter sig till förtroendenätet. Således kommer endast de identifieringsverktyg som tillhandahålls av dessa leverantörer av identifieringstjänster att göras tillgängliga för leverantörer av tjänster för identifieringsförmedling, som kan tillhandahålla dem vidare till e-tjänsterna. Det föreslås dock inte att autentiseringslagen tillämpas på europeiska digitala identitetsplånböcker eller på tillhandahållare av dessa. Detta beror på att det i princip inte är möjligt att ställa ytterligare

nationella krav på plånböcker enligt den reviderade eIDAS-förordningen och på dem som tillhandahåller dessa, vilket bestämmelserna om leverantörer av identifieringstjänster och förtroendenätet i autentiseringslagen de facto utgör. I praktiken faller alltså de europeiska digitala identitetsplånböckerna och tillhandahållarna av dessa utanför förtroendenätet. Det är därför nödvändigt att separat föreskriva om rätten för leverantörer av tjänster för identifieringsförmedling att förmedla identifieringstransaktioner som baserar sig på en plånbok.

Det är fråga om en möjliggörande reglering, och det är inte obligatoriskt för leverantörer av tjänster för identifieringsförmedling att förmedla identifieringar som baserar sig på en plånbok på samma sätt som i fråga om de identifieringsverktyg som ingår i förtroendenätet. Enligt artikel 5b.10 i eIDAS-förordningen ska mellanhänder som agerar för förlitande parter räknas betraktas som förlitande parter och får inte lagra uppgifter om transaktionens innehåll. I praktiken kräver alltså förmedling av identifiering som baserar sig på en plånbok att leverantören av tjänster för identifieringsförmedling registrerar sig i det register över förlitande parter i anslutning till den europeiska digitala identiteten som förs av Transport- och kommunikationsverket. När en leverantör av tjänster för identifieringsförmedling förmedlar identifiering som baserar sig på en plånbok kan således bestämmelserna om förlitande parter i eIDAS-förordningen tillämpas på detta. När en leverantör av tjänster för identifieringsförmedling däremot är verksam i förtroendenätet och förmedlar identifiering som baserar sig på de identifieringsverktyg som finns där, omfattas denna alltså av bestämmelserna i autentiseringslagen. Leverantörer av tjänster för identifieringsförmedling behöver t.ex. inte ingå ett separat avtal med en tillhandahållare av en europeisk digital identitetsplånbok om förmedling av identifiering som baserar sig på plånboken på samma sätt som med leverantörer av identifieringsverktyg som ingår i förtroendenätet.

17 §. Identifiering av en fysisk person som ansöker om ett identifieringsverktyg. Det föreslås att det till 2 mom. fogas en hänvisning till den e-legitimation som avses i lagen om e-legitimation för att det ska vara möjligt att använda denna vid inledande identifiering. Formuleringen i bestämmelsen är dock inte förpliktande, eftersom utnyttjande av e-legitimation kräver praktiska integrationsåtgärder och ekonomiska resurser från den förlitande parten när systemreformer ska genomföras.

21 a §. Återaktivering av identifieringsverktyg. Det föreslås att en ny paragraf om återaktivering av identifieringsverktyg fogas till i lagen. Vid återaktivering av identifieringsverktyg ska kraven i punkt 2.2.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering iakttas.

I nuläget innehåller autentiseringslagen inga bestämmelser om återaktivering av identifieringsverktyg. Enligt punkt 2.2.3 i bilagan till förordningen om tillitsnivåer för elektronisk identifiering är ett villkor för återaktivering att samma krav angående tilliten som fastställts före upphävandet eller återkallelsen fortsätter att uppfyllas. Återaktivering blir aktuellt i situationer där ett identifieringsverktygs giltighet har upphävts eller återkallats på initiativ av antingen leverantören eller innehavaren av identifieringsverktyget. Det är således fråga om en situation där identifieringsverktygets giltighet har upphävts t.ex. på grund av en säkerhetsrisk eller misstanke om missbruk. Som återaktivering kan i praktiken betraktas t.ex. situationer där en ny PIN-kod installeras i stället för en bortglömd kod eller låsta användarkoder öppnas. I sådana situationer krävs det dock inte att tjänsteleverantören avbryter eller återkallar identifieringsverktygets giltighet innan återaktiveringen genomförs. Det föreslås att begreppet återaktivering används i lagen, eftersom det är förenligt med förordningen om tillitsnivåer för elektronisk identifiering.

24 §. Registrering och användning av uppgifter om identifieringstransaktioner och identifieringsverktyg. Till 2 mom. fogas en skyldighet för leverantörer av identifieringsverktyg

att utan dröjsmål förmedla information om verktyg för stark autentisering som använts vid inledande identifiering av en sökande till leverantören av identifieringsverktyget i fråga. Om det i den inledande identifieringen används ett identifieringsverktyg som tillhandahålls av en annan leverantör av identifieringsverktyg, ska information om den inledande identifieringstransaktionen förmedlas till den berörda leverantören av identifieringsverktyg i samband med identifieringstransaktionen. Syftet med förslaget är att säkerställa att informationen om användningen av ett identifieringsverktyg vid inledande identifiering rör sig mellan tjänsteleverantörerna, varvid det också blir möjligt att på ett effektivare sätt utreda missbrukssituationer.

Informationen om inledande identifiering är också av betydelse för faktureringen av den ersättning som ska betalas för användningen av identifieringstjänsten och vid ansvarsfördelningen i felsituationer. Maximipriset för inledande identifiering har tidigare fastställts genom en temporär lagändring. De temporära ändringarna upphörde att gälla den 31 mars 2023. Därefter har det inte längre föreskrivits om maximipriset för inledande identifiering, och följaktligen är det möjligt för leverantörer av identifieringsverktyg att för denna transaktion ta ut en högre ersättning än för andra identifieringstransaktioner. Skyldigheten att förmedla uppgifter om inledande identifiering säkerställer att rätt pris tas för inledande identifiering och förtydligar ansvarsfördelningen för felsituationer enligt 17 § i autentiseringslagen.

Informationen om inledande identifiering ska förmedlas i samband med identifieringstransaktionen, t.ex. via gränssnittet eller tjänsten för identifieringsförmedling. I övrigt ändras paragrafen inte.

29 §. Bedömning av överensstämmelse hos en elektronisk identifieringstjänst. Paragrafen ändras så att gällande 2 mom. stryks, och gällande 3 mom. flyttas och blir ett nytt 2 mom. Enligt det 2 mom. som föreslås utgå föreskrivs det om bedömningen av överensstämmelse hos ett system för elektronisk identifiering som ska anmälas till Europeiska kommissionen i EU:s förordning om elektronisk identifiering och betrodda tjänster samt i förordningen om tillitsnivåer för elektronisk identifiering. Det föreslås dock att autentiseringslagen inte längre ska innehålla bestämmelser som kompletterar eIDAS-förordningen, utan att de i framtiden ska ingå i den föreslagna eIDAS-lagen. Dessutom stryks i gällande 3 mom. hänvisningen till gällande 2 mom.

30 §. Bedömning av överensstämmelse hos den nationella noden för elektronisk identifiering. Denna paragraf i autentiseringslagen upphävs som helhet. I fortsättningen föreskrivs det om bedömning av överensstämmelse hos den nationella noden för elektronisk identifiering i den föreslagna eIDAS-lagen.

31 §. Inspektionsberättelse. Paragrafens 1 mom. ändras så att hänvisningen till Myndigheten för digitalisering och befolkningsdata stryks. Hänvisningen har tidigare behövts med avseende på den bedömning av överensstämmelse hos den nationella noden som Myndigheten för digitalisering och befolkningsdata ansvarat för. I fortsättningen regleras bedömningen av den nationella nodens överensstämmelse emellertid i den föreslagna eIDAS-lagen, och därför är hänvisningen till Myndigheten för digitalisering och befolkningsdata onödig.

32 §. Fastställande av överensstämmelse hos betrodda tjänster. Denna paragraf i autentiseringslagen upphävs i sin helhet. I fortsättningen ingår motsvarande bestämmelser i den föreslagna eIDAS-lagen.

36 §. Certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter eller kvalificerade elektroniska stämplat. Denna paragraf i autentiseringslagen upphävs i sin helhet. I fortsättningen ingår motsvarande bestämmelser i den föreslagna eIDAS-lagen.

37 §. Verksamheten vid organ för bedömning av överensstämmelse. Paragrafen ändras så att hänvisningarna till certifieringsorgan stryks. Även paragrafens rubrik ändras i överensstämmelse med detta genom att omnämnandet av verksamheten vid certifieringsorgan stryks. Ändringen behövs eftersom överensstämmelsen hos nationella identifieringstjänster inte påvisas genom certifieringar utan genom en bedömning av överensstämmelse. Tidigare har bestämmelserna om certifieringsorgan behövts, eftersom det krävts att sådana anordningar för skapande av kvalificerade elektroniska underskrifter eller kvalificerade elektroniska stämplat som avses i 36 §, som nu föreslås bli upphävd, ska certifieras.

38 §. Återkallande av godkännande som organ för bedömning av överensstämmelse. Paragrafen ändras genom att hänvisningarna till certifieringsorgan stryks. Även paragrafens rubrik ändras i överensstämmelse med detta genom att omnämnandet av verksamheten vid certifieringsorgan stryks. Ändringen behövs eftersom överensstämmelsen hos nationella identifieringstjänster inte påvisas genom certifieringar utan genom en bedömning av överensstämmelse. Tidigare har bestämmelserna om certifieringsorgan behövts, eftersom det krävts att betrodda tjänster enligt 36 §, som nu föreslås bli upphävd, ska certifieras.

4 a kap. Bestämmelser om betrodda tjänster

Det föreslås att 4 a kap. upphävs i sin helhet. De bestämmelser som kompletterar eIDAS-förordningen och därmed också de kompletterande bestämmelserna om betrodda tjänster ingår i fortsättningen i den föreslagna eIDAS-lagen.

42 §. Transport- och kommunikationsverkets föreskrifter. Paragrafen ändras så att det nuvarande 1 mom. som gäller den allmänna styrnings- och utvecklingsuppgiften upphävs och paragrafen i fortsättningen endast föreskriver om de föreskrifter av Transport- och kommunikationsverket som för närvarande ingår i 2 mom. Dessutom upphävs de i det nuvarande 2 mom. angivna bemyndigandena för Transport- och kommunikationsverket att utfärda föreskrifter till den del de gäller bestämmelser som kompletterar eIDAS-förordningen. I fortsättningen ingår all nationell reglering som kompletterar eIDAS-förordningen i eIDAS-lagen, och motsvarande bemyndiganden att utfärda föreskrifter avses ingå i samma lag. Det föreslås också att bemyndigandena att utfärda föreskrifter utökas med ytterligare ett bemyndigande. I övrigt ändras inte de bemyndiganden som ingår i gällande 2 mom. För att rubriken för paragrafen ska motsvara paragrafens nya innehåll föreslås det att den ändras så att hänvisningen till allmän styrning stryks.

Paragrafens 1 mom. upphävs. Efter att lagförslagen i propositionen har trätt i kraft fördelas lagstiftningsansvaret för stark autentisering mellan kommunikationsministeriet och finansministeriet. Det är därför inte längre motiverat att den allmänna styrningen och utvecklingen hör endast till kommunikationsministeriet.

Förslaget om att stryka kommunikationsministeriets allmänna styrnings- och utvecklingsuppgift bedöms inte påverka verksamheten i praktiken. Enligt reglementet för statsrådet (262/2003) ska ministeriet i vilket fall som helst bereda t.ex. lagstiftning som gäller dess ansvarsområde och behandla internationella ärenden samt delta i EU:s institutioners verksamhet. I 14 § i statsrådets förordning om kommunikationsministeriets arbetsordning (470/2023) föreskrivs det om ministeriets interna arbetsfördelning bl.a. i frågor som gäller elektronisk identifiering. Kommunikationsministeriet har dock för närvarande förutom beredning av lagstiftning i praktiken inga andra styrnings- och utvecklingsuppgifter i fråga om elektronisk identifiering och betrodda tjänster, som det hänvisas till i momentet. Ministeriet har t.ex. inte meddelat några relaterade anvisningar, utan Transport- och kommunikationsverket svarar för myndighetsrådgivningen, och vid behov för myndighetsanvisningar, i dessa frågor.

Med tanke på att regleringsansvaret är uppdelat mellan kommunikationsministeriet och finansministeriet kan strykningen av styrnings- och utvecklingsuppgiften t.o.m. i viss mån anses förtydliga nuläget.

I gällande 2 mom. föreskrivs det om Transport- och kommunikationsverkets bemyndiganden att utfärda föreskrifter. Bestämmelser som kompletterar eIDAS-förordningen ingår i fortsättningen i den föreslagna eIDAS-lagen, vilket innebär att det i den gällande 5 punkten (nya 6 punkten) avsedda bemyndigandet att utfärda föreskrifter om grunderna för bedömningen av överensstämmelsen hos en betrodd tjänst och den nationella noden upphävs. Vidare upphävs i den gällande 6 punkten (nya 7 punkten) skyldigheten att beakta vad som föreskrivs i EU:s förordning om elektronisk identifiering. Dessutom upphävs den gällande 8 punkten, enligt vilken Transport- och kommunikationsverket kan utfärda föreskrifter om de krav som ställs på certifieringsorgan, förfarandet vid certifiering och kraven på anordningar för skapande av elektroniska underskrifter och elektroniska stämplat med beaktande av vad som föreskrivs i EU:s förordning om elektronisk identifiering. Bemyndigandet att utfärda föreskrifter behövs inte längre, eftersom nationella identifieringstjänster inte certifieras.

Det föreslås att en ny 5 punkt fogas till bemyndigandena att utfärda föreskrifter, varvid den gällande 5 punkten flyttas och blir 6 punkten. På motsvarande sätt blir gällande 6 och 7 punkten nya 7 och 8 punkter. Enligt den nya 5 punkten får Transport- och kommunikationsverket meddela närmare föreskrifter om de behövliga uppgifter som avses i 24 § 2 mom. och som ska registreras om den inledande identifieringen av sökanden och om de handlingar eller om den elektroniska identifiering som används i den inledande identifieringen. Antalet inledande identifieringar av sökanden på distans har ökat avsevärt. Till exempel fjärravläsning av pass eller identitetskort och andra tillförlitliga metoder för att identifiera sökande på distans utvecklas hela tiden. Leverantörer av identifieringsverktyg kan få in mycket olika uppgifter om inledande identifieringar, beroende på hur en inledande identifiering genomförs. Det är motiverat att mer exakt definiera vilka uppgifter som ska registreras för att säkerställa att de uppgifter som är nödvändiga för att utreda felsituationer finns att tillgå. I synnerhet förfarandet för identifiering på distans ökar behovet av att definiera de tekniska detaljerna om de uppgifter som ska lagras. Bemyndigandet att utfärda föreskrifter omfattar en detaljerad definition av de uppgifter som ska registreras både om identifieringstransaktionen och om den handling som används och även om den elektroniska identifieringen.

42 a §. *Transport- och kommunikationsverkets uppgifter.* I paragrafen stryks 3 mom., där det föreskrivs om Transport- och kommunikationsverkets uppgifter i anslutning till eIDAS-förordningen. Bestämmelser om de uppgifter som anges i den reviderade eIDAS-förordningen finns i fortsättningen i den föreslagna eIDAS-lagen. Dessutom stryks i 2 mom. hänvisningen till de uppgifter som anges i 42 § 1 mom. i lagen, eftersom 42 § 1 mom. föreslås utgå.

42 c §. *Uppgifter som ankommer på Myndigheten för digitalisering och befolkningsdata.* Paragrafen upphävs eftersom bestämmelser om Myndigheten för digitalisering och befolkningsdatas uppgift att upprätthålla en nationell nod i fortsättningen finns i den föreslagna eIDAS-lagen.

45 §. *Administrativa tvångsmedel I 1 mom.* stryks Transport- och kommunikationsverkets behörighet att med stöd av autentiseringslagen ge en anmärkning till den som bryter mot EU:s förordning om elektronisk identifiering eller bestämmelser som utfärdats med stöd av den. I fortsättningen föreskrivs det om tillsynsåtgärder för överträdelser av förordningen i den föreslagna eIDAS-lagen. Det föreslås också att den informativa hänvisningen till viteslagen i momentet stryks, eftersom det inte längre rekommenderas att den lagen används.

45 a §. Interimistiska beslut. I paragrafen stryks Transport- och kommunikationsverkets behörighet att med stöd av autentiseringslagen meddela ett interimistiskt beslut om ett fel eller en försummelse som gäller eIDAS-förordningen eller bestämmelser eller föreskrifter som utfärdats med stöd av den eller om en störning i datasäkerheten. I 1 mom. stryks hänvisningen till eIDAS-förordningen. Formuleringen i paragrafen förtydligas så att det av 1 mom. direkt framgår vilka de interimistiska åtgärderna är, dvs. förbjuda eller avbryta verksamheten. I 2 mom. stryks Transport- och kommunikationsverkets möjlighet att med stöd av autentiseringslagen som en interimistisk åtgärd förbjuda eller avbryta tillhandahållandet av tjänster, som det föreskrivs om direkt i eIDAS-förordningen. Därmed stryks 1–4 punkterna i sin helhet. I fortsättningen föreskrivs det om Transport- och kommunikationsverkets rätt att fatta interimistiska beslut om de berörda aktörerna och tjänsterna i den föreslagna eIDAS-lagen.

46 §. Inspektionsrätt. I paragrafen upphävs Transport- och kommunikationsverkets rätt att med stöd av autentiseringslagen utföra inspektioner av certifieringsorgan för anordningar för skapande av kvalificerade elektroniska underskrifter och elektroniska stämplat, av certifikatutfärdare som tillhandahåller kvalificerade certifikat samt av tillhandahållare av betrodda tjänster och deras tjänster. I 1, 2 och 3 mom. stryks hänvisningarna till certifikatutfärdare som tillhandahåller kvalificerade certifikat och tillhandahållare av betrodda tjänster. I fortsättningen föreskrivs det om Transport- och kommunikationsverkets rätt att utföra inspektioner av de berörda aktörerna i den föreslagna eIDAS-lagen.

47 §. Avgifter till Transport- och kommunikationsverket. I 1 mom. upphävs den första meningen, som gäller en registreringsavgift. I fortsättningen ska en leverantör av identifieringstjänster eller en sammanslutning av tjänsteleverantörer som har gjort en anmälan enligt 10 § betala Transport- och kommunikationsverket en avgift för behandling av anmälan i enlighet med lagen om grunderna för avgifter till staten. Det föreslås att avgiftens storlek i fortsättningen fastställs på förordningsnivå i stället för på lagnivå, dvs. i förordningen om avgifter för elektronisk kommunikation. Vid behandlingen av anmälan är det fråga om att tillsynsmyndigheten på grundval av en anmälan bedömer godkännandet av en tjänsteleverantör och registrerar denna, dvs. en prestation. Bestämmelser om de allmänna grunderna för när statens prestationer ska vara avgiftsbelagda och för storleken av avgifterna finns i lagen om grunderna för avgifter till staten.

Den gällande avgift som enligt lag ska tas ut för registreringen motsvarar inte kostnaderna för registreringen. Det har föreskrivits om registreringsavgiften för leverantörer av identifieringstjänster 2009. Då gick det inte att visa på något tydligt vederlag från det dåvarande Kommunikationsverkets sida för registreringsavgifterna, varvid det ansågs vara fråga om avgifter av skattenatur (RP 36/2009 rd s. 86). År 2009 var det inte möjligt att bedöma om myndigheternas verksamhet överensstämde med prestationerna, eftersom marknaden för identifieringstjänster ännu var under utveckling och det inte fanns någon etablerad verksamhet eller något etablerat antal aktörer. I nuläget är verksamheten etablerad, vilket har lett till att kostnaderna för behandlingen av anmälningar kan identifieras i detalj. En behandlingsavgift kan tas ut i enlighet med kostnadsmotsvarighetsprincipen, eftersom prestationen och myndigheternas kostnader i anslutning till denna kan specificeras och betalningsskyldigheten inte direkt följer av lagen. Därmed kan kriterierna för en avgift anses bli uppfyllda. I samband med motiveringen till lagstiftningsordningen i avsnitt 12.6 görs en mer detaljerad bedömning av vederlagsförhållandet och ändringen på lagstiftningsnivå.

I 1 mom. föreskrivs det även i fortsättningen om en tillsynsavgift som en leverantör av identifieringstjänster eller en sammanslutning av tjänsteleverantörer årligen ska betala till Transport- och kommunikationsverket. Tillsynsavgiftens nuvarande belopp (14 000 euro) höjs med 3 000 euro till följd av en ökning av den allmänna kostnadsnivån. Senast tillsynsavgifterna höjdes var 2016. Höjningen baserar sig på Transport- och kommunikationsverkets beräkningar,

som bygger på Statistikcentralens prisindex för offentliga utgifter. När man räknar med en höjning enligt delindexet för löner och andra personalkostnader i prisindexet för offentliga utgifter från 2016 års nivå till 2024 års nivå och en liten avrundning blir avgiften 17 000 euro om den införs vid utgången av 2026, när lagen ska träda i kraft. Framöver uppgår den årliga tillsynsavgiften således till 17 000 euro per tjänsteleverantör. Höjningen kan anses vara rimlig och motiverad på grundval av den allmänna ökningen av kostnadsnivån och de faktiska kostnader som Transport- och kommunikationsverket orsakas av tillsynen. I motsats till en registreringsavgift betraktas tillsynsavgiften konstitutionellt sett som skatt, vilket innebär att det även i fortsättningen ska föreskrivas om den i lag. Med leverantör av identifieringstjänster avses i paragrafen en leverantör av identifieringstjänster enligt definitionen i 2 § 3 punkten i lagen.

Enligt definitionerna i den reviderade eIDAS-förordningen är den europeiska digitala identitetsplånboken samtidigt en metod för elektronisk identifiering. Kraven på plånboken och tillhandahållandet av den anges dock på ett uttömmande sätt i den reviderade eIDAS-förordningen, och därmed faller plånböckerna och tillhandahållarna av dem utanför den nationella lagstiftningen om stark autentisering. Detta innebär att en tjänsteleverantör som är skyldig att i enlighet med det första lagförslaget betala en tillsynsavgift för den plånbok som denna tillhandahåller inte är skyldig att för samma tjänst betala en tillsynsavgift för leverantörer av identifieringstjänster enligt 1 mom.

Paragrafens 2 mom. upphävs i sin helhet, eftersom det är nödvändigt att i paragrafen stryka alla sådana avgifter till Transport- och kommunikationsverket som har samband med eIDAS-förordningen. I paragrafens 2 mom. föreskrivs det för närvarande om registrerings- och tillsynsavgifter som ska betalas av en kvalificerad tillhandahållare av betrodda tjänster som gjort en anmälan enligt artikel 21 i eIDAS-förordningen och en certifikatutfärdare som tillhandahåller kvalificerade betrodda tjänster. Bestämmelser om dessa ingår i fortsättningen antingen i den föreslagna nya eIDAS-lagen eller, i den mån de betraktas som avgifter i stället för skatt, i lagen om grunderna för avgifter till staten och i den förordning om avgifter för elektronisk kommunikation som utfärdas med stöd av den.

I paragrafens nya 2 mom. föreskrivs det om tillsynsavgiften för ett organ för bedömning av överensstämmelse. Bestämmelser om detta ingår i den gällande paragrafens 3 mom., som flyttas och blir ett nytt 2 mom. Samtidigt höjs tillsynsavgiftens nuvarande belopp (15 000 euro) med 3 000 euro till följd av en ökning av den allmänna kostnadsnivån. Senast tillsynsavgifterna höjdes var 2016. Höjningen kan på grundval av den allmänna ökningen av kostnadsnivån anses vara rimlig och motiverad. Framöver uppgår den årliga tillsynsavgiften till 18 000 euro. I momentet stryks bestämmelsen om att ett organ för bedömning av överensstämmelse är skyldigt betala Transport- och kommunikationsverket en utnämningsavgift på 10 000 euro. I fortsättningen ska en avgift enligt lagen om grunderna för avgifter till staten betalas för behandlingen av en ansökan som avses i lagens 35 §.

Det gällande 4 mom. upphävs i sin helhet av motsvarande orsaker som 2 mom. I det gällande 4 mom. föreskrivs det om de utnämnings- och tillsynsavgifter som ett certifieringsorgan ska betala. Bestämmelser om dessa ingår i fortsättningen antingen i den föreslagna nya eIDAS-lagen eller, i den mån de betraktas som avgifter i stället för skatt, i lagen om grunderna för avgifter till staten och i den förordning om avgifter för elektronisk kommunikation som utfärdas med stöd av den.

De nuvarande 5, 6 och 7 mom. flyttas och blir nya 3, 4 och 5 mom. Från dessa moment stryks hänvisningarna till en registreringsavgift och utnämningsavgift, som det inte längre föreskrivs om i autentiseringslagen. Dessutom görs vissa språkliga ändringar i momenten i syfte att förtydliga ett strukturerat innehåll eller en formulering. Från det gällande 5 mom., dvs. det nya 3

mom., stryks som onödigt ett uttryckligt omnämnande av att tillsynsavgiften täcker Transport- och kommunikationsverkets kostnader för tillsynen över efterlevnaden av denna lag. Transport- och kommunikationsverkets kostnader för att utföra uppgifterna enligt lagen täcks inte av en registrerings- och tillsynsavgift, utan i stället tas det ut en avgift för behandling av anmälan eller ansökan som motsvarar kostnaderna för behandlingen av dessa. Tillsynsavgiften används även i fortsättningen till att täcka Transport- och kommunikationsverkets kostnader för tillsynen över efterlevnaden av lagen, även om det uttryckliga omnämnandet av detta stryks. Bemyndigandet i gällande 6 mom. att genom förordning av kommunikationsministeriet få utfärda närmare bestämmelser om verkställigheten av avgifterna stryks som onödigt. I övrigt ändras inte sakinnehållet i momenten.

I det nya 6 mom. finns en informativ hänvisning enligt vilken det i lagen om grunderna för avgifter till staten föreskrivs om behandlingen av en anmälan som avses i autentiseringslagens 10 § och en ansökan som avses i 35 § samt om den avgift som tas ut för en sådan inspektion som avses i 46 § 1 mom. En informativ hänvisning ansågs vid beredningen vara nödvändig, eftersom den syftar till att klargöra att en avgift som motsvarar kostnaderna för behandlingen av anmälan och ansökan i enlighet med lagen om grunderna för avgifter till staten i fortsättningen tas ut i stället för den registreringsavgift och utnämningsavgift som stryks från 1 och 3 mom. i den gällande paragrafen. Syftet är alltså inte att göra dessa åtgärder avgiftsfria. Behandlingsavgiftens storlek fastställs inte i lag, utan i stället i förordningen om avgifter för elektronisk kommunikation, och den bestäms enligt kostnadsmotsvarighetsprincipen, som ingår i lagen om grunderna för avgifter till staten, dvs. avgiftens storlek motsvarar de totala kostnader som utförandet av prestationen orsakar staten.

49 a §. *Sökande av ändring i beslut av organ för bedömning av överensstämmelse.* Det föreslås att hänvisningarna till sökande av ändring i ett beslut som fattats av ett certifieringsorgan stryks från paragrafen. Bestämmelserna behövs inte längre, eftersom nationella identifieringstjänster inte ska certifieras. I enlighet med denna ändring stryks också omnämnandet av certifieringsorgan i paragrafens rubrik.

Ikraftträdandebestämmelse. Paragrafen innehåller en bestämmelse om stegvist ikraftträdande. En närmare motivering till lagens ikraftträdande finns i avsnitt 9 (Ikraftträdande).

7.3 Lagen om e-legitimation

1 §. *Lagens syfte.* Paragrafen definierar lagens tillämpningsområde och syfte. Lagen gäller ett nytt tillförlitligt sätt att styrka identiteten eller visa bestyrkta personuppgifter. E-legitimation kan till stor del jämföras med fysiska handlingar, pass och identitetskort som utfärdats av en myndighet för att styrka en persons identitet. Även om det är möjligt för användaren att styrka sin identitet med en e-legitimation och det handlar om ett intyg i elektronisk form, är det ändå inte fråga om ett elektroniskt identifieringsverktyg. Förleden ”e” i ordet e-legitimation syftar på ett identitetsbevis som endast finns i elektronisk form i den europeiska digitala identitetsplånboken. E-legitimationen ska i första hand användas vid fysiska besök, men i framtiden kan möjligheterna att utnyttja den utvecklas och utvidgas. När det gäller andra än fysiska besök kan det i framtiden t.ex. finnas användningsområden där det är nödvändigt att kunna visa bestyrkta personuppgifter före ett egentligt fysiskt besök. Det kan bl.a. handla om att boka biljetter eller hotell eller att bekräfta en bokning före incheckning på en flygplats eller ett hotell.

Finska medborgare och utlänningar som vistas i Finland kan få tillgång till e-legitimation för detta ändamål i enlighet med den föreslagna lagen.

2 §. Definitioner. I paragrafen definieras de centrala begrepp som används i lagen. Att definitionerna är exakta är av betydelse med tanke på rättssäkerheten, en konsekvent tillämpning av lagen, myndigheternas uppgifter och EU-lagstiftningens tillämplighet. Exempelvis definitionerna av bestyrkta uppgifter, förlitande part och teknisk utrustning förtydligar den tekniska och rättsliga ramen för e-legitimationer.

I *1 punkten* definieras bestyrkta uppgifter, som avser personuppgifter som ingår i det passregister som avses i 29 § i passlagen eller i det identitetskortsregister som avses i 31 § i lagen om identitetskort. Förutom att de bestyrkta uppgifterna ska ingå i ovannämnda register ska de också, för att vara ännu tillförlitligare, ha verifierats elektroniskt av en myndighet. Den elektroniska verifieringen syftar på behandlingen av uppgifterna under hela deras livscykel. Som exempel kan nämnas åtgärder som tryggar uppgifternas integritet och tillförlitlighet hos både polisen och Myndigheten för digitalisering och befolkningsdata. Åtgärderna omfattar alltså redan t.ex. identifieringen av personen i samband med utfärdande av pass och identitetskort, informationssäkerhetsåtgärder vid behandling och överföring av uppgifter från polisen till Myndigheten för digitalisering och befolkningsdata samt certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för att säkerställa äktheten och integriteten hos de uppgifter som registrerats i den tekniska delen av passet och identitetskortet. Med bestyrkta uppgifter avses också personuppgifter i attributsintyg, som det föreskrivs om i bilaga V till eIDAS-förordningen och i 4 § i den föreslagna lagen om e-legitimation. En datamängd som består av bestyrkta uppgifter som definierats på detta sätt utgör e-legitimationens innehåll. Den förteckning som finns i 4 § 2 mom. i den föreslagna lagen om e-legitimation föreslås utgöra en uttömmande förteckning över de uppgifter som bildar en datamängd.

I *2 punkten* definieras eIDAS-förordningen.

I *3 punkten* definieras förlitande part. Bestämmelsen motsvarar i enlighet med det första lagförslaget den definition som finns i artikel 3.6 i eIDAS-förordningen, enligt vilken förlitande part avser en fysisk eller juridisk person som förlitar sig på elektronisk identifiering, europeiska digitala identitetsplånböcker eller andra medel för elektronisk identifiering eller på en betrodd tjänst. Förlitande parter kan i praktiken förekomma t.ex. i handels- och köpsituationer samt kundservicesituationer eller utgöra parter vid ingående av ett avtalsförhållande eller en myndighet eller privat aktör som övervakar åldersgränser.

I *4 punkten* i paragrafen definieras användare som en fysisk person som Myndigheten för digitalisering och befolkningsdata tillhandahåller ett kvalificerat elektroniskt attributsintyg. Bestämmelser om Myndigheten för digitalisering och befolkningsdatas uppgift att tillhandahålla attributsintyg finns i 7 § 3 mom. Användaren kan endast vara en fysisk person, eftersom en e-legitimation enligt den föreslagna lagstiftningen alltid baserar sig på en sådan identitetshandling, ett sådant pass eller identitetskort, som endast kan beviljas en fysisk person.

I *5 punkten* definieras teknisk utrustning som en mobil terminal eller annan motsvarande utrustning, t.ex. en pekplatta, som användaren av den europeiska digitala identitetsplånboken innehar och i vilken plånboken har tagits i bruk. Definitionen begränsar användningsområdet för e-legitimation till en konkret utrustning, vilket är av avgörande betydelse för informationssäkerheten och användbarheten.

I *6 punkten* definieras europeisk digital identitetsplånbok med en hänvisning till eIDAS-förordningen.

I 7 punkten definieras kvalificerat elektroniskt attributsintyg som ett intyg enligt eIDAS-förordningen som är utfärdat av en kvalificerad tillhandahållare av betrodda tjänster och som uppfyller de krav som anges i bilaga V till eIDAS-förordningen. Definitionen understryker att EU-lagstiftningen lägger grunden för det tekniska genomförandet av e-legitimationen.

I 8 punkten definieras kvalificerad tillhandahållare av betrodda tjänster som en aktör enligt eIDAS-förordningen som tillhandahåller en eller flera kvalificerade betrodda tjänster och som beviljats statusen kvalificerad av det tillsynsorgan som avses i förordningen. Definitionen är viktig med tanke på e-legitimationens tillförlitlighet och överensstämmelsen med EU-lagstiftningen.

I 9 punkten definieras handling som utgör grund för en e-legitimation för det första som ett giltigt finskt pass enligt 3, 3 c eller 4 § i passlagen. Passen enligt de ovannämnda paragraferna är grundläggande pass som beviljas finska medborgare på ansökan (3 §), provisoriskt pass (3 c §) samt diplomatpass och tjänstepass (4 §). Alternativt kan den handling som utgör grund för en e-legitimation vara ett i 2 § 1 mom. i lagen om identitetskort avsett grundläggande identitetskort, även ett identitetskort som används som resedokument, ett i 14 § avsett identitetskort för utlänningar, ett i 15 a § avsett provisoriskt identitetskort eller ett i 17 § 3 mom. avsett identitetskort som inte kan användas som resedokument. Däremot uppfyller t.ex. ett tillfälligt pass eller identitetskort, ett nödpass eller sjömanspass inte definitionen av en handling som utgör grund för e-legitimation. Utfärdandet av handlingar som faller utanför den föreslagna definitionen grundar sig på särskilda omständigheter eller på sökandens uppgifter. Ett tillfälligt pass eller temporärt identitetskort kan t.ex. utfärdas endast av grundad anledning, om det inte är möjligt att ens genom påskyndat förfarande utfärda en handling som upprättats centraliserat. Ett nödpass kan utfärdas i undantagsfall för en resa och endast för att användas för denna resa. Ett tillfälligt pass, sjömanspass, nödpass och temporärt identitetskort innehåller inte heller någon teknisk del. Denna avgränsning är väsentlig för att e-legitimationen ska basera sig på de mest tillförlitliga uppgifterna som bestyrks av en myndighet. I praktiken kräver den föreslagna regleringen ändringar i passlagen och lagen om identitetskort. Ändringarna i lagen om identitetskort föreslås i det fjortonde lagförslaget och ändringarna i passlagen i det sjuttonde lagförslaget. Enligt förslagen innefattar de ovannämnda passen och identitetskorten i framtiden rätten att ta i bruk en e-legitimation som avses i denna föreslagna lag. Lagförslagen innehåller också förslag till övergångsbestämmelser som garanterar att befintliga pass och identitetskort också är giltiga när det gäller att få tillgång till en e-legitimation.

Enligt definitionen i 10 punkten avses med åldersbevis ett attributsintyg eller motsvarande intyg som härletts ur de bestyrkta uppgifterna och med vilket användaren kan bekräfta för en förlitande part att användaren hör till en viss åldersgrupp. Enligt eIDAS-förordningen ska medlemsstaterna integrera olika integritetsbevarande tekniker i den europeiska digitala identitetsplånboken. Ett exempel på sådan teknik är enligt skäl 14 i den reviderade eIDAS-förordningen ett nollkunskapsbevis. Dessa kryptografiska metoder bör göra det möjligt för en förlitande part att validera om ett visst påstående baserat på personens identifieringsuppgifter och attributsintyg är sant, utan att några uppgifter med anknytning till detta påstående förmedlas, och därigenom bevara användarens integritet. I praktiken kan användaren t.ex. på ett tillförlitligt sätt berätta att hon eller han är myndig utan att avslöja sin egentliga ålder. Användaren kan således vara t.ex. 23 eller 45 år gammal, men den enda information som förmedlas till den förlitande parten är att användaren är myndig. I 10 punkten definieras åldersbeviset som ett attributsintyg eller motsvarande intyg som gör det möjligt för användaren att visa att han eller hon tillhör en viss åldersgrupp utan att andra personuppgifter avslöjas. Definitionen stöder således dataskyddet och gör det möjligt att använda åldersbegränsade tjänster utan onödigt utlämnande av personuppgifter. Användning av åldersbevis är av särskild betydelse i situationer där tjänsteleverantören endast behöver försäkra sig om användarens ålder utan att hans eller

hennes födelsedatum, personbeteckning eller andra individualiserande personuppgifter anges. Ett exempel på en sådan situation är en filmvisning med åldersgräns. Definitionen skapar en teknisk och rättslig grund för ett sådant begränsat påvisande av uppgifter och stärker användarens hantering av sina egna uppgifter.

3 §. E-legitimation. I paragrafen föreskrivs det om e-legitimationens rättsliga karaktär. I 1 mom. definieras e-legitimationen utifrån dess användningsändamål. Med en e-legitimation kan användaren styrka sin identitet eller visa sina bestyrkta uppgifter på motsvarande sätt som med det pass eller identitetskort som utgör grund för e-legitimationen. Den föreslagna bestämmelsen stärker kopplingen mellan e-legitimationen och det fysiska passet eller identitetskortet och främjar e-legitimationens ställning som en digital version av dessa och ett pålitligt verktyg för styrkande av identiteten.

Det är önskvärt att e-legitimationen i fortsättningen godkänns i lika stor utsträckning som de traditionella dokumenten. Någon förpliktande bestämmelse om godkännande av e-legitimation föreslås dock inte, och någon sådan ingår inte heller i den gällande lagstiftningen om pass och identitetskort. I praktiken förutsätter användningen av e-legitimation t.ex. inom handeln maskinell kontroll för att det ska kunna säkerställas att en e-legitimation är äkta och giltig. Mellan fysiska personer sker kontrollen med hjälp av den europeiska digitala identitetsplånboken som finns i användarens egen tekniska utrustning.

Användaren kan få e-legitimationen som ett kvalificerat elektroniskt attributsintyg i användarens europeiska digitala identitetsplånbok. Denna bestämmelse skapar en teknisk och rättslig grund för förekomsten och användningen av e-legitimation.

Tillhandahållandet av e-legitimation som ett kvalificerat elektroniskt attributsintyg som avses i eIDAS-förordningen säkerställer att e-legitimationen uppfyller de höga kraven på uppgifternas äkthet, integritet och tillförlitlighet och att tillhandahållandet omfattas av tillsyn. Samtidigt begränsar definitionen intygets användningsområde till den europeiska digitala identitetsplånboken. Med andra ord är det inte möjligt att få en e-legitimation för plånbokslösningar som inte uppfyller kraven i den reviderade eIDAS-förordningen.

I 2 mom. konstateras det att e-legitimationen inte är ett resedokument. Bestämmelsen begränsar e-legitimationens användningsändamål och hindrar att den används vid gränsöverskridande eller internationella resor.

4 §. Uppgifter som ingår i e-legitimationer. I paragrafen definieras på ett uttömmande sätt vilka uppgifter som ingår i e-legitimationen. Datainnehållet motsvarar till stor del de uppgifter som finns i ett fysiskt pass eller identitetskort, och därför kan e-legitimationen jämföras med de traditionella handlingarna. I paragrafen hänvisas det också till de uppgifter som det föreskrivs om i bilaga V till eIDAS-förordningen. Bilagan fastställer vilka uppgifter som ska ingå i ett kvalificerat elektroniskt attributsintyg och därmed även vilka uppgifter som ingår i e-legitimationen. Till skillnad från pass och identitetskort innehåller en e-legitimation inga fingeravtrycks- och signaturuppgifter.

I 1 mom. föreskrivs det att uppgifterna i en e-legitimation ska motsvara uppgifterna i polisens passregister eller identitetskortsregister. I momentet fastställs vilka uppgifter en e-legitimation ska innehålla. Bestämmelsen säkerställer samtidigt att identitetsbeviset baserar sig på en informationskälla som upprätthålls och uppdateras av en myndighet. Uppgifternas överensstämmelse är av avgörande betydelse för e-legitimationens tillförlitlighet.

Paragrafens 2 mom. innehåller en förteckning över de uppgifter som ingår i en e-legitimation. En e-legitimation ska innehålla sådana personuppgifter som normalt behövs för att styrka identiteten i olika situationer i vardagen. I en e-legitimation ska ingå följande uppgifter: efternamn, förnamn, kön som antecknats i ett giltigt finskt pass eller identitetskort, födelsetid, personbeteckning, uppgift om finskt medborgarskap, den myndighet som utfärdat passet eller identitetskortet, dagen för utfärdande av passet eller identitetskortet, sista giltighetsdag och nummer samt ansiktsbild som har förts in i pass- eller identitetskortsregistret. I 3 mom. föreskrivs det att ett kvalificerat elektroniskt attributsintyg också kan innehålla åldersbevis. Momentet möjliggör ett begränsat bevis som härrör från de uppgifter som ingår i e-legitimationen och som visar att användaren tillhör en viss åldersgrupp utan att annan information röjs. Detta är ändamålsenligt t.ex. i tjänster där det är nödvändigt att ange åldersgränser, men ingen annan individualiserande personuppgift behövs.

I 4 mom. finns en informativ hänvisning till bilaga V till eIDAS-förordningen, där det föreskrivs om krav som ställs på alla kvalificerade elektroniska attributsintyg. I bilagan krävs det att en jämförelsevis stor mängd information ska ingå i ett kvalificerat elektroniskt attributsintyg. Bestämmelserna i bilagan påverkar i hög grad datainnehållet i det kvalificerade attributsintyget, som innehåller delvis samma uppgifter som e-legitimationen. Det finns dock ingen anledning att föreskriva om detta på nationell nivå, eftersom bestämmelserna redan ingår i en förordning som är direkt förpliktande för medlemsstaterna.

5 §. Förutsättningar för att få tillgång till e-legitimation. I paragrafen föreskrivs det om förutsättningarna för att få tillgång till e-legitimation. Enligt 1 mom. kan en finsk medborgare samt en utlänning som vistas i Finland få tillgång till e-legitimation. Personen ska dessutom ha en giltig handling som utgör grund för e-legitimationen samt en europeisk digital identitetsplånbok som har tagits i bruk. Förutsättningarna bygger på principen att endast personer vars identitet redan har styrkts av en myndighet kan få tillgång till e-legitimation. För att få tillgång till e-legitimation krävs det självklart också att personen har en europeisk digital identitetsplånbok som har tagits i bruk och för vilken e-legitimationen uteslutande tillhandahålls.

I 2 mom. föreskrivs det om en teknisk kontroll, som också är en förutsättning för att en person ska få tillgång till e-legitimation. Kontrollen går till så att Myndigheten för digitalisering och befolkningsdata fjärrläser uppgifterna i den tekniska delen av den handling som utgör grund för den digitala identiteten och kontrollerar att uppgifterna motsvarar identifieringsuppgifterna för den fysiska personen i personens europeiska digitala identitetsplånbok. Kontrollen av uppgifterna utgör en tvåstegsåtgärd som hör till de uppgifter som en kvalificerad tillhandahållare av betrodda tjänster ska sköta. Å ena sidan kan de personuppgifter som erhålls ur den tekniska delen av handlingen jämföras med identifieringsuppgifterna för den fysiska personen i användarens europeiska digitala identitetsplånbok. Å andra sidan säkerställs äktheten och integriteten hos det lästa passet eller identitetskortet med hjälp av de certifikat som ingår i den tekniska delen av handlingen. Syftet med kontrollen är att förhindra missbruk på förhand och att se till att sökanden faktiskt innehar en föreskriven handling som utgör grund för e-legitimationen. De uppgifter som används i jämförelsen får inte sparas, utan jämförelsen ska göras ur minnet.

Enligt den i 2 § 9 punkten angivna definitionen av handling som utgör grund för en e-legitimation kan en person samtidigt ha fler än en handling som kan godkännas som grund. Grund för e-legitimationen blir den handling vars uppgifter blir fjärravlästa. På så sätt gör personen själv valet i sitt eget ärende, och myndigheten ges inget utrymme för egen bedömning i ärendet.

Den förutsättning som gäller fjärravläsning uppfylls också om användaren i samband med att den europeiska digitala identitetsplånboken tas i bruk gör en lyckad fjärravläsning av passet eller identitetskortet på samma gång.

Med teknisk del avses i fråga om pass den tekniska del som avses i 5 a § i passlagen och i fråga om identitetskort den tekniska del som avses i 5 § i lagen om identitetskort.

Identifiering med den europeiska digitala identitetsplånboken motsvarar i bestämmelsen kravet på stark autentisering, om vilket det är möjligt att jämförbara uppgifter.

6 §. Giltigheten för e-legitimationer. I 1 mom. föreskrivs det att en e-legitimation kan vara i kraft lika länge som det pass eller identitetskort som utgör grund för den digitala identiteten är i kraft. Huvudprincipen föreslås således vara att den digitala versionen av ett pass eller identitetskort inte ska vara i kraft längre än den handling som utgör grund för den.

I 2 mom. föreskrivs det att om den handling som utgör grund för e-legitimationen dras in på den grunden att innehavaren har anmält att den har förkommit eller stulits, fortsätter rätten till e-legitimationen trots detta 30 dygn. Momentet gör det möjligt att fortsätta använda e-legitimationen under en kort övergångsperiod, vilket är praktiskt i situationer där anskaffningen av en ny handling fortfarande pågår. Förlängningen stöder kontinuiteten i tjänsterna och minskar de olägenheter som följer av att användningen avbryts. Enligt 12 § upphör dock en e-legitimation att gälla trots det föreslagna momentet, om det till personen inom den 30 dygn långa förlängningen lämnas ut en ny handling som utgör grund för e-legitimationen. I så fall ska personen med hjälp av den nya utlämnade handlingen ansöka om en ny e-legitimation. Trots att rätten till e-legitimationen förlängs med 30 dygn är det med stöd av bestämmelsen inte möjligt att få tillgång till en ny e-legitimation på grundval av en handling som innehavaren har anmält som förkommen eller stulen, eftersom anmälan leder till att den fysiska handling som utgör grund för e-legitimationen dras in. Syftet med bestämmelsen är att göra det möjligt att använda en tidigare erhållen e-legitimation i 30 dygn från det att den handling som utgör grund för e-legitimationen har dragits in på grund av en anmälan om förkommen eller stulen handling.

I 3 mom. föreskrivs det att en e-legitimation kan användas som ett kvalificerat elektroniskt attributsintyg samtidigt på två separata tekniska utrustningar. E-legitimationer som används på olika tekniska utrustningar ska tydligt skiljas från varandra med hjälp av identifieringsuppgifter, vilket också krävs med tanke på att användaruppgifterna ska vara spårbara enligt artikel 5a.4 i eIDAS-förordningen. Momentet gör det möjligt att använda e-legitimationen t.ex. via användarens telefon och pekplatta, vilket ökar dess flexibilitet och användbarhet. Samtidig användning förutsätter dock att informationssäkerheten och e-legitimationen integritet bevaras på båda plattformarna.

I 4 mom. ges Myndigheten för digitalisering och befolkningsdata behörighet att bedöma giltighetstiden för ett kvalificerat elektroniskt attributsintyg. Giltighetstiden för ett kvalificerat elektroniskt attributsintyg kan vara kortare än giltighetstiden för den underliggande handlingen, vilket gör det möjligt att uppdatera uppgifterna och förnya det kvalificerade elektroniska attributsintyget så ofta som det är tekniskt sett behövs. Den maximala giltighetstiden och sista giltighetsdagen för ett kvalificerat elektroniskt attributsintyg bestäms enligt den sista giltighetsdagen för den handling som ligger till grund för attributsintyget.

7 §. Behöriga myndigheter, myndighetsuppgifter och uppgiftsbehandling. I 1 mom. föreskrivs det att när polisen eller någon annan behörig myndighet utfärdar en handling som utgör grund för en e-legitimation beviljar den samtidigt rätt att få tillgång till en e-legitimation. Syftet med förslaget är att förenkla processen för utfärdande och samtidigt se till att e-legitimationen bygger

på aktuella uppgifter som bestyrkts av myndigheten. Förfarandet bidrar också till en smidig ärendehantering och kan genomföras utan att det behöver föreskrivas om ett nytt ansöknings- och tillståndsförfarande.

Den föreslagna bestämmelsen leder till att de myndigheter som har till uppgift att utfärda den handling som utgör grund för e-legitimationen är behöriga. Förutom polisen är dessa myndigheter enligt 10 § 2 mom. i passlagen och 9 § 2 mom. i lagen om identitetskort en finsk ambassad, ett konsulat som leds av en utsänd tjänsteman, någon annan finsk beskickning med en anställd finsk medborgare som utrikesministeriet har bemyndigat att utfärda pass, någon annan finsk beskickning som utfärdar pass med en anställd finsk medborgare som utrikesministeriet har bemyndigat att utfärda identitetskort samt utrikesministeriet.

I 2 *mom.* föreskrivs det att polisen lämnar ut de uppgifter som ska ingå i en e-legitimation till Myndigheten för digitalisering och befolkningsdata för tillhandahållande av ett kvalificerat elektroniskt attributsintyg. Momentet fastställer ansvarsfördelningen mellan myndigheterna och säkerställer en ändamålsenlig överföring av uppgifter. Innan uppgifterna lämnas ut ska polisen noggrant kontrollera att de är korrekta.

Enligt 3 *mom.* ska Myndigheten för digitalisering och befolkningsdata tillhandahålla de certifikat som behövs för att säkerställa äktheten och integriteten hos uppgifterna i ett kvalificerat elektroniskt attributsintyg och stämpla uppgifterna med en kvalificerad elektronisk stämpel. Med kvalificerad elektronisk stämpel avses enligt artikel 3.27 i eIDAS-förordningen en avancerad elektronisk stämpel som skapas med hjälp av en kvalificerad anordning för skapande av elektroniska stämplat och som är baserad på ett kvalificerat certifikat för elektroniska stämplat. Denna bestämmelse säkerställer uppgifternas tillförlitlighet och oföränderlighet.

Ett kvalificerat elektroniskt attributsintyg ska vara förenligt med artikel 45d i eIDAS-förordningen, vilket säkerställer att det kvalificerade elektroniska attributsintyg som används som e-legitimation och Myndigheten för digitalisering och befolkningsdata, som tillhandahåller det till användaren, uppfyller de krav som följer av EU-lagstiftningen. Momentet innebär att Myndigheten för digitalisering och befolkningsdata i egenskap av tillhandahållare av ett kvalificerat elektroniskt attributsintyg på de sätt som avses i artiklarna 20 och 21 i eIDAS-förordningen ska ansöka om kvalificering av sin betrodda tjänst hos tillsynsorganet och se till att kraven på betrodda tjänster uppfylls under tjänstens livscykel, så att statusen som kvalificerad hålls i kraft för myndigheten och för det elektroniska attributsintyg som den tillhandahåller.

Myndigheten för digitalisering och befolkningsdata kan därför tillhandahålla ett kvalificerat elektroniskt attributsintyg endast om den uppfyller de skyldigheter som följer av eIDAS-förordningen, inklusive den nationella tillsynsmyndighetens övervakning av Transport- och kommunikationsverket. För att kunna tillhandahålla kvalificerade elektroniska attributsintyg måste Myndigheten för digitalisering och befolkningsdata med andra ord förvärva statusen som kvalificerad tillhandahållare av betrodda tjänster, vilket förutsätter att kraven enligt eIDAS-förordningen uppfylls, att överensstämmelsen bedöms samt att Transport- och kommunikationsverket gör en anteckning om Myndigheten för digitalisering och befolkningsdata i förteckningen över kvalificerade tillhandahållare av betrodda tjänster i Finland.

I 4 *mom.* föreskrivs det att Myndigheten för digitalisering och befolkningsdata ska behandla uppgifter som polisen lämnar ut i Finland. E-legitimationens tillförlitlighet grundar sig till stor del på säkerhetsfaktorerna i de handlingar som utgör grund för e-legitimationen. Bestämmelser

om dessa säkerhetsfaktorer finns i passlagen och lagen om identitetskort. Enligt 35 § 3 mom. i passlagen och 22 § 4 mom. i lagen om identitetskort ska individualiseringen av handlingarna och kontrollen av handlingarnas kvalitet utföras i Finland. Grundlagsutskottet har ansett (GrUU 6/2013 rd) att detta krav är motiverat med tanke på uppgifternas art och de skyldigheter som följer av tjänsteansvar. Det internationella säkerhetsläget har under de senaste åren förändrats i en väsentligt mer instabil riktning, och även detta talar för att nationella åtgärder behöver vidtas för att göra det möjligt att skydda nationellt viktiga uppgifter så att uppgifterna är säkra och tillgängliga även under undantagsförhållanden, där förbindelserna till andra länder är svaga eller obefintliga. I en allvarlig kris är det särskilt viktigt att personer kan identifieras tillförlitligt, enkelt och snabbt, och i krissituationer sörjer varje land i första hand för sina egna behov. Omkring 4,5 miljoner finländare, av vilka cirka 700 000 är minderåriga, har för närvarande ett pass eller identitetskort som är i kraft. Genomförandet av e-legitimationer baserar sig på de uppgifter som införts i pass- och identitetskortsregistren. Uppgifterna i fråga täcker alltså majoriteten av Finlands befolkning, vars personuppgifter den föreslagna lagstiftningen avser skydda.

8 §. Register över e-legitimationer. I 1 mom. föreskrivs det om polisens skyldighet att föra ett register över e-legitimationer. Syftet med registret är att göra det möjligt att sköta de uppgifter som föreskrivs i lagen. Registret föreslås innehålla de uppgifter som avses i 4 § 2 mom. i fråga om de personer som har tagit i bruk en e-legitimation. Dessutom innehåller registret uppgifter om e-legitimationerna och behandlingen av dem. Dessa uppgifter omfattar uppgifter om beviljande, indragning och giltighetens upphörande.

I enlighet med bestämmelserna i passlagen och lagen om identitetskort kan en finsk medborgare som vistas utomlands under vissa förutsättningar ansöka om pass och identitetskort hos Finlands ambassad, hos konsulat som leds av en utsänd tjänsteman och hos andra finska beskickningar. En e-legitimation enligt den föreslagna lagstiftningen kan också grunda sig på en handling som utfärdats t.ex. av Finlands ambassad. Bestämmelser om förande av register finns i 29 § i passlagen och 31 § i lagen om identitetskort. Enligt de ovannämnda paragraferna för polisen ett register över de uppgifter som enligt lagarna ska skötas av polisen och utrikesförvaltningen. I denna paragraf föreslås det i enlighet med gällande lagstiftning att enbart polisen ska föra ett register över e-legitimationer.

I 2 mom. hänvisas det i fråga om behandlingen av personuppgifter i registret till lagen om behandling av personuppgifter i polisens verksamhet (616/2019) och till dess 11–15 §, som gäller användning av personuppgifter. Bestämmelser om utlämnande och radering av personuppgifter finns i 4 kap. 38 § i den lagen. Hänvisningarna syftar till att säkerställa att behandlingen av uppgifter i registret sker i enlighet med gällande dataskyddsbestämmelser om polisens verksamhet och att användningen av registret begränsas till lagenliga ändamål. När det föreskrivs om ett nytt tillförlitligt sätt att styrka identiteten är det ändamålsenligast att samma bestämmelser tillämpas på behandlingen av uppgifterna i det relaterade registret som på behandlingen av uppgifterna i passregistret och identitetskortsregistret.

På behandlingen av personuppgifter i registret över e-legitimationer tillämpas den allmänna dataskyddsförordningen. Behandlingen av personuppgifter är nödvändig för att polisen ska kunna fullgöra sina lagstadgade skyldigheter, och den grundar sig på artikel 6.1 c i förordningen. Den personuppgiftsansvariges ställning bestäms i enlighet med artikel 4.7 i den allmänna dataskyddsförordningen, och i den föreslagna regleringen förtydligas att polisen är personuppgiftsansvarig för registret över e-legitimationer, så att rollen som personuppgiftsansvarig och de myndighetsuppgifter som anknyter till detta blir så tydliga som möjligt. I regleringen utnyttjas det nationella handlingsutrymme som artikel 6.3 och 6.4 i den allmänna dataskyddsförordningen ger. Handlingsutrymmet utnyttjas så att de uppgifter som ska

behandlas på nationell nivå avgränsas noggrant genom att de definieras som uppgifter som avses i 4 § 2 mom. i den föreslagna lagen och genom att uppgifterna begränsas till att gälla endast de personer som har tagit i bruk en e-legitimation. Enligt det föreslagna 8 § 1 mom. innehåller registret också uppgifter om behandlingen av e-legitimationer vid polisen, vilket bekräftar att uppgifterna behandlas lagligt och korrekt. Bestämmelserna om förande av registret uppfyller ett mål av allmänt intresse, eftersom det är nödvändigt för att säkerställa en tillförlitlig verifiering av identitet och personuppgifter och tryggheten av säkerheten. Bestämmelserna är proportionerliga, eftersom endast de personuppgifter som anges i lagen och uppgifter om behandlingen av e-legitimationen förs in i registret, och uppgifterna får användas för andra behandlingsändamål endast i enlighet med lagen om behandling av personuppgifter i polisens verksamhet. Som personuppgiftsansvarig ansvarar polisen för all behandling av personuppgifter i enlighet med principerna i artikel 5 i den allmänna dataskyddsförordningen, dvs. principerna om ändamålsbegränsning, uppgiftsminimering och lagringsminimering. Den registrerades rättigheter bestäms enligt kapitel III i den allmänna dataskyddsförordningen och lagen om behandling av personuppgifter i polisens verksamhet. Lagringen av personuppgifter omfattas av principen om lagringsminimering, som det föreskrivs om i artikel 5.1 e i den allmänna dataskyddsförordningen. Enligt denna princip får personuppgifter förvaras i en form som möjliggör identifiering av den registrerade enbart så länge som det är nödvändigt för användningsändamålet för uppgifterna. Den personuppgiftsansvarige ansvarar för att fastställa förvaringstiderna och säkerställa att de är proportionella i förhållande till syftet med behandlingen.

För polisens del fastställs förvaringstiderna enligt 38 § i lagen om behandling av personuppgifter i polisens verksamhet. På grundval av dessa bestämmelser grundar sig bedömningen av förvaringstiderna i polisens register på de uppgifter som föreskrivs i lagen och på huruvida personuppgifterna behövs för att dessa ska kunna utföras. Enligt huvudregeln ska personuppgifter som behandlas för utförande av tillståndsförvaltnings- och tillsynsuppgifter raderas senast tjugo år efter beslutet eller dess upphörande, efter utgången av den giltighetstid som nämns i beslutet eller efter anteckningen av personuppgifterna.

9 §. Register över kvalificerade elektroniska attributsintyg. I paragrafen föreskrivs det om skyldigheten för Myndigheten för digitalisering och befolkningsdata att föra register över kvalificerade elektroniska attributsintyg och de europeiska digitala identitetsplånböcker för vilka ett kvalificerat elektroniskt attributsintyg har tagits i bruk. Syftet med registret är att göra det möjligt att utföra de uppgifter som det föreskrivs om i den föreslagna lagen, t.ex. förvaltning av kvalificerade elektroniska attributsintyg och övervakning av deras giltighet. Registret innehåller inte personuppgifter som lämnats ut ur polisens informationssystem, utan främst mer tekniska identifierare, såsom en identifierare för kvalificerat elektroniskt attributsintyg och en tillhörande identifierare för plånboken samt uppgifter om utfärdaren och innehavaren av attributsintyget.

I artikel 5a.4 i eIDAS-förordningen föreskrivs det bl.a. om spårbarheten av användningen av användaruppgifterna för användaren själv och användarens tillgång till en logg över alla transaktioner som utförts via plånboken, vilket innebär direkta skyldigheter för tillhandahållaren av plånboken. På grund av förordningens tvingande karaktär föreslås inga bestämmelser om dessa.

På behandlingen av kvalificerade elektroniska attributsintyg och personuppgifterna i de register som gäller dessa tillämpas EU:s allmänna dataskyddsförordning, och i regleringen utnyttjas det nationella handlingsutrymme som artikel 6.3 och 6.4 i den allmänna dataskyddsförordningen ger. Den föreslagna bestämmelsen binder uppgiftsbehandlingen till en myndighet för skötseln av de uppgifter som föreslås i lagförslaget och avgränsar den till de uppgifter som har samband

med i lagförslaget avsedda kvalificerade elektroniska attributsintyg och till de europeiska digitala identitetsplånböcker för vilka ett kvalificerat elektroniskt attributsintyg har tagits i bruk. Behandlingen av personuppgifter är nödvändig för att Myndigheten för digitalisering och befolkningsdata ska kunna fullgöra sina lagstadgade skyldigheter, och den grundar sig på artikel 6.1 c i förordningen. Den personuppgiftsansvariges ställning fastställs enligt artikel 4.7 i den allmänna dataskyddsförordningen. Enligt den föreslagna paragrafen är Myndigheten för digitalisering och befolkningsdata personuppgiftsansvarig för registret över kvalificerade elektroniska attributsintyg. Det är nödvändigt att föreskriva om detta för att det inte ska uppstå oklarheter om den personuppgiftsansvarige och dess skyldigheter.

Bestämmelserna om förande av registret uppfyller ett mål av allmänt intresse, eftersom de är nödvändiga för att säkerställa tillförlitligheten hos användarens bestyrkta uppgifter och informationssäkerheten. Bestämmelserna är också proportionerliga eftersom inga personuppgifter som lämnats ut från polisens informationssystem förs in i registret, utan endast tekniska identifierare och uppgifter om utfärdaren och innehavaren av attributsintyget. Som personuppgiftsansvarig ansvarar Myndigheten för digitalisering och befolkningsdata för all behandling av personuppgifter i enlighet med de principer som det föreskrivs om i artikel 5 i den allmänna dataskyddsförordningen, dvs. ändamålsbegränsning, uppgiftsminimering och lagringsminimering. Den registrerades rättigheter bestäms i enlighet med kapitel III i den allmänna dataskyddsförordningen, vilket innebär att t.ex. rätten att radera uppgifter enligt artikel 17 inte gäller eftersom uppgiftsbehandlingen grundar sig på en lagstadgad skyldighet. Inga särskilda bestämmelser om förvaringstider föreslås i fråga om Myndigheten för digitalisering och befolkningsdata. Fastställandet av förvaringstiden grundar sig således på de allmänna principerna i den allmänna dataskyddsförordningen. Den personuppgiftsansvarige ska följaktligen bedöma förvaringstiden i förhållande till registrets användningsändamål och se till att uppgifterna inte förvaras längre än nödvändigt. Hanteringen av förvaringstider utgör en väsentlig del av den personuppgiftsansvariges skyldighet att vidta tekniska och organisatoriska åtgärder enligt den allmänna dataskyddsförordningen.

10 §. Polisens behörighet att dra in rätten till e-legitimation. I paragrafen föreskrivs det om polisens behörighet att dra in rätten till e-legitimation i vissa situationer. I 1 mom. anges grunderna för indragning, enligt vilka polisen ska dra in rätten till en e-legitimation, om e-legitimationen används av någon annan än användaren eller om säkerheten vid användningen av den annars har allvarligt äventyrats. Exempel på allvarligt äventyrande av säkerheten vid användning är identitetsstöld, teknisk sårbarhet eller andra missbruk. Bestämmelsen är av avgörande betydelse när det gäller att säkerställa att en e-legitimation är tillförlitlig. Indragningen av rätten gäller den handling som utgör grund för e-legitimationen och som använts för att möjliggöra en sådan fjärravläsning som avses i det föreslagna 5 § 2 mom. Paragrafen innehåller inga bestämmelser om datatekniska lösningar för polisen t.ex. när det gäller registeranteckningar. Den indragning som avses i paragrafen kan i praktiken antecknas i polisens informationssystem så att passet eller identitetskortet i fråga inte längre får användas som handling som utgör grund för en e-legitimation.

Polisen ska enligt 2 mom. utan dröjsmål underrätta Myndigheten för digitalisering och befolkningsdata om en indragning.

Polisen ska också meddela ett förvaltningsbeslut om indragning av rätt till e-legitimation i enlighet med procedurbestämmelserna i förvaltningslagen. Detta är av central betydelse med tanke på användarens rättsskydd, eftersom det i det föreslagna 11 § 3 mom. föreskrivs att Myndigheten för digitalisering och befolkningsdata ska dra in ett kvalificerat elektroniskt attributsintyg om polisen med stöd av 10 § 1 mom. har dragit in rätten till e-legitimationen. Eftersom Myndigheten för digitalisering och befolkningsdatas behörighet att dra in ett

attributsintyg direkt beror på en indragningsåtgärd som polisen vidtagit med stöd av denna bestämmelse, föreslås det att det i 13 § 3 mom. föreskrivs om ett undantag från procedurbestämmelserna i förvaltningslagen, enligt vilket Myndigheten för digitalisering och befolkningsdata inte ska ge något förvaltningsbeslut om en sådan indragningsåtgärd.

Enligt 3 mom. kan den indragna rätten till en e-legitimation inte återinföras. Detta understryker att beslutet om indragning är slutgiltigt och hindrar att en riskfylld e-legitimation tas i bruk på nytt. Efter indragningen uppstår rätten till e-legitimation när personen får en ny motsvarande handling som utgör grund för en e-legitimation. Indragningen gäller en specifik handling, och när en rätt dras in på grundval av ett giltigt pass påverkar det således inte den rätt som samma person har på grundval av ett identitetskort eller tvärtom.

11 §. Indragning av kvalificerade elektroniska attributsintyg. I paragrafen föreskrivs det om Myndigheten för digitalisering och befolkningsdatas behörighet att dra in ett kvalificerat elektroniskt attributsintyg i olika situationer.

Bestämmelser om indragning av kvalificerade elektroniska attributsintyg finns i artikel 4 i Europeiska kommissionens genomförandeförordning (EU) 2025/1569, vars bestämmelser utgör direkt tillämplig rätt. Artikel 3 c i genomförandeförordningen medger emellertid nationellt handlingsutrymme i frågan. Syftet med den föreslagna paragrafen är att komplettera bestämmelserna i genomförandeförordningen på nationell nivå. Enligt artikel 4.3 a i genomförandeförordningen ska ett kvalificerat elektroniskt attributsintyg, när det utfärdats med en giltighetstid på mer än 24 timmar, återkallas på uttrycklig begäran av den person som det elektroniska attributsintyget har utfärdats för. Enligt artikel 4.3 b ska attributsintyg återkallas om leverantören vet att säkerheten eller tillförlitligheten hos de kvalificerade elektroniska attributsintygen har äventyrats. Enligt artikel 4.3 c kan attributsintyg även återkallas i andra situationer i enlighet med kraven i unionsrätten eller nationell rätt, eller enligt vad som fastställs av leverantörerna i deras policyer enligt punkt 1 i artikeln.

I det föreslagna 1 mom. föreskrivs det att Myndigheten för digitalisering och befolkningsdata ska dra in ett kvalificerat elektroniskt attributsintyg om det används av någon annan än användaren.

I 2 mom. föreskrivs det att Myndigheten för digitalisering och befolkningsdata ska dra in ett kvalificerat elektroniskt attributsintyg om polisen har dragit in rätten till e-legitimationen. Genom denna bestämmelse säkerställs att bestyrkta uppgifter inte utnyttjas obehörigt.

I 3 mom. föreskrivs det att Myndigheten för digitalisering och befolkningsdata ska dra in ett kvalificerat elektroniskt attributsintyg om intyget innehåller ett uppenbart fel. Denna bestämmelse gör det möjligt att korrigera tekniska fel eller andra fel som beror på myndighetens verksamhet utan att användaren särskilt begär det. Myndigheten för digitalisering och befolkningsdata ska utan dröjsmål tillhandahålla användaren ett nytt kvalificerat elektroniskt attributsintyg efter det att det har dragits in med stöd av det föreslagna momentet.

Enligt 4 mom. kan ett indraget kvalificerat elektroniskt attributsintyg inte återinföras. Denna bestämmelse hindrar att ett attributsintyg som har bedömts vara riskabelt tas i bruk på nytt, men inte att ett nytt attributsintyg kan tillhandahållas medan den handling som utgör grund för intyget är i kraft och de övriga villkoren uppfylls.

12 §. Giltighetens upphörande. I 1 mom. föreskrivs det om situationer där en e-legitimation och de kvalificerade elektroniska attributsintyg som hänför sig till den upphör att gälla utan särskilt

beslut. Giltighetens upphörande är en teknisk följd som inte kräver någon aktiv åtgärd från myndigheternas sida, utan det sker direkt med stöd av lagen.

Giltigheten kan upphöra på följande grunder:

1. En ny handling som utgör grund för e-legitimation lämnas ut till personen, när det är fråga om en handling som fastställer e-legitimationens giltighet. Detta är fallet om personen beviljas en ny handling som har använts för fjärravläsning av uppgifter enligt 5 § 2 mom. Den föreslagna bestämmelsen följer de gällande bestämmelserna i passlagen och lagen om identitetskort, enligt vilka det tidigare passet och identitetskortet upphör att gälla när en ny handling lämnas ut till sökanden. När personen beviljas en ny handling som utgör grund för e-legitimation upphör det kvalificerade elektroniska attributsintyg som tillhandahållits på grundval av den tidigare handlingen automatiskt att gälla. Detta hindrar att flera intyg som baserar sig på olika identitetshandlingar används samtidigt och säkerställer att uppgifterna är aktuella.
2. Den handling som utgör grund för e-legitimationen dras in. Om det pass eller identitetskort som utgör grund för e-legitimationen dras in av någon annan orsak än den som avses i 6 § 2 mom., upphör också e-legitimationen att gälla. Denna bestämmelse är nödvändig för att säkerställa ett direkt samband mellan den fysiska handlingen och dess digitala version.
3. Uppgifterna motsvarar inte varandra. Om personuppgifterna i e-legitimationen och i den europeiska digitala identitetsplånboken inte motsvarar varandra, upphör e-legitimationen att gälla. Denna bestämmelse hindrar att felaktiga eller föråldrade uppgifter används.
4. Plånboken tas ur bruk. Om användaren återkallar giltigheten för den europeiska digitala identitetsplånboken upphör den e-legitimation som är kopplad till plånboken att gälla. Denna bestämmelse stöder användarens rätt att ha kontroll över sin egen identitet och förhindrar att passiva e-legitimationer hålls i kraft.

Enligt 2 mom. ska Myndigheten för digitalisering och befolkningsdata utan dröjsmål informera användaren om att giltigheten för ett kvalificerat elektroniskt attributsintyg upphör. Informationen behöver dock inte lämnas om användaren själv tar den europeiska digitala identitetsplånboken ur bruk.

Om giltigheten upphör hindrar detta inte att ett nytt kvalificerat elektroniskt attributsintyg utfärdas, förutsatt att det inte finns någon sådan grund för giltighetens upphörande som anges i paragrafen.

13 §. *Avvikelse från förvaltningslagens förfarandebestämmelser.* I paragrafen föreskrivs det om undantag från förvaltningslagens förfarandebestämmelser när det gäller e-legitimationer och kvalificerade elektroniska attributsintyg som hänför sig till dessa. Undantagen gäller situationer där det inte ges något förvaltningsbeslut eller någon besväransvisning eller upplysning om besvärsförbud.

Enligt paragrafen ges det inte något förvaltningsbeslut eller någon besväransvisning eller upplysning om besvärsförbud vid beviljande av rätten att få tillgång till en e-legitimation och vid indragning av ett kvalificerat elektroniskt attributsintyg.

14 §. Besvärshälsbud och sökande av ändring. I paragrafen föreskrivs det om begränsningar av rätten att söka ändring när det gäller e-legitimationer och kvalificerade elektroniska attributsintyg som hänför sig till dessa. Begränsningen av besvärshälsrätten gäller situationer där åtgärderna är tekniska, automatiska eller direkt grundade på lag och inte förknippade med ett egentligt förvaltningsbeslut.

Enligt 1 mom. får ändring inte sökas genom besvär i situationer som avses i 12 §, när det är fråga om att en e-legitimation och de kvalificerade elektroniska attributsintyg som hänför sig till den upphör att gälla. Giltigheten upphör automatiskt och myndigheten har i detta fall ingen prövningsrätt, vilket innebär att det inte finns någon besvärshälsrätt.

I 2 mom. föreskrivs det att i avgöranden som gäller beviljande eller indragning i enlighet med 13 § och som ges utan förvaltningsbeslut eller besvärshälsanvisning får ändring inte sökas genom besvär. I dessa fall kan det t.ex. handla om att rätt att få tillgång till e-legitimation beviljas eller ett attributsintyg dras in utan att något förvaltningsbeslut ges.

Enligt 3 mom. finns det bestämmelser om sökande av ändring i förvaltningsdomstol i lagen om rättegång i förvaltningsärenden. Det föreslagna momentet är informativt och visar samtidigt att det är möjligt att söka ändring i ett förvaltningsärende, där ett förvaltningsbeslut ges.

15 §. Ikraftträdande. Paragrafen innehåller en ikraftträdandebestämmelse och en övergångsbestämmelse. En närmare motivering till lagens ikraftträdande och övergångsbestämmelsen finns i avsnitt 9 (Ikraftträdande).

7.4 Lagen om tillhandahållande av digitala tjänster

3 §. Lagens tillämpningsområde. Det föreslås att 1 mom. 4 punkten ändras på grund av ändringen av rubriken på autentiseringslagen.

6 §. Elektronisk identifiering av tjänsteanvändarna. Paragrafens 2 mom. ändras så att den gällande lagstiftningen kompletteras med en skyldighet för den offentliga sektorn att godkänna också en europeisk digital identitetsplånbok som metod för stark autentisering. Dessutom ändras autentiseringslagens rubrik som nämns i bestämmelsen, och hänvisningen ändras lagtekniskt eftersom paragrafen efter de föreslagna ändringarna endast har ett moment.

Regleringen behövs för att på nationell nivå genomföra de skyldigheter som anges i artikel 5f.1 i den reviderade eIDAS-förordningen. I denna artikel konstateras det att i de fall då medlemsstater kräver elektronisk identifiering och autentisering för att få åtkomst till en nättjänst som tillhandahålls av ett offentligt organ, ska de även godta europeiska digitala identitetsplånböcker som tillhandahålls i enlighet med den förordningen. Den offentliga sektorn ska således också godta plånboken som identifieringsmetod i en situation som kräver stark autentisering.

7.5 Lagen om förvaltningens gemensamma stödtjänster för e-tjänster

3 §. Stödtjänster. I 1 mom. 4 och 5 punkten föreslås en teknisk ändring som beror på att autentiseringslagens rubrik ändras. I 4 punkten korrigeras dessutom autentiseringslagens författningssamlingsnummer.

Det föreslås att 2 mom. ändras så att en fysisk person som använder elektroniska tjänster inom den offentliga förvaltningen i fortsättningen kan identifieras i tjänsten för identifiering av fysiska personer även med hjälp av den europeiska digitala identitetsplånboken. Artikel 5f.1 i

den reviderade eIDAS-förordningen gäller gränsöverskridande användning av europeiska digitala identitetsplånböcker, och där konstateras det att i de fall då medlemsstater kräver elektronisk identifiering och autentisering för att få åtkomst till en nättjänst som tillhandahålls av ett offentligt organ, ska de även godta europeiska digitala identitetsplånböcker som tillhandahålls i enlighet med eIDAS-förordningen. Det är därför ändamålsenligt att tillhandahålla också denna identifieringsmetod så att den kan förmedlas centraliserat till myndigheterna via tjänsten för identifiering av fysiska personer. Den offentliga sektorns e-tjänster kan således fullgöra den skyldighet som anges i eIDAS-förordningen genom att använda tjänsten för identifiering av fysiska personer, som flera e-tjänster inom den offentliga sektorn är skyldiga att använda.

7.6 Lagen om verkställighet av böter

1 §. Tillämpningsområde. Till 1 mom. fogas en ny 64 punkt så att administrativa påföljdsavgifter enligt den föreslagna eIDAS-lagen inkluderas i lagens tillämpningsområde. Det är fråga om påföljdsavgifter enligt 42–46 § i eIDAS-lagen för tillhandahållare av betrodda tjänster, kvalificerade tillhandahållare av betrodda tjänster, icke-kvalificerade tillhandahållare av betrodda tjänster, kvalificerade tillhandahållare av betrodda tjänster som tillhandahåller kvalificerade certifikat och kvalificerade tillhandahållare av betrodda tjänster som tillhandahåller kvalificerade elektroniska attributsintyg.

7.7 Lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata

2 §. Tillämpningsområde. Hänvisningen i 2 mom. 2 punkten till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras.

28 §. Allmänna förutsättningar för utlämnande av uppgifter. Till 1 mom. fogas författningsnumret på dataskyddslagen.

43 §. Utlämnande av identifieringsuppgifter. I 2 mom. 1 punkten föreslås ett tillägg enligt vilket elektroniska kommunikationskoder också kan överlåtas, om koden används som en uppgift som identifierar innehavaren av identifieringsuppgifter för en fysisk person i samband med produktion av tjänster eller prestationer som baserar sig på användningen av identifieringsuppgifter för fysiska personer som Myndigheten för digitalisering och befolkningsdata utfärdar med stöd av eIDAS-lagen. Med identifieringsuppgifter för fysiska personer avses enligt artikel 3.3 i eIDAS-förordningen en uppsättning uppgifter som utfärdas i enlighet med unionsrätten eller nationell rätt, som gör det möjligt att fastställa identiteten på en fysisk person. Enligt 3 § i eIDAS-lagen utfärdar Myndigheten för digitalisering och befolkningsdata identifieringsuppgifter för fysiska personer för den europeiska digitala identitetsplånbok som myndigheten tillhandahåller. Bestämmelser om obligatoriska och frivilliga personidentifieringsuppgifter för fysiska personer finns i bilagan till kommissionens genomförandeförordning (EU) 2024/2977, som utfärdats med stöd av artikel 5a i eIDAS-förordningen. Med stöd av bestämmelserna i den genomförandeförordningen kan en elektronisk kommunikationskod användas som identifieringsuppgift för personidentifieringsuppgifter för fysiska personer.

Hänvisningen i 2 mom. 2 punkten till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att

det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras. I momentet görs också en lagteknisk korrigering.

62 §. *Uppgifter som ska ingå i certifikat för certifierad elektronisk kommunikation.* Hänvisningarna i paragrafen till lagen om stark autentisering och betrodda elektroniska tjänster ändras till hänvisningar till lagen om stark autentisering. Ändringarna föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras.

63 §. *Tekniska identifieringskoder och elektroniska kommunikationskoder samt skapande av dessa.* Det föreslås att 2 mom. ändras så att det till 1 punkten fogas ett omnämnande av identifieringsuppgifter för fysiska personer som Myndigheten för digitalisering och befolkningsdata med stöd av eIDAS-lagen utfärdar för fysiska personer. Enligt 3 § i eIDAS-lagen utfärdar Myndigheten för digitalisering och befolkningsdata identifieringsuppgifter för fysiska personer för den europeiska digitala identitetsplånbok som myndigheten tillhandahåller. En elektronisk kommunikationskod kan också användas på det sätt som föreslås ovan i 43 § 2 mom. som en uppgift som identifierar innehavaren av identifieringsuppgifter för en fysisk person.

66 §. *Ansökan om och utfärdande av medborgarcertifikat.* Hänvisningarna i 2 och 3 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till hänvisningar till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras. I paragrafen görs också en lagteknisk korrigering.

67 §. *Ansökan om och utfärdande av andra certifikat.* Hänvisningen i 1 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras.

7.8 Lagen om behandling av kunduppgifter inom social- och hälsovården

8 §. *Identifiering av dem som deltar i behandlingen av kunduppgifter.* Hänvisningen i 2 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Kortnamnet på lagen ändras till autentiseringslagen. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras. I paragrafen görs också en lagteknisk korrigering.

65 §. *De riksomfattande informationssystemtjänsterna inom social- och hälsovården.* I 3 mom. används på finska det i 8 § angivna kortnamnet tunnistus- ja luottamuspalvelulaki, som i enlighet med den ändrade 8 § på finska ändras till tunnustuslaki. I paragrafen ändras dessutom omnämnandet av Tillstånds- och tillsynsverket för social- och hälsovården till Tillstånds- och tillsynsverket.

7.9 Lagen om förhindrande av penningtvätt och av finansiering av terrorism

3 kap. Kundkontroll

11 §. *Skärpta åtgärder för kundkontroll vid identifiering på distans.* Hänvisningen i 3 punkten till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras. Också den

hänvisning till eIDAS-förordningen som finns i bestämmelsen ändras så att det framgår av den att förordningen har reviderats.

7.10 Jordabalken

9 a kap. Elektroniska ärendehanteringssystem och deras användning

1 §. *Användning av ärendehanteringssystem och elektronisk identifiering i ett ärendehanteringssystem.* Hänvisningen i 1 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras. Också den hänvisning till eIDAS-förordningen som finns i bestämmelsen ändras så att det framgår av den att förordningen har reviderats.

7.11 Lagen om medborgarinitiativ

7 §. *Tekniska krav på elektroniskt förfarande.* Hänvisningen i 1 mom. 1 punkten till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras.

7.12 Lagen om förfarandet vid rådgivande folkomröstningar i välfärdsområden och kommuner

4 §. *Initiativ till folkomröstning.* Hänvisningen i 3 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras.

7.13 Lagen om fonderna inom området för inrikes frågor under programperioden 2021–2027

15 §. *Ansökan om understöd.* Hänvisningen i 4 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras.

26 §. *E-tjänst- och behandlingssystemet för programmet för fonderna inom området för inrikes frågor samt behandling av uppgifter.* Hänvisningen i 3 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras. Dessutom ändras hänvisningen lagtekniskt, eftersom paragrafen efter de föreslagna ändringarna endast har ett moment.

7.14 Lagen om identitetskort

1 a §. *E-legitimation.* Det föreslås att det till lagen fogas en ny paragraf, enligt vilken det i identitetskort som avses i 2 § 1 mom., 14 och 15 a § samt 17 § 3 mom. ingår rätt att få tillgång till en e-legitimation som avses i det tredje lagförslaget. Genom bestämmelsen säkerställs entydigt den rättsliga ställningen för en i 2 § 1 mom. 9 punkten i det tredje lagförslaget avsedd handling som utgör grund för en e-legitimation i fråga om de identitetskort som nämns i den föreslagna paragrafen.

11 §. Identifiering av sökanden och verifiering av sökandens identitet. Hänvisningen i 4 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras.

7.15 Partilagen

3 §. Registreringsansökan. Hänvisningen i 1 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras.

7.16 Lagen om finansiering av projekt inom regionutveckling och Europeiska unionens regional- och strukturpolitik

52 §. Stark autentisering vid användning av informationssystemet för Europeiska unionens regional- och strukturpolitiska program. Hänvisningen i paragrafen till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras.

7.17 Passlagen

3 d §. E-legitimation. Det föreslås att det till lagen fogas en ny paragraf, enligt vilken det i pass som avses i 3 och 3 c § samt 4 § ingår rätt att få tillgång till en e-legitimation som avses i lagen om e-legitimation. Genom bestämmelsen säkerställs entydigt den rättsliga ställningen för en i 2 § 1 mom. 9 punkten i det tredje lagförslaget avsedd handling som utgör grund för en e-legitimation i fråga om de pass som nämns i den föreslagna paragrafen.

6 §. Ansökan om pass. Hänvisningen i 4 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras.

7.18 Lagen om stödjande av landsbygdens utveckling under finansieringsperioden 2023–2027

31 §. Ansökan om stöd. Hänvisningen i 1 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras. I paragrafen görs också en lagteknisk korrigering.

7.19 Lagen om verkställighet av vissa av Europeiska unionens jordbruksstöd och vissa nationella jordbruksstöd

12 §. Ansökan om stöd. Hänvisningen i 1 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras. I paragrafen görs också en lagteknisk korrigering.

7.20 Lagen om det nationella genomförandet av Europeiska unionens gemensamma fiskeripolitik

32 §. *Innehavarens rätt att använda uppgifterna i fiskekvotsregistret.* Hänvisningen i 2 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras. Dessutom ändras hänvisningen lagtekniskt, eftersom paragrafen efter de föreslagna ändringarna endast har ett moment.

7.21 Lagen om behandling av personuppgifter i polisens verksamhet

41 §. *Tillgodoseende av den registrerades rätt till insyn.* Hänvisningen i 2 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras. I finska paragrafen görs också en lagteknisk korrigering.

7.22 Lagen om behandling av personuppgifter inom Tullen

35 §. *Tillgodoseende av den registrerades rätt till insyn.* Hänvisningen i 2 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras. I paragrafen görs också en lagteknisk korrigering.

7.23 Lagen om strukturstöd till jordbruket

29 §. *Ansökan om stöd.* Hänvisningen i 1 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering, och samtidigt korrigeras ett tekniskt fel i hänvisningen till lagen. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras. I paragrafen görs också en lagteknisk korrigering.

7.24 Lagen om behandling av personuppgifter vid Gränsbevakningsväsendet

50 §. *Tillgodoseende av den registrerades rätt till insyn.* Hänvisningen i 2 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras.

7.25 Lagen om en marknadsordning för jordbruksprodukter

70 a §. *Elektronisk ansökan.* Hänvisningen i 1 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering, och samtidigt korrigeras ett tekniskt fel i hänvisningen till lagen. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras. I paragrafen görs också en lagteknisk korrigering.

7.26 Konsumentskyddslagen

6 kap. Hemförsäljning och distansförsäljning

12 c §. *Kontroll av identiteten hos konsumenter och bevarande av uppgifterna om kontrollen i vissa fall.* Hänvisningen i 1 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras.

7 kap. Konsumentkrediter

15 §. *Kontroll av kreditsökandens identitet.* Hänvisningen i 1 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras.

7 a kap. Konsumentkrediter som har samband med bostadsegendom

33 §. *Tillsynsmyndigheter.* Hänvisningen i 2 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras. I paragrafen korrigeras också namnet på Transport- och kommunikationsverket.

10 kap. Tidsdelat boende och långfristiga semesterprodukter

6 §. *Avtalets form och språk.* Det föreslås att 1 mom. ändras. Hänvisningen i det gällande momentet till lagen om stark autentisering och elektroniska signaturer ändras till en hänvisning till eIDAS-förordningen. Den nuvarande hänvisningen i momentet är föråldrad och bestämmelser om elektroniska signaturer finns i eIDAS-förordningen.

Till momentet fogas också en informativ hänvisning till 7 a kap. i konsumentskyddslagen, som innehåller bestämmelser om konsumentkrediter som har samband med bostadsegendom.

7.27 Lagen om strukturstöd för renhushållning och naturnäringar

48 §. *Ansökan om stöd.* Hänvisningen i 1 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras. I paragrafen görs också en lagteknisk korrigering.

7.28 Skjutvapenlagen

119 a §. *Elektroniska tjänster.* Hänvisningen till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras.

7.29 Fordonslagen

84 §. *Bestämmelser om registreringsanmälan.* Hänvisningen i 3 mom. till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras.

7.30 Konkurrenslagen

39 §. Informationsutbytet mellan myndigheterna. Hänvisningen i 1 mom. 9 punkten till lagen om stark autentisering och betrodda elektroniska tjänster ändras till en hänvisning till lagen om stark autentisering. Ändringen föranleds av att det i det andra lagförslaget föreslås att namnet på lagen om stark autentisering och betrodda elektroniska tjänster ändras. Dessutom ändras hänvisningen till den upphävda lagen om stöd för byggande av bredband i glesbygdsområden (1186/2009) till en hänvisning till lagen om stöd för byggande av fast bredband (1262/2020).

8 Bestämmelser på lägre nivå än lag

Propositionen innehåller flera förslag om bemyndiganden för Transport- och kommunikationsverket att utfärda föreskrifter. Det är huvudsakligen fråga om att bevara befintliga bemyndiganden att utfärda föreskrifter så att en del av dem flyttas från autentiseringslagen till den föreslagna nya eIDAS-lagen. Dessutom föreslås ett antal nya bemyndiganden för Transport- och kommunikationsverket att utfärda föreskrifter.

Följande föreslås:

- Enligt 7 § 4 mom. i eIDAS-lagen får Transport- och kommunikationsverket utfärda närmare föreskrifter om hur de uppgifter som avses i 2 och 3 mom. ska lämnas. Det är fråga om ett nytt normgivningsbemyndigande.
- Enligt 16 § 3 mom. i eIDAS-lagen får Transport- och kommunikationsverket utfärda närmare föreskrifter om genomförandet av förlitandepartcertifikat och förlitandepartregistreringscertifikat för en europeisk digital identitetsplånbok samt om certifikatspolicy och certifieringspraxis för dem, med iakttagande av bestämmelser som utfärdats med stöd av artikel 5b i eIDAS-förordningen. Det är fråga om ett nytt normgivningsbemyndigande.
- Enligt 24 § 2 mom. i eIDAS-lagen får Transport- och kommunikationsverket utfärda närmare föreskrifter om bedömningsgrunderna för bedömning av överensstämmelse av den nationella noden med iakttagande av eIDAS-förordningen och bestämmelser som utfärdats med stöd av den. Det är fråga om ett normgivningsbemyndigande i 42 § 2 mom. 5 punkten i autentiseringslagen som enligt förslaget flyttas till den föreslagna eIDAS-lagen.
- Enligt 25 § 3 mom. i eIDAS-lagen får Transport- och kommunikationsverket utfärda närmare föreskrifter om den nationella certifieringsordningen för en europeisk digital identitetsplånbok samt om bedömningsgrunderna för bedömning av överensstämmelse av plånboken och om det förfarande som ska iakttas vid bedömning av överensstämmelse, med iakttagande av eIDAS-förordningen och bestämmelser som har utfärdats med stöd av den. Det är fråga om ett nytt normgivningsbemyndigande.
- Enligt 26 § 4 mom. i eIDAS-lagen får Transport- och kommunikationsverket, med iakttagande av eIDAS-förordningen och bestämmelser som utfärdats med stöd av den, utfärda närmare föreskrifter om förutsättningarna för att utse ett organ för bedömning av överensstämmelse, de uppgifter som ska ingå i en ansökan om utseende av ett organ för bedömning av överensstämmelse och inlämnandet av uppgifterna till Transport- och kommunikationsverket samt grunderna för bedömning av överensstämmelse i fråga om system för elektronisk identifiering och betrodda tjänster och förfarandet vid bedömning av överensstämmelse. Det är fråga om normgivningsbemyndiganden som

finns i 42 § 2 mom. 5–7 punkten i autentiseringslagen och som enligt förslaget i något förändrad form flyttas till den föreslagna eIDAS-lagen.

- Enligt 28 § 4 mom. i eIDAS-lagen får Transport- och kommunikationsverket utfärda närmare föreskrifter om kraven på certifierare, det förfarande som ska iakttas vid certifiering samt kraven på anordningar för skapande av elektroniska underskrifter och elektroniska stämplatser med iakttagande av eIDAS-förordningen och bestämmelser som utfärdats med stöd av den. Det är fråga om ett normgivningsbemyndigande som finns i 42 § 2 mom. 8 punkten i autentiseringslagen och som enligt förslaget flyttas till den föreslagna eIDAS-lagen.

Dessutom innehåller autentiseringslagens 42 §, som föreslås bli ändrad, bemyndiganden att utfärda föreskrifter, vilka, med undantag av ett, redan ingår i den gällande lagen. Av de bemyndiganden att utfärda föreskrifter som ingår i 42 § i autentiseringslagen stryks i såväl 42 § 2 mom. 5 och 8 punkten som 42 § 2 mom. 6 punkten i den gällande lagen skyldigheten att beakta vad som föreskrivs i EU:s förordning om elektronisk identifiering. Punkterna i fråga gäller bestämmelser som kompletterar eIDAS-förordningen. I fortsättningen ingår all nationell reglering som kompletterar eIDAS-förordningen i eIDAS-lagen, och avsikten är att normgivningsbemyndiganden som motsvarar de punkter som föreslås bli strukna från autentiseringslagen fogas till 24, 26 och 28 § i eIDAS-lagen på det sätt som beskrivs ovan.

Till 42 § i autentiseringslagen fogas ett nytt normgivningsbemyndigande, dvs. en ny 5 punkt, enligt vilken Transport- och kommunikationsverket får meddela närmare föreskrifter om de behövliga uppgifter som avses i 24 § 2 mom. och som ska registreras om den inledande identifieringen av sökanden och om de handlingar eller om den elektroniska identifiering som används i den inledande identifieringen. Antalet inledande identifieringar av sökanden på distans har ökat avsevärt. Till exempel fjärravläsning av pass eller identitetskort och andra tillförlitliga metoder för att identifiera sökande på distans utvecklas hela tiden. Leverantörer av identifieringsverktyg kan få in mycket olika uppgifter genom inledande identifieringar, beroende på hur en inledande identifiering genomförs. Det är motiverat att mer exakt definiera vilka uppgifter som ska registreras för att säkerställa att de uppgifter som är nödvändiga för att utreda felsituationer finns att tillgå. I synnerhet förfarandet för identifiering på distans ökar behovet av att definiera de tekniska detaljerna om de uppgifter som ska lagras.

Föreskrifter som utfärdas på grundval av de i autentiseringslagen föreskrivna bemyndigandena för Transport- och kommunikationsverket att utfärda föreskrifter ska eventuellt anmälas till Europeiska kommissionen i enlighet med direktivet (EU) 2015/1535 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster. Anmälningsskyldigheten gäller nationella lagändringar eller andra föreskrifter som innehåller tekniska specifikationer eller andra krav som ställs på produkter eller informationssamhällets tjänster. Efter anmälningen inleds en tre månader lång väntetid i enlighet med direktivet som måste löpa ut innan förslaget till föreskrift kan godkännas. Medlemsstaterna ska till kommissionen överlämna utkastet till teknisk föreskrift ännu en gång om de gör ändringar i det som i väsentlig grad förändrar dess tillämpningsområde, förkortar den tid som ursprungligen tänkts för genomförandet, lägger till specifikationer eller andra krav eller skärper dessa. Behovet av att anmäla föreskrifter bedöms närmare när innehållet i dem preciseras.

9 Ikraftträdande

Det föreslås att lagarna träder i kraft så snart som möjligt under hösten 2026. Ändringarna av eIDAS-förordningen trädde i kraft den 20 maj 2024. Lagförslagen omfattar dock övergångsperioder och små undantag i fråga om tidpunkten för ikraftträdandet.

Myndigheten för digitalisering och befolkningsdata ska anpassa sin verksamhet så att den överensstämmer med 3, 4, 7–9 § och 17 § 1 mom. och 23 § i det första lagförslaget senast den 24 december 2026. På samma sätt ska Patent- och registerstyrelsen anpassa sin verksamhet så att den överensstämmer med 5 och 6 § i det första lagförslaget inom motsvarande tid. I paragraferna i fråga föreskrivs det om utfärdande av identifieringsuppgifter för fysiska och juridiska personer och registren i anslutning till dessa, tillhandahållande av plånboken och förande av register i anslutning till denna, inklusive lagringstid, samt en valideringsmekanism för plånbokens äkthet och giltighet. Avsikten är också att genom 23 § genomföra artikel 45e i den reviderade eIDAS-förordningen. Enligt den reviderade eIDAS-förordningen ska plånboken tillhandahållas och de åtgärder som avses i artikel 45e vidtas inom 24 månader från den dag då de genomförandeförordningar som antagits med stöd av artiklarna 5a och 5c träder i kraft. Genomförandeförordningarna i fråga trädde i kraft den 24 december 2024, vilket innebär att skyldigheterna enligt förordningen ska fullgöras senast den 24 december 2026. Genom övergångsperioden säkerställs det att Myndigheten för digitalisering och befolkningsdata samt Patent- och registerstyrelsen kan utnyttja hela den tidsfrist som anges i den reviderade eIDAS-förordningen för tillhandahållande av plånboken och därtill hörande tjänster samt för genomförande av åtgärderna enligt artikel 45e.

Myndigheten för digitalisering och befolkningsdata ska anpassa sin verksamhet så att den överensstämmer med 18 § 1 och 2 mom. i det första lagförslaget senast den 24 december 2026. I paragrafen i fråga föreskrivs det om skyldigheten för Myndigheten för digitalisering och befolkningsdata att genomföra identitetsmatchning. Kommissionen har antagit en genomförandeförordning vad gäller gränsöverskridande identitetsmatchning av fysiska personer (EU) 2025/846, och den ska tillämpas från och med den 24 december 2026. Övergångsperioden överensstämmer således med tidpunkten för när kommissionens genomförandeförordning ska börja tillämpas. eIDAS-lagens 18 § 3 mom. tillämpas dock först fr.o.m. den 1 januari 2028. I det föreslagna 18 § 3 mom. föreskrivs det om den privata sektorns rätt att använda den identitetsmatchning som genomförs av Myndigheten för digitalisering och befolkningsdata. Momentet börjar tillämpas efter det att skyldigheten för e-tjänster inom den privata sektorn att godta identifiering med den europeiska digitala identitetsplånboken har trätt i kraft.

Transport- och kommunikationsverket ska anpassa sin verksamhet så att den överensstämmer med 16 § och 17 § 2 mom. i det första lagförslaget senast den 24 december 2026. I de ovannämnda paragraferna föreskrivs det om Transport- och kommunikationsverkets skyldighet att inrätta ett nationellt register över europeiska digitala identitetsplånböckers förlitande parter och att tillhandahålla en valideringsmekanism som gäller äkthet och giltighet för identiteten hos förlitande parter. Kommissionen har antagit en genomförandeförordning vad gäller registrering av förlitande parter (EU) 2025/848, och den tillämpas fr.o.m. den 24 december 2026. Övergångsperioden överensstämmer således med tidpunkten för när kommissionens genomförandeförordning ska börja tillämpas.

Avsikten är att e-legitimation ska kunna användas i den europeiska digitala identitetsplånboken, som ska tillhandahållas på det sätt som beskrivs ovan senast den 24 december 2026. Det föreslås därför att myndigheterna ska anpassa sin verksamhet så att den överensstämmer med det tredje lagförslaget senast den 24 december 2026. Övergångsperioden är alltså i linje med tidsfristen

för tillhandahållande av plånboken. Även de lagförslag som gäller lagen om identitetskort och passlagen innehåller övergångsbestämmelser med avseende på e-legitimation. De föreslagna övergångsbestämmelserna ger upphov till en rätt till e-legitimation med ett sådant identitetskort som avses i 2 § 1 mom., 14 och 15 a § samt 17 § 3 mom. i lagen om identitetskort och med ett sådant pass som avses i 3, 3 c och 4 § i passlagen och som har utfärdats innan den föreslagna lagen träder i kraft.

Med avvikelse från den ovan föreslagna tidpunkten för lagens ikraftträdande träder 7 b § och 17 § 2 mom. i det andra lagförslaget i kraft först den 1 januari 2027. I dessa paragrafer föreskrivs det om en ny skyldighet för leverantörer av identifieringstjänster att kontrollera vissa handlingars giltighet och möjliggörs användning av e-legitimation i samband med inledande identifiering. I enlighet med vad som beskrivs ovan föreslås en övergångsperiod fram till den 24 december 2026 för genomförandet av e-legitimationer, och det ska alltså vara möjligt att använda dessa vid inledande identifiering först efter denna övergångsperiod. En övergångsperiod behövs också för att tjänsteleverantörerna ska hinna göra nödvändiga ändringar i sina system så att de i myndighetens informationssystem kan kontrollera giltigheten hos handlingar som används vid inledande identifiering.

10 Verkställighet och uppföljning

Enligt artikel 46e i den reviderade eIDAS-förordningen ska kommissionen inrätta en europeisk samarbetsgrupp för digital identitet bestående av företrädare som utnämns av medlemsstaterna och av kommissionen. Syftet med samarbetsgruppen är att stödja och underlätta medlemsstaternas gränsöverskridande samarbete och informationsutbyte om betrodda tjänster, europeiska digitala identitetsplånböcker och anmälda system för elektronisk identifiering. Samarbetsgruppen arbetar strategiskt, bl.a. genom att utbyta råd och samarbeta med kommissionen om nya politiska initiativ och genom att utvärdera utvecklingen på området digitala identitetsplånböcker. Gruppen har dock också uppgifter som kräver djupare och mer teknisk kompetens, såsom att anordna sakkunnigbedömningar av system för elektronisk identifiering som ska anmälas enligt denna förordning. Myndigheten för digitalisering och befolkningsdata ska delta i samarbetsgruppens arbete och dessutom deltar Myndigheten för digitalisering och befolkningsdata och Transport- och kommunikationsverket i en arbetsgrupp som inrättats under samarbetsgruppen. Detta gör det möjligt att påverka samarbetsgruppens arbete och få information om arbetet.

Artikel 49 i den reviderade eIDAS-förordningen innehåller en s.k. översynsklausul. Kommissionen ska senast den 21 maj 2026 göra en översyn över tillämpningen av förordningen och rapportera resultaten till Europaparlamentet och rådet. I rapporten ska kommissionen särskilt utvärdera huruvida det är lämpligt att ändra förordningens tillämpningsområde eller dess särskilda bestämmelser, inbegripet särskilt bestämmelserna i artikel 5c.5, med beaktande av den erfarenhet som erhållits vid tillämpningen av förordningen samt den tekniska och rättsliga utvecklingen och marknadsutvecklingen. Kommissionen ska vid behov bifoga ett förslag till ändring av den reviderade eIDAS-förordningen.

Dessutom kräver den reviderade eIDAS-förordningen att medlemsstaterna ska säkerställa att det samlas in statistik om hur europeiska digitala identitetsplånböcker och de kvalificerade betrodda tjänsterna används. Enligt artikel 48a i den reviderade eIDAS-förordningen ska medlemsstaterna varje år lämna en rapport om den statistik som samlats in i enlighet med den artikeln till kommissionen.

Transport- och kommunikationsverket är redan nu den myndighet som utövar tillsyn över efterlevnaden av autentiseringslagen. Enligt propositionen är verket också tillsynsorgan enligt

artikel 46a i den reviderade eIDAS-förordningen och gemensam kontaktpunkt enligt artikel 46c i den förordningen. Dessutom utövar verket tillsyn över efterlevnaden av eIDAS-lagen. Transport- och kommunikationsverket ansvarar således för uppföljningen och styrningen av genomförandet av bestämmelserna om europeiska digitala identitetsplånböcker, stark autentisering och elektroniska betrodda tjänster samt för rådgivningen i anslutning till detta. Det föreslås också att Transport- och kommunikationsverket i fortsättningen bevakar t.ex. iakttagandet av kostnadsmotsvarighetsnivån för de avgifter som den tar ut. Grundlagsutskottet har i en situation där det har ansetts vara fråga om en avgift i stället för en skatt sett det som nödvändigt att statsrådet bevakar iakttagandet av avgifternas kostnadsmotsvarighetsnivå.

11 Förhållande till andra propositioner

Regeringens proposition till riksdagen med förslag till lagstiftning om genomförande av cyberresiliens-förordningen (RP 179/2025 rd) har överlämnats till riksdagen. I den propositionen föreslås det att det stiftas en ny lag om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering, som det hän-visas till i 36 § i det första lagförslaget. I den ovannämnda propositionen föreslås det också en ändring av lagen om verkställighet av böter, som är av betydelse för det sjätte lagförslaget i denna proposition. Dessa propositioner ska vid behov samordnas i riksdagen.

Riksdagen behandlar för närvarande flera propositioner där det – i likhet med det sjätte lagförslaget i denna proposition – föreslås en ändring av 1 § 2 mom. i lagen om verkställighet av böter. Dessa propositioner är utöver den proposition som nämns i det föregående stycket även regeringens proposition till riksdagen med förslag till lag om karens i anslutning till uppdraget som medlem av statsrådet och lag om ändring av 1 § i lagen om verkställighet av böter (RP 90/2024 rd), regeringens proposition till riksdagen med förslag till lag om underlättande av utbyggnad av nät med mycket hög kapacitet och till lagar om ändring av 249 och 303 § i lagen om tjänster inom elektronisk kommunikation och 1 § i lagen om verkställighet av böter (RP 74/2025 rd), regeringens proposition till riksdagen med förslag till lag om tillsyn över skyldigheterna och om påföljder enligt EU:s avskogningsförordning samt till lagar som har samband med den (RP 77/2025 rd), regeringens proposition till riksdagen med förslag till lag om ändring av renskötsellagen och till lagar som har samband med den (RP 161/2025 rd) och regeringens proposition till riksdagen med förslag till lagstiftning om europeiska utlämnandeorder och europeiska bevarande-order för elektroniska bevis (RP 175/2025 rd). Dessutom pågår ett projekt för beredning av regeringens proposition till riksdagen med förslag till lag om ändring av lagen om jämställdhet mellan kvinnor och män (genomförande av lönetransparensdirektivet), [STM069:00/2024](#), som ska överlämnas till riksdagen vecka 11/2026. I den propositionen föreslås även en ändring av 1 § 2 mom. i lagen om verkställighet av böter. De ovannämnda lagförslagen om ändring av 1 § 2 mom. i lagen om verkställighet av böter ska vid behov samordnas i riksdagen.

Ett projekt om ändring av passlagen och lagen om identitetskort, [SM020:00/2025](#), har inletts med avsikten att bereda en regeringsproposition som ska överlämnas till riksdagen vecka 14/2026. I den propositionen torde också, i likhet med det sjuttonde lagförslaget i denna proposition, ingå ett förslag till ändring av 6 § passlagen. Dessa lagförslag ska vid behov samordnas i riksdagen.

12 Förhållande till grundlagen samt lagstiftningsordning

12.1 Inledning

Regeringspropositionens lagförslag är av betydelse med tanke på 6, 8, 10, 15, 18, 21, 80, 81 och 124 § i grundlagen.

12.2 Jämlikhet

Det första lagförslaget i regeringens proposition har konsekvenser för den jämlikhet som garanteras i grundlagen. Enligt 6 § 1 mom. i grundlagen är alla lika inför lagen. I bestämmelsen uttrycks utöver kravet på rättslig jämlikhet även en tanke på faktisk jämställdhet. Där ingår ett förbud mot godtycke och ett krav på likabehandling i likartade fall. Den allmänna jämlikhetsbestämmelsen kompletteras genom diskrimineringsförbudet i 6 § 2 mom. i grundlagen, enligt vilket ingen utan godtagbart skäl får särbehandlas på grund av kön, ålder, ursprung, språk, religion, övertygelse, åsikt, hälsotillstånd eller handikapp eller av någon annan orsak som gäller hans eller hennes person. En sådan annan orsak kan vara t.ex. boningsort (se RP 309/1993 rd, s. 45–47, t.ex. GrUU 15/2018 rd, s. 6–7, GrUU 26/2017 rd, s. 36–41 och 44–45 och GrUU 67/2014 rd, s. 3).

Närmare bestämmelser om likabehandling och förbud mot diskriminering finns i diskrimineringslagen, vars 2 kap. förbjuder både direkt och indirekt diskriminering. Enligt 13 § i den lagen ska indirekt diskriminering anses förekomma när regler, kriterier eller förfaringsätt som framstår som jämlika kan komma att missgynna någon på grund av en omständighet som gäller honom eller henne som person, om inte regeln, kriteriet eller förfaringsättet har ett godtagbart syfte och medlen för att nå detta syfte är lämpliga och behövliga. Även grundlagsutskottet har betonat att förbudet mot diskriminering gäller också åtgärder som indirekt leder till ett diskriminerande resultat (GrUU 31/2014 rp, s. 3).

Diskriminering förbjuds också uttryckligen i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och i EU:s stadga om de grundläggande rättigheterna. Enligt artikel 14 i Europakonventionen ska åtnjutandet av de fri- och rättigheter som anges i konventionen säkerställas utan diskriminering på någon grund såsom kön, ras, hudfärg, språk, religion, politisk eller annan åsikt, nationellt eller socialt ursprung, tillhörighet till nationell minoritet, förmögenhet, börd eller ställning i övrigt. Inom EU-rätten har jämlikhetsprincipen fastställts i artikel 20 i EU:s stadga om de grundläggande rättigheterna, enligt vilken alla är lika inför lagen. Förbudet mot diskriminering ingår i artikel 21.1 som förbjuder all diskriminering på grund av bland annat kön, ras, hudfärg, etniskt eller socialt ursprung, genetiska särdrag, språk, religion eller övertygelse, politisk eller annan åskådning, tillhörighet till nationell minoritet, förmögenhet, börd, funktionshinder, ålder eller sexuell läggning. I artikel 21.2 förbjuds dessutom diskriminering på grund av nationalitet.

Finland har dessutom förbundit sig att uppfylla kraven i konventionen om rättigheter för personer med funktionsnedsättning (funktionsrättskonventionen). Både EU och alla dess medlemsstater är parter i FN:s konvention om rättigheter för personer med funktionsnedsättning. Konventionen ålägger konventionsstaterna att vidta lämpliga åtgärder för att säkerställa att personer med funktionsnedsättning får lika tillgång till bl.a. informations- och kommunikationsteknik och IKT-system. Artikel 12.3 i konventionen kräver att konventionsstaterna tillåter personer med funktionsnedsättning att vid behov sköta sina ärenden med assistans av en annan person. Enligt artikel 12.3 ska konventionsstaterna vidta ändamålsenliga åtgärder för att erbjuda personer med funktionsnedsättning tillgång till det stöd de kan behöva för att utöva sin rättskapacitet. Stöd för utövande av rättskapacitet ska erbjudas

med respekt för personernas rättigheter, vilja och preferenser, t.ex. i form av en personlig assistent som kan hjälpa dem i en digital miljö.

Ett av målen med lagstiftningen om den europeiska digitala identitetsplånboken är att främja möjligheten till elektronisk identifiering. Likabehandlingen av personer med funktionsnedsättning när det gäller användningen av plånboken har uttryckligen tryggats genom artikel 5a.21 i den reviderade eIDAS-förordningen, enligt vilken europeiska digitala identitetsplånböcker ska göras tillgängliga för användning av personer med funktionsnedsättning, på samma villkor som andra användare, i enlighet med tillgänglighetsdirektivet.

I denna proposition innehåller 14 § i det första lagförslaget en bestämmelse om att användare av den europeiska digitala identitetsplånboken ska använda applikationen omsorgsfullt och inte överlåta den till någon annan. Enligt den föreslagna 15 § 1 mom. 1 punkten ansvarar dessutom användaren av plånboken för obehörig användning av applikationen endast om användaren har överlåtit applikationen till någon annan för användning. Grundlagsutskottet har tidigare betraktat motsvarande bestämmelser som problematiska med tanke på FN:s funktionsrättskonvention och 6 § 2 mom. i grundlagen (GrUU 83/2022 rd). Grundlagsutskottet konstaterade i sitt utlåtande att det, om unionsrätten möjliggör det, genom bestämmelser i lag ska tillåtas att en assistent till en person med funktionsnedsättning på begäran av personen i fråga kan bistå denne vid användningen av ett identifieringsverktyg. Likaså ska det tydligt framgå av lagen att det i detta fall inte är fråga om obehörig användning eller överlåtelse av verktyget för att användas av någon annan. I propositionen föreslås en reglering som motsvarar bestämmelserna i den proposition som var föremål för det ovannämnda utlåtandet av grundlagsutskottet (RP 133/2022 rd). Regleringen har i den mån det är möjligt enligt EU-rätten beretts med iakttagande av de ställningstaganden som förts fram i grundlagsutskottets utlåtande (GrUU 89/2022 rd).

Bestämmelsen i 14 § i det första lagförslaget är i första hand en bestämmelse som fastställer omfattningen av användarens aktsamhetsplikt och som understryker den personliga karaktären hos den europeiska digitala identitetsplånboken. Den reviderade eIDAS-förordningen reglerar inte användarens skyldigheter eller ansvarssituationer, utan dessa hör till det nationella handlingsutrymmet. I specialmotiveringen till den föreslagna 14 § anges uttryckligen att bestämmelsen inte begränsar principen i den reviderade eIDAS-förordningen, enligt vilken plånboken ska vara tillgänglig för personer med funktionsnedsättning på lika villkor som för andra användare. Syftet med bestämmelserna om användarens ansvar är således inte att begränsa eller på annat sätt ta ställning till vilka krav enligt tillgänglighetsdirektivet som kan eller inte kan tillämpas på användningen av plånboken.

Utöver bestämmelserna i den reviderade eIDAS-förordningen ska tillhandahållaren av plånboken också ta hänsyn till bestämmelserna i diskrimineringslagen. Enligt 15 § i diskrimineringslagen ska myndigheter, utbildningsanordnare, arbetsgivare och de som tillhandahåller varor eller tjänster göra sådana ändamålsenliga och rimliga anpassningar som behövs i det enskilda fallet för att göra det möjligt för personer med funktionsnedsättning att på lika villkor som andra använda myndigheters tjänster samt att få utbildning och arbete samt varor och tjänster som tillhandahålls allmänheten och att klara av sina arbetsuppgifter och avancera i arbetet. Vid bedömningen av vilka anpassningar som är rimliga beaktas i första hand behoven hos personer med funktionsnedsättning och dessutom aktörens storlek och ekonomiska ställning, arten och omfattningen av aktörens verksamhet, de uppskattade kostnaderna för anpassningarna och stöd som kan fås för åtgärderna. Exempel på möjliga anpassningsformer kan vara, beroende på användarnas behov, att skicka dokument med punktskrift, tillhandahålla koder i elektronisk form, identifiera fingeravtryck eller tillåta anlitande av en personlig assistent.

Den som tillhandahåller plånboken ska dock bedöma vilka anpassningsformer som är möjliga när det gäller den europeiska digitala identitetsplånboken med hänsyn till de krav som EU-rätten ställer på plånboken, så att principen om lika rättigheter för personer med funktionsnedsättning kan genomföras i praktiken.

I specialmotiveringen till den föreslagna 14 § konstateras det att om den som tillhandahåller plånboken har gjort anpassningar som gör det möjligt för personer med funktionsnedsättning att använda den europeiska digitala identitetsplånboken på lika villkor som andra och möjliggjort exempelvis användning av personlig assistent, ska dessa anpassningar beaktas när man bedömer om användaren har överlåtit plånboken till någon annan för användning. Det är t.ex. i regel inte fråga om överlåtande av plånboken till någon annan för användning om den som tillhandahåller plånboken som en rimlig anpassning har gjort det möjligt att använda personlig assistent. Likaså har det i specialmotiveringen till den föreslagna 15 § konstaterats att vid bedömning av användarens ansvar för obehörig användning av plånboken i situationer där personen själv har överlåtit plånboken till någon annan för användning ska hänsyn tas till huruvida tillhandahållaren av plånboken har gjort anpassningar som möjliggör användning av den europeiska digitala identitetsplånboken på lika villkor och t.ex. gjort det möjligt att använda personlig assistent. Av specialmotiveringen framgår det således på det sätt som grundlagsutskottet kräver tydligt att det i regel inte är fråga om obehörig användning av instrumentet eller överlåtelse av verktyget för att användas av någon annan, när den som tillhandahåller plånboken har gjort det möjligt att anlita personlig assistent.

Vid beredningen av propositionen har det dock inte ansetts vara möjligt ur EU-rättslig synvinkel att på det sätt som anges i grundlagsutskottets utlåtande uttryckligen på lagnivå fastställa att det alltid är möjligt att anlita en personlig assistent för att använda den europeiska digitala identitetsplånboken. I den reviderade eIDAS-förordningen och i Europeiska kommissionens genomförandeförordningar, som kompletterar denna, fastställs gemensamma krav för alla plånböcker som tillhandahålls i EU. I punkt 2.2 i förordningen om tillitsnivåer för elektronisk identifiering föreskrivs det om kraven på hanteringen av medel för elektronisk identifiering. Enligt denna ska medlet för elektronisk identifiering på tillitsnivån väsentlig vara utformat så att det kan antas att det endast används under ägarens kontroll eller innehav. Detta krav tillämpas också på tillitsnivån hög, vars krav måste uppfyllas när det gäller att tillhandahålla en europeisk digital identitetsplånbok. Medlemsstaterna har inget nationellt handlingsutrymme för att närmare föreskriva om dessa krav.

När en personlig assistent anlitas är det sannolikt att lösenord eller andra autentiseringsfaktorer i samband med användningen av den europeiska digitala identitetsplånboken måste överlämnas till assistenten. I praktiken kan detta leda till en situation där plånboken inte längre används under ägarens kontroll eller innehav på det sätt som avses i förordningen om tillitsnivåer för elektronisk identifiering, eftersom lösenord eller andra identifieringsuppgifter som överlämnas till en personlig assistent gör det möjligt att använda plånboken på egen hand utan den egentliga användarens medverkan. I bestämmelserna om användningen av personlig assistent är det därför inte längre fråga om reglering av användarens ansvar i samband med användningen av plånboken, vilket avses i 14 och 15 § i det första lagförslaget. Vid beredningen av propositionen har det bedömts att en uttrycklig nationell bestämmelse om att en personlig assistent i regel alltid kan hjälpa en person med funktionsnedsättning att använda en europeisk digital identitetsplånbok snarare utgör reglering som preciserar innehavet av eller kontrollen över plånboken och följaktligen i princip överlappar punkt 2.2 i förordningen om tillitsnivåer för elektronisk identifiering, i fråga om vilken medlemsstaterna inte har något nationellt handlingsutrymme. Grundlagsutskottet har i sin utlåtandep Praxis konstaterat att det i och för sig är klart att unionslagstiftningen enligt EU-domstolens rättspraxis har företräde framför nationell rätt i överensstämmelse med de villkor som lagts fast i denna rättspraxis (se t.ex. GrUU 14/2018

rd, s. 13 och GrUU 20/2017 rd, s. 6), och att det inte finns skäl att i vår nationella lagstiftning gå in för lösningar som strider mot EU-lagstiftningen (GrUU 15/2018 rd, s. 49, GrUU 14/2018 rd, s. 13, GrUU 26/2017 rd, s. 42).

Trots att det inte finns någon uttrycklig bestämmelse som möjliggör anlitande av en personlig assistent vid användningen av en europeisk digital identitetsplånbok är de lika möjligheterna för personer med funktionsnedsättning att använda en europeisk digital identitetsplånbok tryggade på ett korrekt sätt och på författningsnivå genom artikel 5a.21 i den reviderade eIDAS-förordningen. För att en plånbok ska kunna certifieras på det sätt som förutsätts i eIDAS-förordningen och tillhandahållas i en medlemsstat måste kraven i den reviderade eIDAS-förordningen och i bestämmelser som kompletterar denna uppfyllas. Den som tillhandahåller plånboken ska dessutom beakta bestämmelserna om rimliga anpassningar i 15 § i diskrimineringslagen. Tillhandahållaren ska dock bedöma vilka anpassningsformer som är möjliga inom de gränser som EU-rätten sätter. Med hänsyn till den ovannämnda EU-lagstiftningen och specialmotiveringen till det första lagförslaget kan man bedöma att den föreslagna lagstiftningen är förenlig med den grundlagstryggade jämlikheten och med funktionsrättskonventionen.

12.3 Skydd av personuppgifter

Bestämmelserna i det första lagförslaget är relevanta med tanke på skyddet för privatlivet och för personuppgifter, som tryggas i 10 § i grundlagen. Enligt 10 § 1 mom. utfärdas närmare bestämmelser om skydd för personuppgifter genom lag. Grundlagsutskottet har tidigare ansett att de regleringsobjekt som är viktiga med tanke på skyddet av personuppgifter är åtminstone registreringens syfte, vilka personuppgifter som ska införas i registret, deras tillåtna användningsändamål, inklusive möjligheten att lämna ut uppgifter, samt uppgifternas förvaringstid i personregistret och den registrerades rättsskydd (GrUU 25/1998 rd). Det har också ansetts att regleringen av dessa objekt på lagnivå ska vara täckande och detaljerad.

Skyddet enligt 10 § i grundlagen kompletteras av skyddet för privatlivet enligt artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (nedan *Europakonventionen*) samt av respekten för privatlivet enligt artikel 7 och skyddet av personuppgifter enligt artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Enligt artikel 52.1 i grundrättighetsstadgan ska varje begränsning i utövandet av de rättigheter och friheter som erkänns i stadgan vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa rättigheter och friheter. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter. Enligt artikel 52.3 i grundrättighetsstadgan ska bestämmelserna i stadgan, i den mån de motsvarar de rättigheter som garanteras i Europakonventionen, ha samma innebörd och räckvidd som i konventionen. Till denna del definierar EU-domstolens domar det centrala innehållet i skyddet för privatlivet och personuppgifter. Likaså har artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna i rättspraxis vid Europeiska domstolen för de mänskliga rättigheterna ansetts omfatta även skyddet för personuppgifter.

12.3.1 Nationellt handlingsutrymme

Den allmänna dataskyddsförordningen är en EU-rättsakt som är förpliktande till alla delar och som tillämpas som sådan i alla medlemsstater. Enligt EU-domstolens vedertagna rättspraxis ska unionens lagstiftning tillämpas primärt i förhållande till nationella bestämmelser i enlighet med de villkor som fastställts i rättspraxisen (se t.ex. GrUU 1/2018 rd). Grundlagsutskottet har

konstaterat att det inte ingår i grundlagsutskottets konstitutionella uppdrag att bedöma regleringen av den nationella verkställigheten med avseende på den materiella EU-rätten (se t.ex. GrUU 31/2017 rd, s. 4). Grundlagsutskottet har dock kommenterat förhållandet mellan EU-lagstiftningen och den nationella lagstiftningen. Utskottet har i sin tolkningspraxis ansett det vara viktigt att till den del EU-lagstiftningen kräver eller möjliggör nationell reglering ska de krav som följer av de grundläggande och mänskliga rättigheterna beaktas i detta nationella handlingsutrymme (se GrUU 25/2005 rd).

Grundlagsutskottet har i sitt utlåtande om lagstiftning som kompletterar den allmänna dataskyddsförordningen sett det som motiverat att justera sin tidigare ståndpunkt om vilka regleringsobjekt som är viktiga med tanke på skyddet av personuppgifter. Utskottet anser att den allmänna dataskyddsförordningens detaljerade bestämmelser, som tolkas och tillämpas i enlighet med de rättigheter som garanteras i EU:s stadga om de grundläggande rättigheterna, över lag utgör en tillräcklig rättslig grund även med avseende på skyddet för privatlivet och personuppgifter enligt 10 § i grundlagen. Enligt utskottets uppfattning motsvarar bestämmelserna i den allmänna dataskyddsförordningen, då de tolkas och tillämpas ändamålsenligt, även den skyddsnivå för personuppgifter som definieras enligt den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Således är det av konstitutionella skäl inte längre nödvändigt att i speciallagstiftningen inom den allmänna dataskyddsförordningens tillämpningsområde ta in täckande och detaljerade bestämmelser om behandlingen av personuppgifter. Enligt grundlagsutskottet bör tillgodoseendet av skyddet för personuppgifter i framtiden i första hand garanteras med stöd av den allmänna dataskyddsförordningen och den nationella allmänna lag som ska stiftas (GrUU 14/2018 rd, s. 4).

Genom lagförslaget kompletteras bestämmelserna om den personuppgiftsansvarige i enlighet med artikel 4.7 i den allmänna dataskyddsförordningen. Med personuppgiftsansvarig avses enligt artikel 4.7 i den allmänna dataskyddsförordningen en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt. Lagen föreslås uttryckligen innehålla en bestämmelse om att Myndigheten för digitalisering och befolkningsdata är personuppgiftsansvarig för den europeiska digitala identitetsplånboken som myndigheten tillhandahåller och de register som gäller tillhandahållandet av den. Plånboken grundar sig på principen om att ha kontroll över sina egna uppgifter, vilket ger användaren möjlighet att bestämma över användningen av uppgifterna i användarens plånbok. De bestämmelser i den reviderade eIDAS-förordningen som gäller att ha kontroll över sina egna uppgifter beskrivs närmare i specialmotiveringen till 8 § i det första lagförslaget. Bestämmelserna om den personuppgiftsansvarige behövs dock för att tydliggöra att Myndigheten för digitalisering och befolkningsdata är personuppgiftsansvarig för den plånbok som den tillhandahåller i den mån det inte är fråga om sådan användning av uppgifter som omfattas av användarens rätt att ha kontroll över sina egna uppgifter. Den föreslagna eIDAS-lagen föreskriver också om rollen som personuppgiftsansvarig i samband med tillhandahållande av identifieringsuppgifter. Myndigheten för digitalisering och befolkningsdata ska föra register över de identifieringsuppgifter för fysiska personer som myndigheten har beviljat och Patent- och registerstyrelsen över de identifieringsuppgifter för juridiska personer som Patent- och registerstyrelsen har beviljat. Den rättsliga grunden för behandling av personuppgifter är artikel 6.1 c i dataskyddsförordningen, som föreskriver om situationer där behandling av personuppgifter behövs för att den personuppgiftsansvariges lagstadgade skyldighet ska fullgöras.

12.3.2 E-legitimation, personuppgifter som ska behandlas och skyddet av dem

I lagförslagen föreskrivs det om ett nytt register över e-legitimationer, som polisen är personuppgiftsansvarig för, och ett nytt register över kvalificerade elektroniska attributsintyg, som Myndigheten för digitalisering och befolkningsdata är personuppgiftsansvarig för. I registren behandlas huvudsakligen personuppgifter som redan finns i befintliga myndighetsregister, såsom uppgifter om personer som införts i befolkningsdatasystemet samt registeruppgifter som ingår i identitetskortsregistret enligt 31 § i lagen om identitetskort och i passregistret enligt 29 § i passlagen. Personuppgifter som ska behandlas är bl.a. personens fullständiga namn och personbeteckning. Andra personuppgifter som ska behandlas är i 4 § i lagen om behandling av personuppgifter i polisens verksamhet avsedda grundläggande uppgifter om en person som införts i identitetskorts- och passregistret, såsom födelsedatum, uppgift om finskt medborgarskap, kön samt fotografi som personen har lämnat till identitetskorts- eller passmyndigheten när han eller hon har ansökt om identitetskort eller pass. Bestämmelser om andra uppgifter som ingår i ett kvalificerat elektroniskt attributsintyg finns dessutom i bilaga V till eIDAS-förordningen. Bestämmelserna i bilagan fastställer datainnehållet i det kvalificerade elektroniska attributsintyget, som innehåller de uppgifter som ingår i e-legitimationen. Med tanke på kravet på nödvändighet när det gäller att samla in uppgifter är det av betydelse att e-legitimationer tas i bruk frivilligt. Dessa nya uppgifter samlas alltså endast in om personer som på eget initiativ tar i bruk en e-legitimation som ett kvalificerat elektroniskt attributsintyg.

I propositionen har hänsyn tagits till de villkor som i den allmänna dataskyddsförordningen ställs på behandling av biometriska uppgifter och uppgifter inom särskilda kategorier av personuppgifter. Med biometriska uppgifter avses enligt artikel 4.14 i den allmänna dataskyddsförordningen personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter. Enligt artikel 9 i den allmänna dataskyddsförordningen omfattar behandling av särskilda kategorier av personuppgifter bl.a. behandling av biometriska uppgifter för att entydigt identifiera en fysisk person. I skäl 51 i den allmänna dataskyddsförordningen konstateras dock uttryckligen att behandling av foton inte systematiskt bör anses utgöra behandling av särskilda kategorier av personuppgifter, eftersom foton endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person. Personuppgifter som hör till särskilda kategorier av personuppgifter bör inte behandlas, såvida inte behandling medges i särskilda fall som fastställs i den allmänna dataskyddsförordningen eller t.ex. för att fullgöra en lagstadgad skyldighet. Utöver de särskilda krav som gäller denna typ av behandling ska också de allmänna principerna och andra reglerna i den allmänna dataskyddsförordningen tillämpas, särskilt när det gäller lagenlig uppgiftsbehandling.

I ett kvalificerat elektroniskt attributsintyg som används som e-legitimation överläts en ansiktsbild på användaren i digital form till användaren själv för att användas i den europeiska digitala identitetsplånboken. Bilden ska användas för att identifiera användaren i samband med fysisk betjäning. Användaren identifieras utifrån den förlitande partens okulära bedömning på samma sätt som när det gäller de traditionella identitetshandlingarna, pass och identitetskort. Förfarandet skiljer sig dock från traditionell skötsel av ärenden med avseende på den elektroniska karaktären hos det verktyg som används för att visa ansiktsbilden och de tekniska lösningarna. För att informationens integritet och tillförlitlighet ska kunna säkerställas kan ansiktsbilden inte kontrolleras på skärmen på användarens egen terminal. Den förlitande parten eller en annan plånboksanvändare lägger trådlöst, t.ex. via en NFC- eller Bluetooth-förbindelse, fram en begäran till användarens plånbok om att få kontrollera ansiktsbilden. Begäran ska utan

undantag innefatta det ändamål som ligger till grund för begäran och som användaren kan godta eller avvisa. Om användaren godtar begäran visas användarens ansiktsbild på den begärande partens enhet i betjäningssituationen. Enligt principen om att användaren har kontroll över sina egna uppgifter kan användaren också själv bestämma om han eller hon godtar eller avvisar en uttrycklig och motiverad begäran från den andra parten om att få registrera användarens uppgifter för något specifikt ändamål. Bestämmelser om användarens rättigheter och den andra partens skyldigheter i detta sammanhang finns förutom i eIDAS-förordningen även i den allmänna dataskyddsförordningen.

Vid identifiering utifrån en ansiktsbild används inga tekniska metoder, utan identifieringen grundar sig alltid på en bedömning som en fysisk person gör utifrån sina egna observationer. E-legitimation gör det således inte möjligt att t.ex. använda särskilda tekniska metoder för att identifiera en person. I det lagförslag som gäller e-legitimation betraktas behandling av fotografier därför inte som sådan behandling av biometriska uppgifter för att entydigt identifiera en fysisk person som avses i artikel 9 i den allmänna dataskyddsförordningen.

Grundlagsutskottet har särskilt lyft fram kravet på ändamålsbundenhet vid behandlingen av känsliga uppgifter. När det gäller omfattande register med biometriska kännetecken av det slag som nu är i fråga finns det enligt grundlagsutskottet orsak att förhålla sig negativt till att uppgifterna används för ändamål som ligger utanför det syfte som de egentligen samlats in och registrerats för (GrUU 14/2009 rd, s. 4/II). Man kan då bara göra exakt avgränsade och som mycket små karakteriserbara undantag från ändamålsbundenheten. Bestämmelserna får inte leda till att någon annan verksamhet än den som är förknippad med det ursprungliga användningsändamålet blir det huvudsakliga ändamålet och inte ens ett betydande användningsändamål (se även t.ex. GrUU 14/2017 rd, s. 5–6). Lagen om behandling av personuppgifter i polisens verksamhet, som stiftats med grundlagsutskottets medverkan, innehåller bestämmelser om behandling av uppgifter i identitetskortsregistret och passregistret för andra ändamål än det ursprungliga. Enligt 13 § 3 mom. i den lagen får fotografi och namnteckningsprov med den berörda personens samtycke även användas för något annat förvaltningstillstånd eller beslut som personen ansökt om än den handling som fotografiet och namnteckningsprovet har lämnats för.

Grundlagsutskottet har velat understryka att när ett register, t.ex. patientregistret, finns på flera ställen och innehåller känsliga uppgifter är det extra viktigt att informationssäkerheten fungerar och förhindrar missbruk och systemet införs samtidigt som registret börjar användas (GrUU 41/2010 rd, s. 3/II). Trots att ansiktsbilder som ingår i de uppgifter som lämnas i samband med ansökan om pass och identitetskort inte som sådana är biometriska uppgifter, ska särskild försiktighet iakttas vid behandlingen av ansiktsbilder på grund av deras särskilda karaktär. Den reviderade eIDAS-förordningen kräver att den europeiska digitala identitetsplånboken uppfyller kraven på tillitsnivån hög. Den ska alltså i princip uppfylla kraven på högsta möjliga nivå av tillförlitlighet och informationssäkerhet. Dessutom certifieras plånboken i enlighet med den reviderade eIDAS-förordningen, och dess överensstämmelse övervakas.

12.3.3 Rätt att få information

Grundlagsutskottet har analyserat bestämmelserna om myndigheternas rätt att trots tystnadsplikten få och lämna ut information med avseende på skyddet för privatlivet och för personuppgifter i 10 § 1 mom. i grundlagen, och då fäst vikt bland annat vid vad och vem rätten att få information gäller och hur rätten är kopplad till nödvändighetskriteriet (GrUU 15/2018 rd). Myndigheternas rätt att få uppgifter och möjlighet att lämna ut uppgifter har kunnat gälla ”behövliga uppgifter” för ett visst syfte, om lagen ger en uttömmande förteckning över innehållet i uppgifterna. Om informationsinnehållen däremot inte anges i form av en

förteckning, ska det i lagstiftningen ingå ett krav på ”att informationen är nödvändig” för ett visst ändamål (se t.ex. GrUU 17/2016 rd, s. 2-3). Å andra sidan har utskottet ansett att grundlagen inte tillåter en generös och ospecificerad rätt att få uppgifter, ens om den är förenad med nödvändighetskriteriet (GrUU 59/2010 rd, s. 4).

Grundlagsutskottet har understrukit att det i åtskiljandet mellan behövligheten och nödvändigheten att få och lämna ut information vid sidan av informationsinnehållets omfång även handlar om att den rätt att få information som går före sekretessbestämmelserna i sista hand går ut på att den myndighet som har rätt att få information i och med sina egna behov åsidosätter de grunder och intressen som är skyddade med hjälp av sekretess som gäller den myndighet som innehar informationen (GrUU 15/2018 rd). Ju mer generella bestämmelserna om rätt till information är, desto större är risken att sådana intressen kan åsidosättas per automatik. Ju fullständigare bestämmelserna kopplar rätten till information till villkor i sak, desto mer sannolikt är det att en begäran om information måste motiveras. Också den som lämnar ut uppgifter har då möjlighet att bedöma om det finns lagliga förutsättningar för att lämna ut uppgifter. Genom att de facto vägra att lämna ut informationen kan den som innehar den göra att det uppstår ett läge där en utomstående myndighet måste undersöka skyldigheten att lämna ut information, det vill säga tolka bestämmelserna. Denna möjlighet är viktig då det gäller att anpassa tillgången till information och sekretessintressena till varandra (GrUU 17/2016 rd, s. 6).

I propositionen har hänsyn tagits till grundlagsutskottets utlåtanden om rätten till information. Bestämmelser om Transport- och kommunikationsverkets rätt att få information finns i 35 § i den föreslagna eIDAS-lagen, enligt vilken Transport- och kommunikationsverket har rätt att av andra myndigheter, tillhandahållare av en europeisk digital identitetsplånbok och plånbokens användare, förlitande parter, tillhandahållare av en betrodd tjänst och användare av tjänsten, organ för bedömning av överensstämmelse, certifierare, tillhandahållare av system för elektronisk identifiering och av dem som handlar för deras räkning få de uppgifter som är nödvändiga för att verket ska kunna utföra sina uppgifter enligt den föreslagna eIDAS-lag och eIDAS-förordningen samt bestämmelser som utfärdats med stöd av dem. Transport- och kommunikationsverkets rätt att få information gäller således endast de uppgifter som är nödvändiga för utförandet av verkets uppgifter. Elektroniska identifieringsmetoder, elektroniska betrodda tjänster och den europeiska digitala identitetsplånboken är viktiga tjänster i det digitala samhället, och de används för att behandla en mängd olika personuppgifter och skapa förtroende för elektroniska processer. Det är ytterst viktigt att de uppfyller de krav som i lagstiftningen ställs på dem och att man får aktuell information om tillhandahållandet av dem. Transport- och kommunikationsverket är tillsynsmyndighet i Finland i fråga om dessa tjänster och det är därför motiverat att verket trots sekretessbestämmelserna har möjlighet att få den information som behövs för skötseln av dess uppgifter. Den föreslagna regleringen anses till denna del vara förenlig med grundlagsutskottets utlåtandepraxis om rätten att få information.

12.4 Rättsskydd

Propositionen innehåller förslag som gäller undantag från förvaltningslagens förfarandebestämmelser samt besvärsförbud. Enligt 50 § i den föreslagna eIDAS-lagen ges inte något förvaltningsbeslut eller några anvisningar om hur man begär omprövning eller någon upplysning om besvärsförbud när identifieringsuppgifter för fysiska och juridiska personer enligt 3 och 5 § i denna lag utfärdas eller återkallas i enlighet med ansökan. Detsamma gäller tillhandahållandet av betrodda tjänster i den europeiska digitala identitetsplånboken samt avbrytande och upphörande av tillhandahållandet i enlighet med mottagarens ansökan. Enligt 13 § i den föreslagna lagen om e-legitimation ges inte något förvaltningsbeslut eller någon besvärсанvisning eller någon upplysning om besvärsförbud vid beviljande av rätten att få

tillgång till en e-legitimation och vid indragning av ett kvalificerat elektroniskt attributsintyg med stöd av 11 § 2 mom. i den lagen. Det är inte heller möjligt att söka ändring i eller begära omprövning av de ovannämnda besluten.

Enligt 21 § i grundlagen har var och en rätt att på behörigt sätt och utan ogrundat dröjsmål få sin sak behandlad av en domstol eller någon annan myndighet som är behörig enligt lag samt att få ett beslut som gäller hans eller hennes rättigheter och skyldigheter behandlat vid domstol eller något annat oavhängigt rättskipningsorgan. Behandlingens offentlighet samt rätten att bli hörd, att få ett motiverat beslut och att ansöka om ändring liksom de andra garantierna för en rättvis rättegång och en god förvaltning tryggas genom lag.

I fråga om tillhandahållande av betrodda tjänster har det inte ansetts vara fråga om en offentlig förvaltningsuppgift, utan om tillhandahållande av en tjänst som även någon annan än en myndighet kan tillhandahålla utan att det i lag föreskrivs separat om detta på det sätt som förutsätts i 124 § i grundlagen. Grundlagsutskottet har tidigare ansett att tillhandahållande av kvalificerade certifikat (vilket hör till betrodda tjänster) kan jämföras med ett identitetsbevis utfärdat av en myndighet, eftersom en signatur är ett lagstadgat villkor för en rättshandling och kan göras med en elektronisk signatur med ett kvalificerat certifikat (GrUU 2/2002 rd, s. 2–3). Senare har grundlagsutskottet i sin bedömning av regeringens proposition om autentiseringslagen konstaterat att karaktären av de affärsekonomiska tjänster som avses i lagförslaget till den grad har distanserat sig från karaktäristika som gäller för offentliga myndighetsuppdrag, att verksamheten inte längre kan betraktas som en offentlig förvaltningsuppgift trots att verktygen för stark elektronisk autentisering och certifiering har betydelse för parternas ställning i olika typer av rättshandlingar (GrUU 16/2009 rd, s. 2–3).

Bestämmelsen i 21 § i grundlagen hindrar inte att man genom lag föreskriver om mindre undantag från garantierna för en rättvis rättegång under förutsättning att undantagen i fråga inte ändrar rättsskyddsgarantiernas ställning som huvudregel eller äventyrar individens rättighet till en rättvis rättegång (RP 309/1993 rd, s. 78, GrUU 68/2014 rd, s. 2–3, GrUU 59/2014 rd, s. 2).

I propositionen gäller undantagen och besvärsförbuden i fråga om meddelande av beslut enligt förvaltningslagen situationer där en myndighet utför en åtgärd på begäran av en kund inom förvaltningen i enlighet med kundens begäran. När det gäller e-legitimationer är det fråga om att rätten till e-legitimation enligt propositionen uppkommer med stöd av lagen utan förvaltningsbeslut eller annat beslut när den handling som utgör grund för e-legitimationen utfärdas. Åtgärderna kan i viss mån anses påminna om faktiska förvaltningsåtgärder, eftersom inte alla dessa åtgärder betraktas som offentliga förvaltningsuppgifter. Om åtgärden av någon anledning inte är förenlig med förvaltningskundens vilja kan han eller hon begära att åtgärden återkallas, t.ex. begära att identifieringsuppgifter eller betrodda tjänster dras in eller att användningen av den europeiska digitala identitetsplånboken upphör helt och hållet. I de fall där en myndighet av en eller annan orsak inte kan handla i enlighet med kundens vilja ska ett förvaltningsbeslut ges, i vilket det även går att söka ändring antingen genom besvär eller genom begäran om omprövning. Den föreslagna regleringen kan därför inte anses äventyra individens rättsskydd.

Enligt 11 § i det tredje lagförslaget ger Myndigheten för digitalisering och befolkningsdata vid indragning av ett kvalificerat elektroniskt attributsintyg som utgör grund för en e-legitimation i situationer som avses i paragrafens 2 mom. inte något förvaltningsbeslut eller någon besvärshanvisning eller någon upplysning om besvärsförbud. I dessa situationer har polisen med stöd av 10 § 1 mom. dragit in rätten till e-legitimation. Syftet med regleringen är att klargöra och förenkla användarens rättsmedel genom att rikta in dem på det bakomliggande

förvaltningsbeslutet av en myndighet, inte på den tekniska indragningen av ett attributsintyg som följer av detta.

Av dessa orsaker anses det med tanke på rättsskyddet inte finnas något behov av vare sig ett beslut eller en möjlighet till ändringssökande i de ovannämnda situationerna. Den föreslagna regleringen kan således inte anses stå i strid med 21 § i grundlagen.

12.5 Påföljdsbestämmelser

12.5.1 Nationellt handlingsutrymme

Enligt artikel 16.1 i den reviderade eIDAS-förordningen ska medlemsstaterna fastställa bestämmelser om sanktioner som ska gälla vid överträdelser av förordningen. Sanktionerna ska vara effektiva, proportionella och avskräckande. Denna reglering begränsar dock inte tillämpningen av artikel 31 i NIS 2-direktivet, som innehåller bestämmelser om de allmänna aspekterna av tillsynen över efterlevnaden av det direktivet och genomförandet av det. Förordningen ger medlemsstaterna nationellt handlingsutrymme när det gäller hur sanktionerna ska genomföras i medlemsstaterna. Medlemsstaterna kan därför i princip själva bestämma om sanktionerna ska genomföras i form av administrativa påföljder eller straffrättsliga straff.

Det nationella handlingsutrymmet begränsas dock av artikel 16.2 i den reviderade eIDAS-förordningen, enligt vilken medlemsstaterna ska säkerställa att överträdelser av förordningen som begås av kvalificerade och icke-kvalificerade tillhandahållare av betrodda tjänster medför administrativa sanktionsavgifter. I förordningen specificeras inte vilken typ av överträdelse av skyldigheterna som kan leda till sanktionsavgift, men utgångspunkten för förordningen är att när det gäller tillhandahållare av betrodda tjänster ska varje överträdelse av skyldigheterna i förordningen förenas med en sanktionsavgift. Förordningen kan dock anses lämna ett nationellt handlingsutrymme genom att medlemsstaten ska fastställa vilka av skyldigheterna enligt förordningen som förenas med myndighetens behörighet att påföra en påföljdsavgift. Det föreslås att det nationella handlingsutrymme som i förordningen ges med avseende på sanktionsavgifter används så att grundlagens ramvillkor kan uppfyllas. En del av de skyldigheter som i förordningen åläggs tillhandahållare av betrodda tjänster har inte formulerats tillräckligt exakt eller kan innehålla kvalitativa eller öppna kriterier.

I artikel 16.2 i förordningen fastställs en miniminivå för maximibeloppen för de administrativa sanktionsavgifterna, och i fråga om dessa finns inget nationellt handlingsutrymme. Enligt artikel 16.2 a är den maximala administrativa sanktionsavgiften minst fem miljoner euro, om tillhandahållaren av betrodda tjänster är en fysisk person, och enligt artikel 16.2 b är den minst fem miljoner euro eller en procent av den totala globala årsomsättningen för det företag som tillhandahållaren av betrodda tjänster tillhörde under det räkenskapsår som föregick det år då överträdelsen inträffade, beroende på vilket som är högst, om tillhandahållaren av betrodda tjänster är en juridisk person. Maximibeloppet av påföljdsavgiften enligt 47 § i den föreslagna eIDAS-lagen motsvarar artikel 16 i förordningen.

12.5.2 Villkor som gäller administrativa påföljder

Enligt grundlagsutskottets praxis är påföljdsavgifter administrativa påföljder av sanktionskaraktär för en lagstridig gärning eller försummelse. Utskottet har i sak jämfört ekonomiska påföljder av straffkaraktär med straffrättsliga påföljder (GrUU 14/2013 rd, GrUU 17/2012 rd, GrUU 9/2012 rd).

I propositionen föreskrivs det om tillsynsåtgärder som föranleds av överträdelser av den reviderade eIDAS-förordningen, om påföljdsavgifter som kan påföras tillhandahållare av betrodda tjänster samt om vite, hot om avbrytande och hot om tvångsutförande, med vilka tillsynsmyndigheten kan effektivisera sitt tillsynsbeslut. Dessa påföljder är av betydelse för egendomsskyddet, som tryggas i grundlagens 15 § 1 mom., och näringsfriheten, som tryggas i grundlagens 18 §. När tillsynsåtgärder tillämpas på en tillhandahållare av betrodda tjänster eller på en tillhandahållare av den europeiska digitala identitetsplånboken innebär det bl.a. att tillsynsmyndigheten har rätt att uppmana aktören att rätta till sin lagstridiga verksamhet eller att avbryta tillhandahållandet av tjänsten. Vid allvarigare överträdelser av skyldigheterna enligt förordningen kan tillsynsmyndigheten också t.ex. återkalla statusen kvalificerad för en tillhandahållare av betrodda tjänster och den tjänst som denna tillhandahåller.

De sanktionsavgifter som påförs för överträdelser av förordningen innebär ett ingrepp i egendomsskyddet. De tillsynsåtgärder och det föreläggande av vite och hot om tvångsutförande som föreslås i propositionen ska betraktas som administrativa påföljder, och påföljdsavgiften i sin tur som en administrativ påföljd av straffkaraktär. Eftersom administrativa påföljdsavgifter i sak är jämförbara med straffrättsliga påföljder måste de uppfylla de förutsättningar som i lag gäller för sådana påföljder. Nedan följer en bedömning av de föreslagna bestämmelserna om påföljder, särskilt bestämmelserna om påföljdsavgifter med tanke på de villkor som i lagstiftningen ställs på administrativa påföljder.

Godtagbarhet. Målet med eIDAS-förordningen är att öka förtroendet för elektroniska transaktioner på den inre marknaden samt att öka effektiviteten hos offentliga och privata nättjänster, elektronisk affärsverksamhet och e-handel i unionen. Ett annat mål med den reviderade eIDAS-förordningen är att främja medborgarnas rätt till en digital identitet som står under deras egen kontroll och som innebär att de kan utöva sina rättigheter i den digitala miljön och delta i den digitala ekonomin. Dessa mål har åtminstone samband med den i grundlagen tryggade jämlikheten (6 §), skyddet för privatlivet (10 §) och garantierna för god förvaltning (21 §). Syftet med bestämmelserna om sanktioner är att se till att aktörerna uppfyller kraven i förordningen. I synnerhet bestämmelserna om påföljdsavgifter har en allmänt avhållande inverkan. De syftar också till att förhindra att åtgärder som redan har vidtagits i strid med kraven i förordningarna fortsätter eller upprepas och att eventuella negativa konsekvenser av åtgärderna kan uppstå för de grundläggande fri- och rättigheterna. De betrodda tjänsterna enligt förordningen kommer i framtiden sannolikt att få en starkare ställning inom olika samhällstjänster på EU-nivå. Bestämmelserna om påföljder kan således anses vara godtagbara med avseende på deras syfte.

Exakthet. Grundlagsutskottet har i sin praxis ansett att även om kravet på exakthet enligt den straffrättsliga legalitetsprincipen i grundlagens 8 § inte direkt gäller administrativa påföljder kan det allmänna kravet på exakthet ändå inte förbigås i ett sammanhang som detta (t.ex. GrUU 9/2018 rd, s. 3, GrUU 39/2017 rd, s. 3, GrUU 2/2017 rd, s. 5, GrUU 15/2016 rd, s. 5, GrUU 10/2016, s. 7 och GrUU 57/2010 rd, s. 2/II). Dessutom har utskottet i praktiken utvidgat sin praxis när det gäller bestämmelser om blankostraff till att även omfatta bestämmelser om administrativa påföljder. Enligt utskottets utlåtandepaxis ska de kedjor av bemyndiganden som blankobestämmelserna kräver vara exakt angivna, och de materiella bestämmelser som är ett villkor för straffbarhet formuleras med den exakthet som krävs av straffbestämmelser. Av det regelverk som bestämmelserna ingår i måste det framgå att brott mot dem är straffbart. Också i själva kriminaliseringsbestämmelsen måste det finnas en behörig beskrivning av den gärning som avses bli kriminaliserad (GrUU 21/2020 rd, s. 2 med hänvisningar).

I det första lagförslaget preciseras det för vilket brott mot bestämmelserna i den reviderade eIDAS-förordningen en påföljdsavgift kan påföras en tillhandahållare av betrodda tjänster.

Vidare ska de föreslagna paragraferna innehålla en saklig beskrivning av den gärning för vilken en påföljd ska påföras. I propositionen föreslås ingen möjlighet att påföra påföljdsavgift för sådana skyldigheter för tillhandahållare av betrodda tjänster enligt den reviderade eIDAS-förordningen som inte anges tillräckligt exakt i förordningen eller som innehåller kvalitativa eller öppna kriterier för förfarandet. Påföljdsavgift kan därför endast påföras för sådana skyldigheter för tillhandahållare av betrodda tjänster som anges tillräckligt exakt i den reviderade eIDAS-förordningen. Den föreslagna regleringen uppfyller således kriterierna för blankobestämmelser.

Eftersom påföljdsavgifterna kan vara betydande måste man enligt grundlagsutskottet fästa särskild uppmärksamhet vid kraven på rättssäkerhet (GrUU 14/2018 rd, s. 18). I 52 § i det första lagförslaget föreskrivs det om möjligheten för tillhandahållare av betrodda tjänster som påförts en påföljdsavgift att i den ordning som föreskrivs i lagen om rättegång i förvaltningsärenden söka ändring genom besvär i beslutet om påförande av påföljdsavgift, vilket säkerställer den betalningsskyldiges rättsskydd. Ett beslut om påföljdsavgift ska vara verkställbart först när det har vunnit laga kraft, vilket har bedömts trygga adekvata garantier för att rättssäkerheten blir tillbörligen tillgodosedd (GrUU 4/2004 rd, s. s. 7–8).

Proportionalitet. Enligt grundlagsutskottets etablerade praxis ska administrativa påföljder av sanktionskaraktär även uppfylla proportionalitetskraven (t.ex. GrUU 39/2017 rd, s. 3, GrUU 2/2017 rd, s. 5, GrUU 15/2016 rd, s. 5 och GrUU 28/2014 rd, s. 2/II). De bestämmelser som är relevanta för proportionaliteten gäller förutom sanktionernas storlek även de omständigheter som ska beaktas vid fastställandet av påföljdens storlek och avstående från påföljdsavgift (GrUU 12/2019 rd, s. 7). Utskottet har också i sin praxis förutsatt att myndighetens prövning vid beslut om att inte påföra påföljdsavgift ska vara bunden till prövning, det vill säga att avgiften inte ska påföras om de villkor som anges i bestämmelsen är uppfyllda (GrUU 46/2021 rd, punkt 17 med hänvisningar). I sina utlåtanden har grundlagsutskottet vid bedömningen av proportionaliteten av påföljdsavgifterna ansett det vara relevant huruvida avgifterna gäller en fysisk person (i fråga om förslaget till förordning om artificiell intelligens, se GrUU 37/2021 rd, GrUU 15/2016 rd, s. 5).

I den föreslagna lagen föreskrivs det om maximi- och minimibeloppet av påföljdsavgiften. I den reviderade eIDAS-förordningen fastställs på det ovan beskrivna sättet vad maximibeloppen av de administrativa sanktionsavgifterna minst ska vara, och i fråga om dessa finns inget nationellt handlingsutrymme. En fysisk person kan vara tillhandahållare av betrodda tjänster och emittera t.ex. elektroniska attributsintyg, varvid de påföljder som fastställs i lag kan tillämpas på honom eller henne på grundval av överträdelse av förordningen. Betrodda tjänster kan också tillhandahållas av privata näringsidkare, som är fysiska personer. I den föreslagna lagen fastställs ett annat minimibelopp av påföljdsavgiften för fysiska personer än för juridiska personer. Detta är motiverat eftersom de ekonomiska effekterna av påföljdsavgiften i allmänhet är relativt sett tyngre för en fysisk person.

Minimibeloppen av påföljdsavgifterna för både fysiska och juridiska personer är relativt låga jämfört med maximibeloppen. I vissa fall kan de maximala belopp som fastställs i den reviderade eIDAS-förordningen uppgå till minst miljontals euro. Syftet med att ha en hög miniminivå för den maximala påföljdsavgiften är att förebygga att överträdelser begås framför allt av stora och multinationella aktörer. Tillhandahållare av betrodda tjänster kan dock också vara mindre aktörer och fysiska personer. Med tanke på proportionaliteten är det motiverat att den behöriga myndigheten har utrymme för skönsmässig bedömning i fastställandet av påföljdsavgiften från fall till fall.

Enligt den föreslagna regleringen baserar sig påförandet av påföljdsavgift och påföljdsavgiftens belopp på en helhetsbedömning. I 47 § 1 mom. i det första lagförslaget finns en förteckning över de faktorer som den behöriga myndigheten ska beakta vid helhetsbedömningen. Bestämmelser om förutsättningarna för avstående från påföljdsavgift finns i 48 §. Transport- och kommunikationsverket har också lindrigare påföljder till sitt förfogande än påföljdsavgifter (anmärkning och tillsynsbeslut enligt 38 § och vite enligt 40 § i det första lagförslaget). Samtidigt kan Transport- och kommunikationsverket också använda påföljder som är strängare än påföljdsavgifter, t.ex. kräva att tillhandahållandet av betrodda tjänster upphör med stöd av den reviderade eIDAS-förordningen. På de ovannämnda grunderna kan de föreslagna bestämmelserna om påföljder anses vara proportionerliga.

Oskuldspresumtion och förbud mot dubbel straffbarhet. Propositionen är inte problematisk med avseende på oskuldspresumtionen, eftersom det inte föreskrivs om ett ansvar som är oberoende av vållande (GrUU 9/2018 rd, s. 4). I den föreslagna lagen ska en förutsättning för påförande av påföljdsavgift alltid vara att tillhandahållaren av betrodda tjänster har begått en överträdelse av den reviderade eIDAS-förordningen genom uppsåtlig eller vårdslös verksamhet.

Enligt förbudet mot dubbel straffbarhet, den s.k. ne bis in idem-regeln, får ingen lagföras eller straffas på nytt i en brottmålsrättegång i samma stat för ett brott för vilket han redan har blivit slutligt frikänd eller dömd i enlighet med lagen och rättegångsordningen i denna stat (GrUU 9/2012 rd, s. 3, GrUU 14/2013 rd, s. 2).

I artikel 4 i protokoll 7 till Europakonventionen fastställs ett förbud mot dubbel straffbarhet, enligt vilket ingen får rannsakas eller straffas på nytt genom brottmålsförfarande i samma stat för ett brott för vilket han eller hon redan blivit slutligt frikänd eller dömd i enlighet med lagen och rättegångsordningen i denna stat. Även i artikel 50 i EU:s stadga om de grundläggande rättigheterna föreskrivs det om rätten att inte bli dömd eller straffad två gånger för samma brott. Enligt unionens domstol är möjligheten till överlappande förfaranden och påföljder förenlig med det väsentliga innehållet i artikel 50 i stadgan om de grundläggande rättigheterna, under förutsättning att det i den nationella lagstiftningen inte är tillåtet att inleda förfaranden och påföra påföljder för samma gärningar på grundval av samma överträdelse eller för att uppnå samma mål utan endast föreskrivs att överlappande förfaranden och påföljder kan förekomma enligt olika regelverk.

I det första lagförslaget har förbudet mot dubbel straffbarhet beaktats i 48 § 2 mom. En administrativ påföljdsavgift får inte påföras den som misstänks för samma gärning i en förundersökning, en åtalsprövning eller ett brottmål som är anhängigt vid en domstol. Påföljdsavgift får inte heller påföras den som för samma gärning har meddelats en lagakraftvunnen dom.

I Europadomstolens avgörandep Praxis sträcker sig räckvidden av förbudet mot dubbel straffbarhet också till olika slag av administrativa påföljder av straffkaraktär (GrUU 9/2012 rd, s. 3). På grundval av EU-domstolens avgöranden utgör förbudet mot dubbel straffbarhet dock inte alltid ett hinder för olika myndigheter att på grundval av samma faktiska omständigheter påföra påföljdsavgifter med stöd av olika rättsakter. Två administrativa påföljdsavgifter på grundval av samma faktiska omständigheter har särskilt behandlats i EU-domstolens rättspraxis (målen C-117/20 bpost och C-151/20 Nordzucker). Avgörandena gäller konkurrensrätten, men de kan ha en vidare innebörd (se mål C-117/20 bpost, punkt 35). Det ska då i varje enskilt fall säkerställas att de förfaranden som myndigheterna inlett har flera kompletterande mål som avser andra aspekter av samma överträdelse (mål C-117/20 bpost, punkt 50). EU-domstolens avgöranden innehåller dock inga exakta krav för myndigheternas verksamhet. I praktiken har det haft betydelse om de överlappande påföljderna har varit förutsebara och om de båda

förfarandena har genomförts på ett sätt som är tillräckligt samordnat, samtidigt som förfarandena ligger nära varandra i tiden (mål C-117/20 bpost, punkterna 51 och 55; se också A och B v. Norge [GC], nr. 24130/11 och 29758/11, § 130, 15.11.2016). Olika sammantagna rättsliga reaktioner får dock inte utgöra en orimlig börda för den berörda personen (inklusive beaktande av den första påföljden när den andra påförs), och de samlade påföljderna ska stå i proportion till överträdelseernas allvar (mål C-117/20 bpost, punkterna 49 och 51).

Tillämpningen av förbudet mot dubbel straffbarhet ska övervägas med tanke på de administrativa påföljderna t.ex. när en aktör misstänks ha brutit mot eIDAS-förordningen, vars efterlevnad övervakas av Transport- och kommunikationsverket, och eventuellt även mot cybersäkerhetslagen och/eller mot bestämmelserna i den allmänna dataskyddsförordningen, vars efterlevnad övervakas av dataombudsmannen. eIDAS-förordningen begränsar inte tillämpningen av NIS 2-direktivet eller den allmänna dataskyddsförordningen. Syftet med bestämmelserna kan delvis överlappa varandra, och därför kan möjligheten till överlappande förfaranden enligt olika regelverk inte helt uteslutas.

I fråga om administrativa påföljder föreslås inte någon bestämmelse om förbud mot dubbel straffbarhet. På grundval av EU-domstolens ovan beskrivna avgöranden gäller förbudet mot dubbel straffbarhet inte nödvändigtvis alla påföljdsavgifter som påförs på grundval av samma faktiska omständigheter. En bestämmelse om dataombudsmannen är svår att formulera så att den blir täckande och kan leda till en felaktig slutsats om att någon annan än dataombudsmannen kan utöva tillsyn över efterlevnaden av den allmänna dataskyddsförordningen. Förbudet mot dubbel straffbarhet gäller som allmän rättsprincip, och det är inte nödvändigt att särskilt föreskriva om detta. Myndigheterna är skyldiga att samarbeta med varandra med stöd av EU-lagstiftningen och förvaltningslagen. I varje enskilt fall ska det genom myndighetssamarbete säkerställas att förbudet mot dubbel straffbarhet genomförs även i det administrativa påföljdsförfarandet.

Den föreslagna regleringen är därför inte problematisk med tanke på förbudet mot dubbel straffbarhet.

12.5.3 Påföljder som gäller myndigheter

Grundlagsutskottet har ansett att en utvidgning av bestämmelserna om påföljdsavgift till myndighetsverksamhet inte är problemfri i konstitutionellt hänseende (se GrUU 14/2018 rd, GrUU 13/2023 rd). I propositionen i fråga hänvisade utskottet till den etablerade ståndpunkten att en administrativ påföljdsavgift som påförs en myndighet är ett främmande förfarande utifrån vårt allmänna rättssystem. Myndigheterna är bundna av legalitetsprincipen i förvaltningen, och myndigheterna måste också iaktta allmänna förvaltningslagar. Till ställningen som tjänsteman hör ett tjänsteansvar för fel som begås i arbetet. Över en myndighets verksamhet kan också förvaltningsklagan anföras hos en högre myndighet. Myndigheternas verksamhet är budgetbunden och effekterna av en påföljd som avser ett penningbelopp är inte desamma som inom den privata sektorn. En myndighet ska i alla situationer sköta sina lagstadgade uppgifter (GrUU 14/2018 rd, s. 20). Under beredningen av den reviderade eIDAS-förordningen kunde man inte i förordningen införa en bestämmelse om att en medlemsstat nationellt kan föreskriva att påföljdsavgifter inte kan påföras en myndighet. Av denna anledning har det inte ansetts vara möjligt att i denna proposition föreskriva om ett undantag för myndigheter när det gäller påförande av påföljdsavgift.

Myndigheter tillhandahåller vanligtvis inte sådana betrodda tjänster eller kvalificerade betrodda tjänster som avses i eIDAS-förordningen. Exempelvis Myndigheten för digitalisering och befolkningsdata tillhandahåller dock certifikat och är i detta avseende en kvalificerad

tillhandahållare av betrodda tjänster. En utmaning med tanke på definitionen av tillhandahållare av betrodda tjänster kan anses vara att begreppet tillhandahållare av betrodda tjänster i eIDAS-förordningen avser en fysisk eller juridisk person som tillhandahåller en eller flera betrodda tjänster, antingen i egenskap av kvalificerad eller icke kvalificerad tillhandahållare av betrodda tjänster.

Även om det inte har ansetts vara problemfritt i konstitutionellt hänseende att utvidga bestämmelserna om påföljdsavgifter så att de även omfattar myndighetsverksamhet bör det dock noteras att justitieministeriet har inlett ett projekt för att införa administrativa påföljder för överträdelser av dataskyddslagstiftningen i den offentliga sektorn (<https://oikeusministerio.fi/sv/projekt?tunnus=OM127:00/2023>). Inom ramen för projektet bereds en regeringsproposition i syfte att göra behövliga lagändringar så att även myndigheter och organ inom den offentliga förvaltningen kan påföras en administrativ påföljdsavgift för överträdelser av dataskyddslagstiftningen. Propositionen har varit ute på remiss i slutet av 2025, och på webbsidorna för projektet har föredragningsveckan för propositionen uppskattats bli 15/2026.

12.6 Överföring av förvaltningsuppgifter på andra än myndigheter

Det första och andra lagförslaget i propositionen ska bedömas utifrån 124 § i grundlagen på grund av att de innehåller bestämmelser om aktörer som utför bedömningar av överensstämmelse och certifieringar samt om underleverantörer till organ för bedömning av överensstämmelse. Vidare föreslås det att det föreskrivs om Transport- och kommunikationsverkets möjlighet att i anslutning till sina uppgifter som ägare av den nationella certifieringsordningen för den europeiska digitala identitetsplånboken samt i anslutning till utseendet av ett organ för bedömning av överensstämmelse anförtro en biträdande uppgift till en underleverantör som har tillräckliga tekniska förutsättningar och tillräcklig kompetens för uppgiften och som uppfyller vad som föreskrivs i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den samt i den föreslagna eIDAS-lagen och föreskrifter som utfärdats med stöd av den.

I 124 § i grundlagen sägs det att offentliga förvaltningsuppgifter kan anförtros andra än myndigheter endast genom lag eller med stöd av lag, om det behövs för en ändamålsenlig skötsel av uppgifterna och det inte äventyrar de grundläggande fri- och rättigheterna, rättssäkerheten eller andra krav på god förvaltning. Uppgifter som innebär betydande utövning av offentlig makt får dock ges endast myndigheter.

När offentliga förvaltningsuppgifter anförtros andra än myndigheter måste kravet på ändamålsenlighet vara uppfyllt. Detta krav är ett juridiskt villkor och det måste bedömas från fall till fall huruvida kravet uppfylls i fråga om varje offentlig förvaltningsuppgift som föreslås bli skött utanför myndighetsorganisationen. Vid bedömningen av ändamålsenligheten ska man enligt förarbetena till grundlagen uppmärksamma dels förvaltningens effektivitet och övriga interna behov, dels enskilda personers och sammanslutningars behov (RP 1/1998 rd, s. 179). Grundlagsutskottet har i sin praxis ansett att det i vissa fall kan vara lämpligt att inspektioner på grund av särskilda yrkesmässiga och tekniska aspekter på de omständigheter som tillsynen gäller utförs av sakkunniga som myndigheterna befullmäktigat därtill (GrUU 40/2002 rd, s. 3). Enligt grundlagsutskottet kan nödvändighetskravet också uppfyllas t.ex. när granskningen förutsätter kompetens eller resurser som saknas hos myndigheterna (GrUU 29/2013 rd, s. 2).

I grundlagsutskottets praxis har det ansetts att tryggnad av kraven på rättssäkerhet och god förvaltning i den bemärkelse som avses i 124 § i grundlagen innebär att de allmänna förvaltningslagarna iaktas när ärenden behandlas och att de som handlägger ärenden handlar

under tjänsteansvar (GrUU 33/2004 rd, s. 7, GrUU 46/2002 rd, s. 9). Enligt grundlagsutskottet är det i allmänhet inte nödvändigt att på grund av 124 § i grundlagen hänvisa till de allmänna förvaltningslagarna, eftersom de allmänna förvaltningslagarna tillämpas med stöd av de i dem ingående bestämmelserna om tillämpningsområde, definition på myndighet eller enskildas skyldighet att ge språklig service också på enskilda när de utför ett offentligt förvaltningsuppdrag (GrUU 42/2005 rd, s. 3). Om man trots allt anser att t.ex. tydligheten kräver det, måste hänvisningen vara omfattande för att e contrario-tolkning ska undvikas (GrUU 11/2006 rd, s. 3, GrUU 42/2005 rd, s. 3). Grundlagsutskottet har dock förutsatt att det till lagförslaget i samband med skötseln av en offentlig förvaltningsuppgift fogas en bestämmelse om tjänsteansvar (GrUU 50/2017 rd, 3, GrUU 26/2017 rd, s. 49–50, GrUU 16/2016 rd, s. 2–3, GrUU 8/2014 rd, s. 5).

Enligt 124 § i grundlagen får uppgifter som innebär betydande utövning av offentlig makt dock ges endast myndigheter. Som betydande utövning av offentlig makt ska betraktas t.ex. på självständig prövning baserad rätt att använda maktmedel eller att på något annat konkret sätt ingripa i en enskild persons grundläggande fri- och rättigheter (RP 1/1998 rd, s. 180 och GrUU 28/2001 rd, s. 5–6, GrUU 5/2014 rd, s. 3).

Trots att Transport- och kommunikationsverket övervakar att de tjänster som tillhandahålls i enlighet med eIDAS-förordningen uppfyller de krav som ställs på dessa tjänster i eIDAS-förordningen, har den bedömning som ett organ för bedömning av överensstämmelse utför och den certifiering som en certifierare utför stor betydelse med tanke på tillhandahållandet av tjänsterna. De bedömningar som görs av dessa aktörer utgör grunden för den bedömning och tillsyn som Transport- och kommunikationsverket utför. Utan bedömning av överensstämmelse eller certifiering är det inte möjligt att tillhandahålla en europeisk digital identitetsplånbok eller att få kvalificerad status i fråga om betrodda tjänster. Följaktligen kan uppgiften för ett organ för bedömning av överensstämmelse och en certifierare samt uppgiften för ett godkänt bedömningsorgan för informationssäkerhet betraktas som en sådan offentlig förvaltningsuppgift som avses i 124 § i grundlagen. Också aktörer som sköter biträdande uppgifter för Transport- och kommunikationsverket och underleverantörer till ett organ för bedömning av överensstämmelse kan i praktiken anses delta i skötseln av offentliga förvaltningsuppgifter.

Det är med hänsyn till uppgiftens innehåll inte problematiskt med avseende på grundlagen att överföra uppgiften som certifierare, organ för bedömning av överensstämmelse eller underleverantör till ett sådant organ eller utförandet av biträdande uppgifter i anslutning till Transport- och kommunikationsverkets uppgifter på andra än myndigheter. Vid bedömning av överensstämmelse för och certifiering av tjänster enligt eIDAS-förordningen är det fråga om uppgifter som kräver mycket tekniska och djupgående specialkunskaper. Utförandet av uppgifterna är inte förknippat med befogenheter som måste anses som betydande utövande av offentlig makt. Uppgifterna i anslutning till bedömning av överensstämmelse och certifiering är bedömningsuppgifter som kräver teknisk specialkunskap, och grundlagsutskottet har i olika sammanhang ansett det vara ändamålsenligt med tanke på 124 § i grundlagen att skötseln av denna typ av uppgifter överförs på aktörer utanför myndighetsmaskineriet (t.ex. GrUU 43/2000 rd, GrUU 16/2002 rd och GrUU 180/2000 rd).

Autentiseringslagen innehåller fortsättningsvis en uttrycklig hänvisning till de allmänna förvaltningslagarna. Det föreslås att en allmän hänvisning till de allmänna förvaltningslagarna fogas till 31 § i den föreslagna eIDAS-lagen. Vidare konstateras det i 31 § i den föreslagna eIDAS-lagen att de i paragrafen avsedda aktörer som sköter en offentlig förvaltningsuppgift ska omfattas av offentlighetslagen också vid skötseln av andra offentliga förvaltningsuppgifter än utövande av offentlig makt. På den som sköter en biträdande uppgift vid Transport- och kommunikationsverket tillämpas vad som i offentlighetslagen föreskrivs om den som verkar på

uppdrag av en myndighet. I 32 § i den föreslagna eIDAS-lagen och 37 § i autentiseringslagen föreskrivs det om dessa aktörers straffrättsliga tjänsteansvar. I 51 § i den föreslagna eIDAS-lagen och 49 a § i autentiseringslagen föreskrivs det om begäran om omprövning av beslut som ges av organ för bedömning av överensstämmelse och certifierare.

Den föreslagna regleringen anses således inte strida mot 124 § i grundlagen.

12.7 Statliga skatter och avgifter

Bestämmelserna om avgifter till Transport- och kommunikationsverket i 41 § i det första lagförslaget och 47 § i det andra lagförslaget ska analyseras utifrån vad som i 81 § i grundlagen föreskrivs om statliga skatter och avgifter. Enligt 81 § 1 mom. i grundlagen föreskrivs det om statsskatt genom lag, och lagen ska innehålla bestämmelser om grunderna för skattskyldigheten och skattens storlek samt om de skattskyldigas rättsskydd. Av den lag som gäller en viss skatt ska entydigt också framgå skattskyldighetens omfattning. Lagbestämmelserna måste också vara såtillvida exakta att de lagtillämpande myndigheterna har bunden prövning när det gäller att bestämma skattens storlek.

För det första föreskrivs det om tillsynsavgifter i 47 § i den gällande autentiseringslagen, och det föreslås att en del av dessa nu flyttas till den nya eIDAS-lagen medan en del bevaras i autentiseringslagen. eIDAS-lagen föreslås dessutom innehålla en ny tillsynsavgift för tillhandahållare av plånböcker som motsvarar tillsynsavgiften för leverantörer av identifieringstjänster och tillhandahållare av betrodda tjänster. De avgifter som det föreskrivs om i 47 § i autentiseringslagen har enligt förarbetena till lagen betraktats som skatter snarare än avgifter (RP 74/2016 och RP 36/2009). Av denna anledning har bestämmelserna i 41 § i den föreslagna eIDAS-lagen till de delar paragrafen gäller tillsynsavgifter formulerats på motsvarande sätt som 47 § i autentiseringslagen så att det av dem framgår åtminstone grunderna för skattskyldigheten och skattens storlek, de skattskyldigas rättsskydd och de skattskyldigas krets på det sätt som förutsatts i 81 § i grundlagen. Det föreslås att de tillsynsavgifter som ingår i autentiseringslagen och i den föreslagna eIDAS-lagen höjs till följd av den allmänna höjningen av kostnadsnivån. De föreslagna bestämmelserna om tillsynsavgifter strider således inte mot 81 § i grundlagen.

För det andra föreslås vissa av de behandlingsavgifter som Transport- och kommunikationsverket tar ut bli upphävda i autentiseringslagen. I 47 § i den gällande autentiseringslagen används benämningarna registreringsavgift och utnämningsavgift för dessa. I fortsättningen ska leverantörer av identifieringstjänster och tillhandahållare av betrodda tjänster betala en avgift för behandling av anmälan om inledande av tillhandahållandet av tjänsten, vars storlek fastställs i förordningen om avgifter för elektronisk kommunikation. På motsvarande sätt ska storleken på ansökningsavgifterna för organ för bedömning av överensstämmelse och utsedda certifieringsorgan (certifierare enligt den föreslagna eIDAS-lagen), som för närvarande ingår i autentiseringslagen, i fortsättningen fastställas på förordningsnivå. Som en del av genomförandet av eIDAS-lagen kommer det också att tas ut en avgift för behandling av anmälan innan tillhandahållandet av den europeiska digitala identitetsplånboken inleds, och avgiftens storlek fastställs enligt samma förordning om avgifter för elektronisk kommunikation.

En betalnings konstitutionella karaktär inverkar på de krav som grundlagen ställer på sättet att reglera betalningen. Om statsskatter bestäms genom lag som ska innehålla bestämmelser om grunder för skattskyldigheten och skattens storlek samt om de skattskyldigas rättsskydd, medan bestämmelser om avgifter samt de allmänna grunderna för storleken på avgifter för de statliga myndigheternas tjänsteåtgärder, tjänster och övriga verksamhet utfärdas genom lag. Kraven på

en skattelag innebär framför allt att det av lagen helt entydigt ska framgå vad skattskyldigheten omfattar och att bestämmelserna i lagen också ska vara såtillvida exakt utformade att den prövningsrätt som de tillämpande myndigheterna har när det gäller att bestämma skattens storlek ska vara bunden till sin natur (RP 1/1998 rd, s. 134–135) (GrUU 61/2002 rd, s. 5/II).

Enligt grundlagsutskottets vedertagna praxis är det utmärkande för konstitutionella avgifter att de utgör ersättningar eller vederlag för service som tillhandahålls av det allmänna. Övriga penningprestationer till staten är däremot skatter i konstitutionell mening (RP 1/1998 rd, s. 134–135; GrUU 61/2002 rd, s. 5/II, GrUU 66/2002 rd, s. 3/II, GrUU 67/2002 rd, s. 3/II). Den väsentliga skillnaden mellan skatter och avgifter har därmed att göra med motprestationer. Om det inte finns någon motprestation är betalningen i konstitutionell mening en skatt. (GrUU 61/2002 rd, s. 5/II).

Frågan om det finns ett motprestationsförhållande eller inte bör bedömas med hänsyn till en rad olika aspekter. De prestationer som det tas ut avgifter för bör gå att specificera på något vis. Enligt grundlagen (RP 1/1998 rd, s. 135/I) ska det genom lag utfärdas allmänna bestämmelser om vilka tjänsteåtgärder, tjänster och varor som kan avgiftsbeläggas eller om vilka typer av prestationer som är avgiftsfria. Genom lag ska likaså utfärdas bestämmelser om de principer som ska iakttas. Om det däremot allmänt tas ut ett penningbelopp för finansiering av någon verksamhet är det snarare frågan om en konstitutionell skatt än en avgift. Det oaktat är full kostnadsmotsvarighet inte villkoret för att en penningprestation skall betraktas som avgift. Avgiftens storlek och grunderna för bestämning av avgiften ska i alla fall ha kvar något slag av samband med kostnaderna för prestationen. Ju större skillnaden mellan en avgift och kostnaderna för en prestation inte minst i samband med en offentlighetsrättslig uppgift är, desto närmare ligger det till hands att betrakta prestationen som en konstitutionell skatt (GrUU 53/2002 rd, s. 2/II). Det spelar också en viss roll om det är frivilligt eller obligatoriskt att ta emot prestationen. Det talar för en skatt om det inte går att tacka nej till prestationer som någon är skyldig att tillhandahålla och skyldigheten direkt med stöd av lag gäller rättssubjekt som uppfyller vissa rekvisit (GrUU 48/2010 rd, s. 8/I, GrUU 12/2005 rd, s. 3/I och GrUU 46/2004 rd, s. 3/I). Att en penningprestation möjligen har ett begränsat syfte spelar ingen roll vid bedömningen av prestationens konstitutionella natur (GrUU 46/2004 rd, s. 3/I, GrUU 61/2002 rd, s. 6/I).

Till exempel kunde den ansökningsavgift för teleföretag som ingick i kommunikationsmarknadslagen (393/2003) och som skulle betalas till Kommunikationsverket (nuvarande Transport- och kommunikationsverket) tydligt betraktas som en avgift ur konstitutionell synvinkel, eftersom det av förslaget till lagstiftningen i fråga utöver avgiftens storlek klart framgick för vilka myndighetsåtgärder avgiften betalas. Däremot är en tillsynsavgift, som uppkommer direkt med stöd av lag, inte ett vederlag för specificerbara prestationer och grunderna för hur avgiften bestäms har inget samband med kostnaderna för prestationer av detta slag. Därför är tillsynsavgiften enligt utskottets sätt att se en skatt i konstitutionellt hänseende (GrUU 61/2002 rd, s. 6/II). Det föreslås att de tillsynsavgifter som ingår i de aktuella första och andra lagförslagen fortfarande regleras på lagnivå, medan det för behandling av en anmälan eller ansökan tas ut en avgift enligt lagen om grunderna för avgifter till staten vars storlek fastställs i förordningen om avgifter för elektronisk kommunikation.

Vid bedömningen av motprestationsförhållandet i fråga om betalningar som ska betraktas som avgifter ska det i fortsättningen med hänsyn till grundlagsutskottets praxis fästas uppmärksamhet vid bl.a. om betalningen går att specificera, om den motsvarar kostnaderna och om den är frivillig eller obligatorisk. Ur konstitutionell synvinkel är det motiverat att betrakta behandlingsavgifter som avgifter i stället för skatt, särskilt på grund av att verksamheten och marknaden för stark autentisering och elektroniska betrodda tjänster har etablerat sig. När

autentiseringslagen stiftades 2009 var marknaden för identifieringstjänster och betrodda tjänster fortfarande under utveckling. Vid den tidpunkten var kostnaderna för behandlingen av anmälningar och registreringen av aktörer inte kända för Kommunikationsverket, som också var tillsynsmyndighet. Eftersom det var fråga om en ny verksamhet och det inte fanns någon kostnads motsvarighetsbedömning att uppge för kostnaderna, ansågs registreringsavgifterna utgöra avgifter av skattenatur. Det är uppenbart att även utbudet på identifieringstjänster och betrodda tjänster fortsätter att utvecklas i takt med att digitaliseringen framskrider och tjänsterna i samhället i allt högre grad blir elektroniska, men under flera år har det inte skett några större förändringar i t.ex. antalet tjänsteleverantörer.

I fortsättningen fastställs storleken på avgiften för behandling av en anmälan eller ansökan utifrån den tid som vid Transport- och Kommunikationsverket har gått åt till att behandla anmälan eller ansökan. Behandlingstiden för anmälan eller ansökan kan verifieras och specificeras i detalj. På så sätt är det möjligt att ta ut avgiften enligt en självkostnads kalkyl, varvid kraven på att betalningen går att specificera och motsvarar kostnaderna uppfylls.

Skyldigheten att betala en avgift för behandling av anmälan uppkommer inte direkt med stöd av lag, utan avgiften tas ut endast i de fall då tjänsteleverantören antingen vill anmäla sig till det offentliga register som Transport- och Kommunikationsverket för över de leverantörer av identifieringstjänster som gjort anmälan och de tjänster som tillhandahålls av dem eller gör en anmälan enligt artikel 21 i eIDAS-förordningen. Som vederlag för avgiften kontrollerar Transport- och Kommunikationsverket att det i anmälan har lagts fram en tillräcklig utredning om att de krav som ställs på tjänsten och tjänsteleverantören uppfylls och för in tjänsteleverantören i det offentliga registret. I praktiken får tjänsteleverantören status som kvalificerad tjänsteleverantör i och med att tjänsteleverantören införs i registret, och tjänsteanvändarna kan kontrollera statusen som kvalificerad i det offentliga registret. På motsvarande sätt gäller ansökningsavgifterna för organ för bedömning av överensstämmelse och för certifierare situationer där aktören genom sin ansökan strävar efter att uppnå en viss status, dvs. möjligheten att verka som ett sådant bedömningsorgan eller en sådan certifierare som avses i lagen. Eftersom det rör sig om en bedömning av en aktör som sker på tjänsteleverantörens initiativ är det fråga om en prestation som kan jämföras med tjänsteleverantörens ansökan, varvid prestationen klart kan specificeras.

Det enda undantaget från frivillig betalning är Myndigheten för digitalisering och befolkningsdata, som enligt det första lagförslaget får i uppdrag att tillhandahålla en europeisk digital identitetsplånbok. Vilka uppgifter Myndigheten för digitalisering och befolkningsdata har i egenskap av statligt ämbetsverk regleras i lag. Därför fastställs också betalningsskyldigheten för den avgift som tas ut för behandlingen av anmälan direkt med stöd av lag. Den avgift som tas ut för behandling av plånbokstillhandahållares anmälan kan dock anses vara motiverad med tanke på marknadens funktion och de likvärdiga konkurrensvillkoren. Lagen hindrar inte andra tjänsteleverantörer från att anmäla sig som tillhandahållare av plånböcker. I praktiken kan även plånböcker som erbjuds av privata aktörer komma in på marknaden i framtiden. Syftet med regleringen är att skapa en permanent ram där även privata tjänsteleverantörer eller andra organisationer kan tillhandahålla europeiska digitala identitetsplånböcker. Om en avgift tas ut för behandlingen av anmälningar om identifieringstjänster och betrodda tjänster men inte för anmälningar om tillhandahållande av en plånbok kan detta snedvrider marknaden och skapa en oproportionerlig konkurrensfördel för dem som tillhandahåller plånböcker.

För att en betalning ska kunna betraktas som avgift, ska det av lag framgå vilka tjänsteåtgärder, tjänster och varor som kan avgiftsbeläggas eller vilka typer av prestationer som är avgiftsfria (GrUU 12/2005 rd, s.3/I). Bestämmelser om de allmänna grunderna för när statens prestationer

ska vara avgiftsbelagda och för storleken av avgifterna finns nuförtiden i lagen om grunderna för avgifter till staten. Lagen är av allmän karaktär och dess bestämmelser kan också tillämpas på avgifter för behandling av anmälningar och ansökningar av det slag som den aktuella propositionen gäller.

Grundlagsutskottet har i en situation där det har ansetts vara fråga om en avgift i stället för en skatt sett det som nödvändigt att statsrådet bevakar iakttagandet av avgifternas kostnadsmotsvarighetsnivå (GrUU 12/2005 rd, s. 3/II). Förslaget om att fastställa storleken på avgiften för behandling av anmälningar och ansökningar på förordningsnivå stöder även i framtiden bedömningen av avgiftens kostnadsmotsvarighet oftare än vad som skulle vara möjligt om avgiftens storlek fastställs på lagnivå. Kommunikationsministeriet och Transport- och kommunikationsverket bevakar avgifternas kostnadsmotsvarighet, och eventuella ändringar i avgifterna kan beaktas i samband med att förordningen om avgifter för elektronisk kommunikation uppdateras.

Med stöd av vad som anförts ovan anses det vara möjligt att för behandlingen av de anmälningar och ansökningar som Transport- och kommunikationsverket tar emot ta ut en behandlingsavgift, vars belopp i euro kan bestämmas genom förordningen om avgifter för elektronisk kommunikation. Däremot fastställs tillsynsavgifterna för leverantörer av identifieringstjänster och tillhandahållare av betrodda tjänster, tillhandahållare av plånböcker, organ för bedömning av överensstämmelse och certifierare fortsättningsvis på lagnivå. I regleringen av dessa avgifter beaktas på det sätt som beskrivits ovan de särskilda krav som gäller för bestämmelser om skatter.

12.8 Bemyndiganden att utfärda föreskrifter

Propositionen innehåller flera förslag om bemyndiganden för Transport- och kommunikationsverket att utfärda föreskrifter. Det är huvudsakligen fråga om att bevara befintliga bemyndiganden att utfärda föreskrifter så att en del av dem flyttas från autentiseringslagen till den föreslagna nya eIDAS-lagen. Dessutom föreslås ett antal nya bemyndiganden för Transport- och kommunikationsverket att utfärda föreskrifter. En sammanfattning av de föreslagna normgivningsbemyndigandena finns i avsnitt 8.2.

Enligt 80 § 2 mom. i grundlagen kan även andra myndigheter genom lag bemyndigas att utfärda rättsnormer i bestämda frågor, om det med hänsyn till föremålet för regleringen finns särskilda skäl och regleringens betydelse i sak inte kräver att den sker genom lag eller förordning. Tillämpningsområdet för ett sådant bemyndigande ska vara exakt avgränsat. Med andra ord ska det definieras noggrant i lag vad bemyndigandet omfattar. Enligt 80 § 1 mom. i grundlagen ska det dock genom lag utfärdas bestämmelser om grunderna för individens rättigheter och skyldigheter samt om frågor som enligt grundlagen i övrigt hör till området för lag.

Bestämmelsen i 80 § 2 mom. i grundlagen förutsätter särskilda skäl i anknytning till ett bemyndigande att utfärda föreskrifter. Enligt grundlagspropositionen (RP 1/1998 rd, s. 134/I) kan ett särskilt skäl anses föreligga närmast när det är fråga om en sådan teknisk reglering av smärre detaljer som inte inbegriper prövningsrätt i någon större utsträckning. Grundlagsutskottet har dessutom ansett att de särskilda yrkesmässiga särdragen hos den reglerande verksamheten är sådana särskilda skäl som avses i 80 § 2 mom. i grundlagen (GrUU 17/2004 rd, s. 3, GrUU 16/2003 rd, s. 3, GrUU 24/2002 rd, s. 3).

Grundlagsutskottet har inte ansett att ett bemyndigande om tekniska detaljer är problematiskt med tanke på grundlagen (GrUU 17/2004 rd, s. 3–4, GrUU 16/2003 rd, s. 3). Jämfört med befogenheten att utfärda förordning är befogenheter att utfärda föreskrifter kopplade till ett

allmänt krav på exakt avgränsning som går ännu längre och som betyder att de behöriga frågorna måste preciseras exakt genom lag (RP 1/1998 rd, s. 134, GrUU 43/2000 rd, s. 3/II och GrUU 46/2001 rd, s. 2-3). Exempelvis i utlåtandet GrUU 10/2014 rd (s. 2-3) betonas kraven på exakthet och noggrann avgränsning. I samma utlåtande konstaterar grundlagsutskottet att det är typiskt för miljölagstiftningen att en betydande del av den detaljerade regleringen ingår i författningar på lägre nivå än lag. Det beror enligt utskottet i stor utsträckning på att bestämmelserna behöver vara synnerligen detaljerade och av teknisk karaktär. Detta gäller även den lagstiftning om gränsöverskridande elektronisk identifiering, elektroniska betrodda tjänster och europeisk digital identitet som nu föreslås. Grundlagsutskottet har dessutom i ett utlåtande ansett att t.ex. Kommunikationsverket (nuvarande Transport- och kommunikationsverket) är en myndighet som kan ges rätt att meddela föreskrifter (bl.a. GrUU 9/2004 rd, s. 8).

Transport- och kommunikationsverket kan med stöd av den föreslagna eIDAS-lagen utfärda föreskrifter om specificerade och lagstadgade kriterier för bedömning av överensstämmelse, certifieringsförfaranden och andra krav på kvalifikation samt tekniska detaljer i samband med anmälan av vissa särskilda uppgifter samt harmoniseringen av dessa med kommissionens genomförandeakter. I propositionen har man tagit hänsyn till det krav som ställs i grundlagen genom att på ett uttömmande och exakt sätt specificera branschspecifika tekniska aspekter, om vilka Transport- och kommunikationsverket kan utfärda närmare föreskrifter. De bemyndiganden att utfärda föreskrifter som ingår i propositionen är noggrant avgränsade och exakta, och de gäller detaljer som är mindre betydande med tanke på regleringen som helhet. Bemyndigandet att utfärda föreskrifter om tekniska aspekter gör det möjligt att ta hänsyn till branschens särdrag och samordna lagstiftningen med kommissionens genomförandeakter som antagits och kommer att antas med stöd av eIDAS-förordningen. Det är fråga om sådana särskilda skäl som avses i 80 § 2 mom. i grundlagen. De normgivningsbemyndiganden som det föreskrivs om i eIDAS-lagen anses vara förenliga med de ovan beskrivna ramvillkoren och med 80 § i grundlagen.

Dessutom föreslås det att det till autentiseringslagen fogas ett nytt bemyndigande för Transport- och kommunikationsverket att utfärda föreskrifter om de behövliga uppgifter som ska registreras om den inledande identifieringen av sökanden och om de handlingar eller om den elektroniska identifiering som används i den inledande identifieringen. Bemyndigandet är sakligt anknutet till den paragraf som berör de frågor som regleras (24 § 2 mom. i autentiseringslagen). Normgivningsbemyndigandet innefattar ingen betydande prövning, och det innehåller inte heller bemyndiganden om frågor om vilka det ska föreskrivas genom lag. Det är fråga om en teknisk reglering som syftar till att precisera den på lagnivå fastställda skyldigheten att registrera den information som krävs om inledande identifiering av en person som ansöker om ett identifieringsverktyg och om den handling eller elektroniska identifiering som används för detta. Det är i praktiken fråga om en mycket detaljerad definition av den information som ska registreras. Transport- och kommunikationsverket kan anses ha särskild och etablerad sakkunskap om detta. Verket har länge varit den myndighet som utövar tillsyn över efterlevnaden av autentiseringslagen och har meddelat föreskrifter om andra tekniska frågor som det föreskrivs om i lagen. Följaktligen är bemyndigandet noggrant avgränsat i fråga om tillämpningsperioden. Det nya normgivningsbemyndigande som det föreskrivs om i autentiseringslagen anses vara förenliga med de ovan beskrivna ramvillkoren och med 80 § i grundlagen.

På de grunder som anges ovan kan lagförslagen behandlas i vanlig lagstiftningsordning. Propositionen innehåller dock ett förslag om att påföljdsavgift också kan påföras den myndighet som tillhandahåller betrodda tjänster. Regeringen anser det önskvärt att grundlagsutskottet ger ett utlåtande i frågan.

Kläm

Eftersom den reviderade eIDAS-förordningen innehåller bestämmelser som föreslås bli kompletterade genom lag, föreläggs riksdagen följande lagförslag:

1.

Lag

om vissa tjänster som möjliggör gränsöverskridande e-tjänster

I enlighet med riksdagens beslut föreskrivs:

1 kap.

Allmänna bestämmelser

1 §

Tillämpningsområde

I denna lag föreskrivs det om tillsynen över efterlevnaden av bestämmelserna i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, nedan *eIDAS-förordningen*, sådan den lyder senast ändrad genom förordning (EU) 2024/1183, och utfärdas det bestämmelser som kompletterar förordningen.

Denna lag tillämpas endast på europeiska digitala identitetsplånböcker som tillhandahålls i Finland.

På gränsöverskridande system för elektronisk identifiering som i enlighet med artikel 9 i eIDAS-förordningen ska anmälas till Europeiska kommissionen tillämpas lagen om stark autentisering (617/2009), om inte något annat följer av denna lag eller eIDAS-förordningen.

2 §

Definitioner

I denna lag avses med

1) *europeisk digital identitetsplånbok* en sådan europeisk digital identitetsplånbok som avses i artikel 3.42 i eIDAS-förordningen,

2) *identifieringsuppgifter för personer* sådana uppgifter för personidentifiering som avses i artikel 3.3 i eIDAS-förordningen,

3) *förlitande part* en sådan förlitande part som avses i artikel 3.6 i eIDAS-förordningen,

4) *nationell nod* en förbindelsepunkt som utgör en del av den interoperativa arkitekturen för elektronisk identifiering och som medverkar vid gränsöverskridande autentisering av personer och som har förmågan att känna igen och behandla eller vidarebefordra överföringar till andra noder genom att bringa den nationella elektroniska identifieringsinfrastrukturen i en medlemsstat i kontakt med nationella elektroniska identifieringsinfrastrukturer i andra medlemsstater,

5) *organ för bedömning av överensstämmelse* ett sådant organ för bedömning av överensstämmelse som avses i artikel 3.18 i eIDAS-förordningen och ett sådant certifieringsorgan som avses i bestämmelser som utfärdats med stöd av artikel 5c i den förordningen,

6) *teknisk utrustning* en mobil terminal eller annan motsvarande utrustning som användaren av den europeiska digitala identitetsplånboken innehar och i vilken plånboken har tagits i bruk.

2 kap.

Europeisk digital identitetsplånbok och medel för elektronisk identifiering

3 §

Utfärdande av identifieringsuppgifter för fysiska personer

Identifieringsuppgifter för fysiska personer för europeiska digitala identitetsplånböcker utfärdas av Myndigheten för digitalisering och befolkningsdata med iakttagande av artikel 5a i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den.

Utöver vad som föreskrivs i 1 mom. kan en person ansöka om identifieringsuppgifter för en fysisk person genom att sköta ärendet vid en finsk beskickning eller Statens ämbetsverk på Åland. Sökandens identitet ska kontrolleras med iakttagande av de krav på styrkande och kontroll av identitet på tillitsnivån hög som avses i artikel 8 i eIDAS-förordningen. Den finska beskickningen och Statens ämbetsverk på Åland registrerar de uppgifter som beskickningen eller ämbetsverket tagit emot av sökanden och andra uppgifter om behandlingen av ärendet i det informationssystem som Myndigheten för digitalisering och befolkningsdata använder vid utfärdandet av identifieringsuppgifter för fysiska personer och svarar för att de registrerade uppgifterna är tillförlitliga och korrekta.

Myndigheten för digitalisering och befolkningsdata ska utfärda identifieringsuppgifter för fysiska personer för sådana europeiska digitala identitetsplånböcker som Transport- och kommunikationsverket har anmält till Europeiska kommissionen i enlighet med 33 § 2 punkten. Myndigheten för digitalisering och befolkningsdata får utfärda identifieringsuppgifter för fysiska personer också för andra plånböcker. Myndigheten för digitalisering och befolkningsdata ska göra allmänt tillgänglig en förteckning över alla europeiska digitala identitetsplånböcker som tillhandahålls i enlighet med eIDAS-förordningen och för vilka myndigheten utfärdar identifieringsuppgifter för fysiska personer.

4 §

Registret över identifieringsuppgifter för fysiska personer

Myndigheten för digitalisering och befolkningsdata för ett register över de identifieringsuppgifter för fysiska personer som myndigheten har utfärdat. I registret införs de uppgifter som behövs för utfärdande, giltighet, uppdatering och återkallande av identifieringsuppgifter för fysiska personer med iakttagande av artikel 5a i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den.

De uppgifter som förts in i registret över identifieringsuppgifter för fysiska personer bevaras i fem år efter det att identifieringsuppgifterna för en fysisk person har upphört att gälla.

5 §

Utfärdande av identifieringsuppgifter för juridiska personer

Patent- och registerstyrelsen har rätt att utfärda identifieringsuppgifter för juridiska personer för europeiska digitala identitetsplånböcker.

Identifieringsuppgifterna för juridiska personer beviljas på ansökan och kan tillhandahållas endast juridiska personer som är registrerade i handelsregistret, med undantag för ideella föreningar och stiftelser.

Patent- och registerstyrelsen ska göra allmänt tillgänglig en förteckning över alla europeiska digitala identitetsplånböcker som tillhandahålls i enlighet med eIDAS-förordningen och för vilka Patent- och registerstyrelsen utfärdar identifieringsuppgifter för juridiska personer.

Patent- och registerstyrelsen får lämna ut personuppgifter om fysiska personer som framgår av en ansökan som avses i 2 mom. till andra än företrädare för den juridiska personen med iakttagande av vad som i 2 § 2 mom. i handelsregisterlagen (564/2023) föreskrivs om utlämnande av en i handelsregistret införd personbetecknings slutled och en utomlands bosatt fysisk persons hemadress.

6 §

Registret över identifieringsuppgifter för juridiska personer

Patent- och registerstyrelsen för register över de identifieringsuppgifter för juridiska personer som den har utfärdat. I registret införs de uppgifter som behövs för utfärdande, giltighet, uppdatering och återkallande av identifieringsuppgifter för juridiska personer med iakttagande av artikel 5a i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den.

De uppgifter som förts in i registret över identifieringsuppgifter för juridiska personer bevaras i fem år efter det att identifieringsuppgifterna för en juridisk person har upphört att gälla.

7 §

Tillhandahållande av europeiska digitala identitetsplånböcker

Myndigheten för digitalisering och befolkningsdata har till uppgift att tillhandahålla europeiska digitala identitetsplånböcker i Finland med iakttagande av artikel 5a i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den.

Bestämmelserna i 1 mom. begränsar inte andra myndigheters eller juridiska eller fysiska personers möjligheter att tillhandahålla europeiska digitala identitetsplånböcker i Finland.

En tillhandahållare av en europeisk digital identitetsplånbok ska innan den börjar tillhandahålla plånboken göra en anmälan till Transport- och kommunikationsverket. Anmälan ska innehålla de uppgifter som avses i artiklarna 5a.18 b och 5d i eIDAS-förordningen samt i de bestämmelser som utfärdats med stöd av dem.

Tillhandahållaren av en europeisk digital identitetsplånbok ska utan dröjsmål underrätta Transport- och kommunikationsverket om ändringar i de uppgifter som avses i 3 mom. Transport- och kommunikationsverket får utfärda närmare föreskrifter om hur de uppgifter som avses i 3 mom. ska lämnas.

8 §

Personuppgiftsansvarig för den europeiska digitala identitetsplånbok som Myndigheten för digitalisering och befolkningsdata tillhandahåller

Myndigheten för digitalisering och befolkningsdata är personuppgiftsansvarig för den europeiska digitala identitetsplånbok som myndigheten tillhandahåller med stöd av 7 § och för behandlingen av personuppgifter i samband med tillhandahållandet av plånboken.

9 §

Bevaringstid för information om tillhandahållande av europeiska digitala identitetsplånböcker

Tillhandahållare av en europeisk digital identitetsplånbok ska bevara informationen om plånboken och informationen i anslutning till tillhandahållandet av den i fem år från det att plånboken upphörde att gälla.

Information om transaktioner som genomförts genom en europeisk digital identitetsplånbok med förlitande parter och andra plånböcker ska finnas tillgänglig i två år från ingången av kalenderåret efter den tidpunkt då informationen registrerades.

10 §

Ibruktagande av en europeisk digital identitetsplånbok för en minderårig

En europeisk digital identitetsplånbok kan tas i bruk självständigt av den som fyllt tretton år. Den som är yngre än detta kan ta i bruk en plånbok med vårdnadshavarens samtycke.

11 §

Utlämnande av källkoder för europeiska digitala identitetsplånböcker

Bestämmelser om öppenheten hos källkoder för komponenter i europeiska digitala identitetsplånböcker finns i artikel 5a.3 i eIDAS-förordningen.

En tillhandahållare av en europeisk digital identitetsplånbok behöver inte lämna ut en källkod för en plånboks komponenter som inte har installerats på den tekniska utrustningen för en användare av den europeiska digitala identitetsplånboken, om det föreligger vederbörligen motiverade skäl för detta.

12 §

Avgifter för kvalificerade elektroniska underskrifter i europeiska digitala identitetsplånböcker

En tillhandahållare av en europeisk digital identitetsplånbok eller en kvalificerad tillhandahållare av en betrodd tjänst som gör det möjligt att skapa en kvalificerad elektronisk underskrift med en europeisk digital identitetsplånbok får ta ut en avgift för en elektronisk underskrift med plånboken när tillhandahållaren på ett tillförlitligt sätt kan verifiera att användaren av plånboken är kopplad till en organisation eller att underskriften är kopplad till ett yrkesmässigt ändamål.

13 §

Skyldigheter för tillhandahållare av europeiska digitala identitetsplånböcker i situationer med säkerhetsincidenter

Tillhandahållaren av en europeisk digital identitetsplånbok svarar i fråga om den plånbok som denne tillhandahåller för att medlemsstatens skyldigheter enligt artikel 5e i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den artikeln fullgörs.

Om en tillhandahållare av en europeisk digital identitetsplånbok av tekniska skäl inte själv kan fullgöra medlemsstatens skyldighet enligt artikel 5e i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den artikeln att anmäla vissa uppgifter, görs anmälan av Transport- och kommunikationsverket. Tillhandahållaren av en europeisk digital identitetsplånbok ska utan obefogat dröjsmål lämna Transport- och kommunikationsverket de uppgifter som behövs för anmälan enligt artikel 5e i eIDAS-förordningen.

14 §

Skyldigheter för användare av europeiska digitala identitetsplånböcker

Användaren av en europeisk digital identitetsplånbok ska använda plånboken omsorgsfullt och får inte överlåta den för att användas av någon annan. Användarens skyldighet börjar när denne har tagit i bruk plånboken.

Användaren av en europeisk digital identitetsplånbok ska utan obefogat dröjsmål göra en anmälan till tillhandahållaren av plånboken om att den tekniska utrustningen obehörigen har kommit i någon annans besittning eller om obehörig användning av plånboken.

15 §

Användarens ansvar för obehörig användning av en europeisk digital identitetsplånbok

Användaren av en europeisk digital identitetsplånbok ansvarar för obehörig användning av plånboken endast om

- 1) användaren har överlåtit den för att användas av någon annan,
- 2) den obehöriga användningen av plånboken beror på användarens oaktsamhet som inte är lindrig, eller
- 3) användaren har försummat sin anmälningsskyldighet enligt 14 § 2 mom.

Användaren av en europeisk digital identitetsplånbok ansvarar dock inte för obehörig användning av plånboken

- 1) till den del plånboken har använts efter att användaren har gjort en anmälan enligt 14 § 2 mom., eller

- 2) om tillhandahållaren av plånboken har försummat att sörja för att plånbokens användare har möjlighet att uppfylla sin anmälningsskyldighet enligt 14 § 2 mom.

Ett avtalsvillkor som avviker från 1 eller 2 mom. till nackdel för konsumenten är ogiltigt.

16 §

Nationellt register över europeiska digitala identitetsplånböckers förlitande parter

Transport- och kommunikationsverket ska inrätta och vara personuppgiftsansvarig för det nationella register över europeiska digitala identitetsplånböckers förlitande parter som avses i artikel 5b i eIDAS-förordningen.

Utöver vad som föreskrivs i 1 mom. svarar Transport- och kommunikationsverket för medlemsstatens skyldigheter i Finland enligt artikel 5b i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den.

Transport- och kommunikationsverket får utfärda närmare föreskrifter om genomförandet av förlitandepartcertifikat och förlitandepartregistreringscertifikat för en europeisk digital identitetsplånbok samt om certifikatspolicy och certifieringspraxis för dem, med iakttagande av bestämmelser som utfärdats med stöd av artikel 5b i eIDAS-förordningen.

17 §

Valideringsmekanismer för ramverket för den europeiska digitala identitetsplånboken

Myndigheten för digitalisering och befolkningsdata tillhandahåller i Finland den valideringsmekanism som avses i artikel 5a.8 a i eIDAS-förordningen och som gäller plånböckers äkthet och giltighet.

Transport- och kommunikationsverket tillhandahåller i Finland den valideringsmekanism som avses i artikel 5a.8 b i eIDAS-förordningen och som gäller äkthet och giltighet för identiteten hos förlitande parter.

18 §

Identitetsmatchning

Myndigheten för digitalisering och befolkningsdata ska centraliserat genomföra identitetsmatchning för myndigheter och andra som sköter offentliga uppdrag med iakttagande av artikel 11a i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den artikeln.

Myndigheten för digitalisering och befolkningsdata ska bevara sådana uppgifter i identitetsmatchningsprocessen som avses i bestämmelser som utfärdats med stöd av artikel 11a i eIDAS-förordningen i högst två år från ingången av kalenderåret efter den tidpunkt då uppgifterna registrerades.

Privata sammanslutningar, stiftelser och näringsidkare får använda i 1 mom. avsedd identitetsmatchning som tillhandahålls av Myndigheten för digitalisering och befolkningsdata.

19 §

Nationell nod

Den nationella noden upprätthålls i Finland av Myndigheten för digitalisering och befolkningsdata.

3 kap.

Betrodda tjänster

20 §

Återkallande av certifikat

En innehavare av uppgifter för skapande av elektroniska underskrifter eller elektroniska stämplat ska utan dröjsmål begära att den certifikatutfärdare som har utfärdat ett kvalificerat certifikat ska återkalla det, om innehavaren har grundad anledning att misstänka att uppgifterna för skapande av elektroniska underskrifter eller elektroniska stämplat används på obehörigt sätt.

En certifikatutfärdare som tillhandahåller kvalificerat certifikat ska utan dröjsmål återkalla ett kvalificerat certifikat, om innehavaren av uppgifter för skapande av elektroniska underskrifter eller elektroniska stämplat begär det. En begäran om återkallande av ett certifikat anses ha kommit in till certifikatutfärdaren när den har stått till utfärdarens förfogande så att begäran har kunnat behandlas.

21 §

Ansvar för obehörig användning av uppgifter för skapande av elektroniska underskrifter eller elektroniska stämplat

Innehavaren av uppgifter för skapande av elektroniska underskrifter eller elektroniska stämplat ansvarar för skada som orsakats av obehörig användning av uppgifter för skapande av en avancerad elektronisk underskrift eller elektronisk stämpel som är baserad på ett kvalificerat certifikat tills en begäran om återkallande av certifikatet har kommit in till certifikatutfärdaren.

Innehavaren av uppgifter för skapande av elektroniska underskrifter eller elektroniska stämplat har dock ansvar enligt 1 mom. endast om

- 1) innehavaren har överlåtit uppgifterna för skapande till någon annan,
- 2) någon som är obehörig att använda uppgifter för skapande har kommit åt dem på grund av att innehavaren varit oaktsam på ett sätt som inte är lindrigt, eller
- 3) innehavaren på annat sätt än det som nämns i 2 punkten har förlorat besittningen till uppgifter för skapande och därefter har underlåtit att begära att certifikatet ska återkallas enligt 20 § 1 mom.

Ett avtalsvillkor som avviker från 1 eller 2 mom. till nackdel för konsumenten är ogiltigt.

22 §

Det ansvar som vilar på tillhandahållare av betrodda tjänster

Bestämmelser om det ansvar som vilar på tillhandahållare av betrodda tjänster finns i artikel 13 i eIDAS-förordningen.

Den certifikatutfärdare som tillhandahållit ett kvalificerat certifikat är ansvarig för skada som den som förlitat sig på det kvalificerade certifikatet orsakats på grund av att certifikatutfärdaren eller en person som denne anlitat inte har återkallat certifikatet på det sätt som föreskrivs i 20 §. Certifikatutfärdaren är fri från ansvar, om den visar att skadan inte har berott på oaktsamhet hos certifikatutfärdaren eller en person som denne anlitat.

23 §

Myndigheten för digitalisering och befolkningsdatas anvisningar för kontroll av attribut mot autentiska källor

Myndigheten för digitalisering och befolkningsdata har till uppgift att utarbeta anvisningar om de elektroniska medel som kvalificerade tillhandahållare av betrodda tjänster för elektroniska attributsintyg kan använda när de vill kontrollera de attribut som avses i bilaga VI till eIDAS-förordningen mot autentiska källor i Finland.

Anvisningarna ska åtminstone innehålla en beskrivning av de autentiska källorna i Finland för de attribut som avses i bilaga VI till eIDAS-förordningen samt en beskrivning av de tekniska gränssnitt som är tillgängliga för de autentiska källorna.

4 kap.

Bedömning av överensstämmelse

24 §

Bedömning av överensstämmelse av den nationella noden

Myndigheten för digitalisering och befolkningsdata ska genom en bedömning som görs av ett godkänt bedömningsorgan för informationssäkerhet som avses i lagen om bedömningsorgan för informationssäkerhet (1405/2011), av ett organ för bedömning av överensstämmelse eller av Transport- och kommunikationsverket, visa att den nationella nod som myndigheten upprätthåller med stöd av 19 § i denna lag uppfyller kraven enligt eIDAS-förordningen och bestämmelser som utfärdats med stöd av den. Myndigheten för digitalisering och befolkningsdata ska skaffa en bedömningsrapport över bedömningen och lämna den till Transport- och kommunikationsverket, om bedömningen görs av ett bedömningsorgan för informationssäkerhet eller ett organ för bedömning av överensstämmelse.

Bedömningsrapporten är i kraft den tid som anges i den standard som använts vid bedömningen, dock högst i två år.

Transport- och kommunikationsverket får utfärda närmare föreskrifter om bedömningsgrunderna för bedömning av överensstämmelse av den nationella noden med iakttagande av eIDAS-förordningen och bestämmelser som utfärdats med stöd av den.

25 §

Nationell certifieringsordning för europeiska digitala identitetsplånböcker

Den i artikel 5c i eIDAS-förordningen och i bestämmelser som utfärdats med stöd av den avsedda ägaren av den nationella certifieringsordningen för en europeisk digital identitetsplånbok i Finland är Transport- och kommunikationsverket.

Transport- och kommunikationsverket får i anslutning till sin uppgift enligt 1 mom. samt i anslutning till utseendet av ett organ för bedömning av överensstämmelse enligt 26 § anförtro en biträdande uppgift till en underleverantör som har tillräckliga tekniska förutsättningar och tillräcklig kompetens för uppgiften och som uppfyller de krav som gäller uppgiften enligt eIDAS-förordningen och bestämmelser som utfärdats med stöd av den samt i denna lag och föreskrifter som utfärdats med stöd av den.

Transport- och kommunikationsverket får utfärda närmare föreskrifter om den nationella certifieringsordningen för en europeisk digital identitetsplånbok samt om bedömningsgrunderna för bedömning av överensstämmelse av plånboken och om det förfarande som ska iaktas vid bedömning av överensstämmelse, med iakttagande av eIDAS-förordningen och bestämmelser som har utfärdats med stöd av den.

26 §

Utseende och anmälan av organ för bedömning av överensstämmelse

Transport- och kommunikationsverket har till uppgift att på ansökan av ett organ för bedömning av överensstämmelse utse och till Europeiska kommissionen anmäla ett i Finland etablerat organ för bedömning av överensstämmelse i enlighet med eIDAS-förordningen och bestämmelser som utfärdats med stöd av den.

En förutsättning för utseende och anmälan är att organet för bedömning av överensstämmelse uppfyller de krav som föreskrivs i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den samt i denna lag och föreskrifter som utfärdats med stöd av den och att det har beviljats ett ackrediteringsintyg, utfärdat av Säkerhets- och kemikalieverkets ackrediteringsenhet (ackrediteringstjänsten FINAS) eller en utländsk ackrediteringsenhet, enligt vilket organet för bedömning av överensstämmelse inom sitt behörighetsområde uppfyller de angivna kraven.

Ett organ för bedömning av överensstämmelse kan i sin uppgift anlita en underleverantör för vars arbete organet ansvarar som för sitt eget. Underleverantören ska ha tillräckliga tekniska förutsättningar och tillräcklig kompetens för uppgiften och uppfylla de krav för uppgiften som föreskrivs i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den samt i denna lag och föreskrifter som utfärdats med stöd av den.

Transport- och kommunikationsverket får, med iakttagande av eIDAS-förordningen och bestämmelser som utfärdats med stöd av den, utfärda närmare föreskrifter om

- 1) förutsättningarna för att utse ett organ för bedömning av överensstämmelse,
- 2) de uppgifter som ska ingå i en ansökan om utseende av ett organ för bedömning av överensstämmelse och inlämnandet av uppgifterna till Transport- och kommunikationsverket,
- 3) grunderna för bedömning av överensstämmelse i fråga om system för elektronisk identifiering och betrodda tjänster och förfarandet vid bedömning av överensstämmelse.

27 §

Tillsyn över organ för bedömning av överensstämmelse

Utöver vad som någon annanstans i lag föreskrivs om tillsynen över organ för bedömning av överensstämmelse övervakar Transport- och kommunikationsverket att ett av verket utsett och anmält organ för bedömning av överensstämmelse

- 1) i sin verksamhet uppfyller de förutsättningar för utseende som avses i 26 §,
- 2) på behörigt sätt utför de uppgifter som föreskrivs för organet i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den samt i denna lag och föreskrifter som utfärdats med stöd av den.

Ett organ för bedömning av överensstämmelse ska underrätta Transport- och kommunikationsverket om varje ändring som kan ha betydelse för uppfyllandet av förutsättningarna för utseende.

Om inte något annat följer av vad som föreskrivs i eller med stöd av eIDAS-förordningen ska Transport- och kommunikationsverket ålägga organet för bedömning av överensstämmelse att avhjälpa sina fel eller försummelser inom en skälig tid.

Om organet för bedömning av överensstämmelse inte korrigerar sin verksamhet inom utsatt tid och ett fel eller en försummelse är väsentlig ska Transport- och kommunikationsverket, om inte något annat följer av vad som föreskrivs i eller med stöd av eIDAS-förordningen, återkalla utseendet av organet för bedömning av överensstämmelse och till Europeiska kommissionen anmäla att organet inte längre uppfyller förutsättningarna för anmälan.

28 §

Certifierare av anordningar för skapande av elektroniska underskrifter och elektroniska stämplor

Transport- och kommunikationsverket kan på ansökan utse och till Europeiska kommissionen anmäla privata eller offentliga aktörer som avses i artiklarna 30 och 39.2 i eIDAS-förordningen och som har i uppgift att certifiera anordningar för skapande av kvalificerade elektroniska underskrifter och kvalificerade elektroniska stämplor (*certifierare*). I ansökan ska lämnas de uppgifter som Transport- och kommunikationsverket begär och som behövs för handläggningen av ansökan.

En förutsättning för att utse en certifierare är att den är funktionellt och ekonomiskt oberoende av tillverkarna av anordningar för skapande av elektroniska underskrifter och elektroniska stämplor och att certifieraren har

- 1) en ansvarsförsäkring som är tillräcklig med hänsyn till verksamhetens omfattning, eller något annat motsvarande arrangemang,
- 2) tillräckligt med yrkeskunnig personal till sitt förfogande,
- 3) de system, anordningar och redskap som verksamheten förutsätter.

Om inte något annat följer av vad som föreskrivs i eller med stöd av eIDAS-förordningen, tillämpas på tillsynen över certifierare och den certifiering som de utför vad som i 27, 29 och 30 § föreskrivs om tillsynen över organ för bedömning av överensstämmelse, organets tillsynsuppgifter och tillsynsmetoder samt återkallande av intyg om överensstämmelse.

Transport- och kommunikationsverket får utfärda närmare föreskrifter om kraven på certifierare, det förfarande som ska iaktas vid certifiering samt kraven på anordningar för skapande av elektroniska underskrifter och elektroniska stämplor med iakttagande av eIDAS-förordningen och bestämmelser som utfärdats med stöd av den.

29 §

Tillsynsuppgift och tillsynsmetoder för organ för bedömning av överensstämmelse

Om inte något annat följer av vad som föreskrivs i eller med stöd av eIDAS-förordningen, ska ett organ för bedömning av överensstämmelse utöva tillsyn över att den till vilken organet har beviljat ett intyg om överensstämmelse (*innehavare av intyg om överensstämmelse*) uppfyller förutsättningarna för erhållande av intyget.

Ett organ för bedömning av överensstämmelse har trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter rätt att av innehavaren av ett intyg om överensstämmelse få de uppgifter som behövs för skötseln av de uppgifter som föreskrivs för organet i eIDAS-förordningen och bestämmelser som utfärdats med stöd av den samt i denna lag och bestämmelser som utfärdats med stöd av den. Innehavaren av ett intyg om överensstämmelse ska underrätta organet för bedömning av överensstämmelse om varje ändring som kan ha betydelse för uppfyllandet av förutsättningarna för erhållande av intyget.

Ett organ för bedömning av överensstämmelse har för fullgörande av sin tillsynsuppgift enligt 1 mom. rätt att utföra inspektion av innehavaren av ett intyg om överensstämmelse och av den produkt eller tjänst som innehavaren tillhandahåller och som är föremål för bedömningen.

30 §

Återkallande av intyg om överensstämmelse

Om ett organ för bedömning av överensstämmelse konstaterar att innehavaren av ett intyg om överensstämmelse eller den produkt eller tjänst som bedömningen gäller inte uppfyller förutsättningarna för erhållande av intyget om överensstämmelse eller att intyget annars inte borde ha utfärdats, ska organet för bedömning av överensstämmelse uppmana innehavaren av intyget om överensstämmelse att avhjälpa bristerna inom utsatt tid, om inte något annat följer av vad som föreskrivs i eller med stöd av eIDAS-förordningen.

Om inte något annat följer av vad som föreskrivs i eller med stöd av eIDAS-förordningen, ska organet för bedömning av överensstämmelse återkalla intyget om överensstämmelse för viss tid eller helt och hållet eller utfärda det med begränsningar, om inte innehavaren av intyget om överensstämmelse avhjälper bristerna inom utsatt tid.

Ett organ för bedömning av överensstämmelse ska underrätta Transport- och kommunikationsverket om de tillsynsåtgärder som avses i 1 och 2 mom.

31 §

Tillämpning av lagstiftningen om offentlighet samt utlämnande av uppgifter vid bedömning av överensstämmelse

Också när det inte är fråga om utövning av offentlig makt tillämpas lagen om offentlighet i myndigheternas verksamhet (621/1999) på sådana organ för bedömning av informationssäkerhet som avses i 24 §, på organ för bedömning av överensstämmelse och av dem använda underleverantörer samt på certifierare i uppgifter i anslutning till verkställigheten av eIDAS-förordningen och bestämmelser som utfärdats med stöd av den samt av denna lag och föreskrifter som utfärdats med stöd av denna lag. Om tillämpningen av andra allmänna förvaltningslagar föreskrivs särskilt.

På tystnadsplikten och förbudet mot att utnyttja uppgifter för en person som är anställd hos en i 1 mom. avsedd aktör eller verksam i aktörens beslutande organ och som behandlar sekretessbelagda uppgifter i anslutning till bedömningsverksamheten tillämpas vad som i 23 §

i lagen om offentlighet i myndigheternas verksamhet föreskrivs om tystnadsplikt och förbud mot utnyttjande för den som är anställd hos en myndighet.

Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet och någon annanstans i lag har en i 1 mom. avsedd aktör trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter rätt att på eget initiativ lämna ut handlingar som aktören fått eller upprättat i samband med skötseln av sina uppgifter enligt det momentet samt att röja sekretessbelagd information för Transport- och kommunikationsverket för skötseln av uppgifter som föreskrivs i eIDAS-förordningen eller bestämmelser som utfärdats med stöd av den eller i denna lag. Bestämmelser om Transport- och kommunikationsverkets rätt att få information finns i 35 §.

32 §

Straffrättsligt tjänsteansvar vid bedömning av överensstämmelse

På anställda hos följande aktörer och personer verksamma i beslutande organ hos följande aktörer tillämpas bestämmelserna om straffrättsligt tjänsteansvar för tjänstemän när de sköter uppgifter som föreskrivs i eIDAS-förordningen eller bestämmelser som utfärdats med stöd av den eller i denna lag:

- 1) de bedömningsorgan för informationssäkerhet som avses i 24 §,
- 2) Transport- och kommunikationsverkets underleverantörer som avses i 25 § 2 mom.,
- 3) organ för bedömning av överensstämmelse och deras underleverantörer,
- 4) certifierare.

Bestämmelser om skadeståndsansvar finns i skadeståndslagen (412/1974).

5 kap.

Tillsyn

33 §

Transport- och kommunikationsverkets uppgifter

Transport- och kommunikationsverket ska utöver vad som föreskrivs ovan i denna lag utöva tillsyn över efterlevnaden av denna lag. Dessutom har Transport- och kommunikationsverket till uppgift att

- 1) informera Europeiska kommissionen om de uppgifter som avses i artikel 5a.18 i eIDAS-förordningen och de bestämmelser som utfärdats med stöd av den artikeln,
- 2) informera Europeiska kommissionen och den samarbetsgrupp som avses i artikel 46e.1 i eIDAS-förordningen om de uppgifter som avses i artikel 5d i den förordningen och i bestämmelser som utfärdats med stöd av den artikeln,
- 3) anmäla system för elektronisk identifiering till Europeiska kommissionen i enlighet med artiklarna 7–10 i eIDAS-förordningen,
- 4) delta i samarbetet mellan Europeiska unionens medlemsstater i det interoperabilitetsramverk för elektronisk identifiering som avses i artikel 12 i eIDAS-förordningen,
- 5) i enlighet med artikel 22 i eIDAS-förordningen föra och publicera förteckningar över kvalificerade tillhandahållare av betrodda tjänster i Finland och över de kvalificerade betrodda tjänster som dessa tillhandahåller,
- 6) vara tillsynsorgan enligt artikel 46a och 46b i eIDAS-förordningen och sköta tillsynsorganets uppgifter enligt förordningen,

7) vara den gemensamma kontaktpunkt som avses i artikel 46c i eIDAS-förordningen och sköta de uppgifter som föreskrivs för den i eIDAS-förordningen,

8) offentliggöra och till Europeiska kommissionen lämna uppgifter som avses i artikel 48a.2 i eIDAS-förordningen med iakttagande av artikel 48a.3 och 48a.4 i förordningen.

34 §

Prioritetsordning för Transport- och kommunikationsverkets uppgifter och lämnande av ett ärende utan prövning

Transport- och kommunikationsverket kan ställa sina uppgifter enligt denna lag i prioritetsordning i enlighet med uppgiftens betydelse för fullgörandet av de skyldigheter som föreskrivs i denna lag eller eIDAS-förordningen eller i bestämmelser eller föreskrifter som utfärdats med stöd av dem.

Transport- och kommunikationsverket får lämna ett ärende utan prövning, om ärendet trots en misstanke om fel eller försummelser endast har en ringa betydelse för fullgörandet av skyldigheterna enligt 1 mom. Transport- och kommunikationsverket ska genast när det är möjligt fatta beslut om att inte ta upp ett ärende till prövning.

35 §

Rätt att få information

Transport- och kommunikationsverket har trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att av andra myndigheter, tillhandahållare av en europeisk digital identitetsplånbok och plånbokens användare, förlitande parter, tillhandahållare av en betrodd tjänst och användare av tjänsten, organ för bedömning av överensstämmelse, certifierare, tillhandahållare av system för elektronisk identifiering och av dem som handlar för deras räkning få de uppgifter som är nödvändiga för att verket ska kunna utföra sina uppgifter enligt denna lag och eIDAS-förordningen samt bestämmelser som utfärdats med stöd av dem. Informationen ska lämnas ut utan dröjsmål, i den form som Transport- och kommunikationsverket begärt och avgiftsfritt.

36 §

Rätt att lämna ut sekretessbelagd information

Utöver vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet och någon annanstans i lag har Transport- och kommunikationsverket trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att på eget initiativ eller på begäran lämna ut handlingar som verket fått eller upprättat i samband med skötseln av sina uppgifter enligt denna lag och eIDAS-förordningen samt att röja sekretessbelagd information till

1) dataombudsmannen, om det är nödvändigt för skötseln av dennes lagstadgade tillsynsuppgifter,

2) de tillsynsmyndigheter i andra medlemsstater i Europeiska unionen som avses i artiklarna 46a och 46b i eIDAS-förordningen och de gemensamma kontaktpunkter i andra medlemsstater i Europeiska unionen som avses i artikel 46c i den förordningen, om det är nödvändigt för skötseln av de uppgifter som föreskrivs i eIDAS-förordningen.

Transport- och kommunikationsverket har i den utsträckning det är nödvändigt rätt att använda sekretessbelagda handlingar och uppgifter som verket upprättat och fått i samband med skötseln av sina uppgifter enligt denna lag och eIDAS-förordningen för skötseln av de uppgifter

som tillhör verket som tillsynsmyndighet enligt 26 § i cybersäkerhetslagen (124/2025), som CSIRT-enhet enligt 19 § i den lagen och som gemensam kontaktpunkt enligt 18 § i den lagen samt som myndighet för cybersäkerhetscertifiering enligt 21 § lagen om cyberresiliens för vissa produkter och om cybersäkerhetscertifiering (/).

37 §

Rätt att utföra inspektioner

Transport- och kommunikationsverket har rätt att utföra inspektioner av en tillhandahållare av en europeisk digital identitetsplånbok och en plånbok som denne tillhandahåller, av ett organ för bedömning av överensstämmelse eller av en certifierare och deras verksamhet, av en tillhandahållare av betrodda tjänster och den betrodda tjänst som denne tillhandahåller samt av dem som handlar för deras räkning. Inspektioner kan utföras för att övervaka att skyldigheterna enligt denna lag eller föreskrifter som utfärdats med stöd av den eller enligt eIDAS-förordningen eller bestämmelser som utfärdats med stöd av den iakttas.

Transport- och kommunikationsverket förordnar en inspektör att utföra de inspektioner som avses i 1 mom. Aktörer som är föremål för inspektion ska i den omfattning som inspektionen förutsätter ge den som utför inspektionen tillträde till det kommunikationsnät eller informationssystem som inspektionen gäller och till andra utrymmen än sådana som är avsedda för boende av permanent natur. Den som utför en inspektion har trots sekretessbestämmelserna rätt att få granska sådana uppgifter som är nödvändiga för tillsynsuppgiften.

På förfarandet vid inspektioner tillämpas 39 § i förvaltningslagen (434/2003).

38 §

Anmärkning och tillsynsbeslut

Transport- och kommunikationsverket kan uppmärksamma en aktör som verket utövar tillsyn över med stöd av denna lag på brister eller ålägga aktören att inom skälig tid avhjälpa brister i iakttagandet av skyldigheterna enligt denna lag eller föreskrifter som utfärdats med stöd av den eller enligt eIDAS-förordningen eller bestämmelser som utfärdats med stöd av dem.

Om aktören efter att ha fått det förpliktande beslutet inte avhjälper de brister som avses i 1 mom. inom utsatt tid, kan Transport- och kommunikationsverket ålägga aktören att avbryta eller upphöra med tillhandahållandet av tjänsten eller i fråga om kvalificerade betrodda tjänster återkalla tjänstetillhandahållarens eller den av tjänstetillhandahållaren tillhandahållna tjänstens status som kvalificerad. När Transport- och kommunikationsverket fattar beslut ska det beakta omfattningen, varaktigheten och följderna av den brist som hänför sig till iakttagandet av skyldigheterna.

Om en behörig myndighet som utsetts eller inrättats med stöd av artikel 8.1 i Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1772 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) eller ett övervakningsorgan som utsetts eller inrättats med stöd av Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) gör en i artikel 20.3a eller 20.3b i eIDAS-förordningen avsedd anmälan till Transport- och kommunikationsverket, får Transport- och kommunikationsverket, utöver vad som föreskrivs i 1 och 2 mom., med beaktande av omfattningen, varaktigheten och följderna av försummelsen i anslutning till iakttagandet av skyldigheterna, återkalla statusen som kvalificerad för den kvalificerade tillhandahållaren av betrodda tjänster eller för den berörda tillhandahållna tjänsten.

39 §

Interimistiska beslut

Om en försummelse av en skyldighet enligt denna lag eller föreskrifter som utfärdats med stöd av den eller eIDAS-förordningen eller bestämmelser som utfärdats med stöd av den eller om en säkerhetsincident omedelbart och i väsentlig grad äventyrar tillförlitligheten hos en tillhandahållen tjänst, får Transport- och kommunikationsverket utan dröjsmål och oberoende av den tidsfrist som avses i 38 § som en interimistisk åtgärd förbjuda eller avbryta i eIDAS-förordningen avsett

- 1) tillhandahållande och användning av en kvalificerad betrodd tjänst enligt artikel 3.17,
- 2) tillhandahållande av en europeisk digital identitetsplånbok enligt artikel 5a,
- 3) tillhandahållande av en valideringsmekanism enligt artikel 5a.8,
- 4) tillhandahållande av ett sådant system för elektronisk identifiering enligt artikel 5a.11 som en del av vilket en europeisk digital identitetsplånbok tillhandahålls,
- 5) tillhandahållande av ett system för elektronisk identifiering som anmälts i enlighet med artikel 9.1,
- 6) tillhandahållande av autentisering enligt artikel 7 f.

Transport- och kommunikationsverket kan delvis förbjuda eller avbryta tillhandahållandet av en tjänst som avses i 1 mom., om det inte är nödvändigt att förbjuda tillhandahållandet av tjänsten i dess helhet.

Transport- och kommunikationsverket ska innan det beslutar om interimistiska åtgärder ge den som är föremål för beslutet tillfälle att bli hörd, utom när detta inte kan ordnas så snabbt som ärendets brådskande natur nödvändigtvis kräver.

De interimistiska åtgärderna kan vara i kraft i högst tre månader. Om en försummelse eller säkerhetsincident inte avhjälpas inom den tidsfrist som anges i beslutet om interimistiska åtgärder, får Transport- och kommunikationsverket ålägga tillhandahållaren av tjänsten att upphöra med tillhandahållandet av tjänsten.

40 §

Vite, hot om tvångsutförande och hot om avbrytande

Transport- och kommunikationsverket kan förena ett i 38 § 1 och 2 mom. avsett tillsynsbeslut och ett i 39 § avsett beslut om interimistiska åtgärder med vite eller med hot om att verksamheten helt eller delvis avbryts eller att den försummade åtgärden vidtas på den försumliges bekostnad. Bestämmelser om vite, hot om avbrytande och hot om tvångsutförande finns i viteslagen (1113/1990).

41 §

Avgifter till Transport- och kommunikationsverket

En tillhandahållare av europeiska digitala identitetsplånböcker ska betala Transport- och kommunikationsverket en årlig tillsynsavgift på 17 000 euro.

En kvalificerad tillhandahållare av betrodda tjänster som har gjort en i artikel 21 i eIDAS-förordningen avsedd anmälan ska betala Transport- och kommunikationsverket en årlig tillsynsavgift på 17 000 euro för den första kvalificerade betrodda tjänst som den tillhandahåller och en årlig tillsynsavgift på 11 000 euro för varje därpå följande kvalificerade betrodda tjänst som den tillhandahåller.

Ett organ för bedömning av överensstämmelse som utsetts enligt 26 § ska betala Transport- och kommunikationsverket en årlig tillsynsavgift på 18 000 euro.

En certifierare som utsetts enligt 28 § ska betala Transport- och kommunikationsverket en årlig tillsynsavgift på 18 000 euro.

Tillsynsavgiften ska betalas till fullt belopp också under det första verksamhetsåret, även om verksamheten inleds senare under året. Tillsynsavgiften återbetalas inte även om tjänsteleverantören upphör med sin verksamhet under året.

Tillsynsavgiften påförs av Transport- och kommunikationsverket och avgiften är direkt utsökbar. Bestämmelser om sökande av ändring i beslut om påförande av avgift finns i 51 §.

Bestämmelser om indrivning av tillsynsavgifter finns i lagen om verkställighet av skatter och avgifter (706/2007). Om avgiften inte betalas senast på förfallodagen, tas årlig dröjsmålsränta ut på det obetalda beloppet enligt den räntesats som föreskrivs i 4 § i räntelagen (633/1982). I stället för dröjsmålsränta kan myndigheten ta ut en dröjsmålsavgift på fem euro om dröjsmålsräntan är mindre än detta belopp.

Bestämmelser om avgifter som tas ut för behandling av en anmälan som avses i 7 § 3 mom., behandling av ansökningar som avses i 26 § 1 mom. och 28 § 1 mom., inspektion som avses i 37 § 1 mom. samt behandling av en anmälan som avses i artikel 21 i eIDAS-förordningen och registrering som avses i artikel 5b.1 i den förordningen finns i lagen om grunderna för avgifter till staten (150/1992). Bestämmelser om avgifter som tas ut för prestationer som avses i 5 § i denna lag och som gäller identifieringsuppgifter för juridiska personer finns i lagen om avgifter för patent- och registerstyrelsens prestationer (1032/1992).

6 kap.

Påföljdsavgifter

42 §

Påföljdsavgifter för tillhandahållare av betrodda tjänster

Påföljdsavgift kan av Transport- och kommunikationsverket påföras en sådan tillhandahållare av betrodda tjänster som uppsåtligen eller av oaktsamhet bryter mot eller försummar den i artikel 15 i eIDAS-förordningen föreskrivna skyldigheten att tillhandahålla sina tjänster på ett klart och begripligt språk i enlighet med Förenta nationernas konvention om rättigheter för personer med funktionsnedsättning (FördrS 27/2016) och tillgänglighetskraven i Europaparlamentets och rådets direktiv (EU) 2019/882 om tillgänglighetskrav för produkter och tjänster.

43 §

Påföljdsavgifter för icke-kvalificerade tillhandahållare av betrodda tjänster

Påföljdsavgift kan av Transport- och kommunikationsverket påföras en sådan icke-kvalificerad tillhandahållare av betrodda tjänster som uppsåtligen eller av oaktsamhet bryter mot eller försummar skyldigheten enligt artikel 19a i eIDAS-förordningen eller i bestämmelser som utfärdats med stöd av den att underrätta tillsynsorganet, identifierbara berörda personer, allmänheten, om det ligger i allmänt intresse, och vid behov andra relevanta behöriga myndigheter om säkerhetsincidenter eller störningar vid tillhandahållandet av tjänsten eller vid genomförandet av de åtgärder som avses i artikel 19a.1.

44 §

Påföljdsavgifter för kvalificerade tillhandahållare av betrodda tjänster

Påföljdsavgift kan av Transport- och kommunikationsverket påföras en sådan kvalificerad tillhandahållare av betrodda tjänster som uppsåtligen eller av oaktsamhet bryter mot eller försummar den i eIDAS-förordningen föreskrivna

1) skyldigheten enligt artikel 20.1 att lämna in en rapport om bedömning av överensstämmelse till tillsynsorganet eller skyldigheten enligt artikel 20.1a att informera tillsynsorganet om en planerad revision,

2) skyldigheten enligt artikel 21.1 att informera tillsynsorganet om sin avsikt att börja tillhandahålla en kvalificerad betrodd tjänst och samtidigt lämna in en rapport om bedömning av överensstämmelse,

3) skyldigheten enligt artikel 23.2 att se till att en länk till den relevanta förteckningen över betrodda tjänsteleverantörer finns på dess webbplats, när tillhandahållaren av betrodda tjänster använder EU-förtroendemärket,

4) skyldigheten

a) enligt artikel 24.2 a att informera tillsynsorganet innan en ändring av tillhandahållandet av dess kvalificerade betrodda tjänster genomförs eller dess verksamhet upphör,

b) enligt artikel 24.2 d att innan den ingår ett avtalsförhållande informera om de exakta villkor och förutsättningar för användningen av den kvalificerade betrodda tjänsten,

c) enligt artikel 24.2 f att använda tillförlitliga system för att lagra uppgifter som har lämnats till den,

d) enligt artikel 24.2 fb att anmäla incidenter eller störningar vid tillhandahållandet av tjänsten eller genomförandet av de åtgärder som avses i artikel 24.2 fa till tillsynsorganet, de identifierbara berörda personerna, vid behov andra relevanta behöriga organ och, på begäran av tillsynsorganet, allmänheten om det ligger i allmänt intresse,

e) enligt artikel 24.2 h att registrera och tillgängliggöra all relevant information om uppgifter som den kvalificerade tillhandahållaren av betrodda tjänster har utfärdat och tagit emot, eller

f) enligt artikel 24.2 i att ha en uppdaterad plan för verksamhetens upphörande.

45 §

Påföljdsavgift för kvalificerade tillhandahållare av betrodda tjänster som tillhandahåller kvalificerade certifikat

Påföljdsavgift kan av Transport- och kommunikationsverket påföras en kvalificerad tillhandahållare av betrodda tjänster som tillhandahåller kvalificerade certifikat, om tillhandahållaren uppsåtligen eller av oaktsamhet bryter mot eller försummar skyldigheten enligt artikel 24.1 i eIDAS-förordningen att kontrollera identiteten och eventuella andra attribut för den fysiska eller juridiska person för vilken det kvalificerade certifikatet utfärdas, skyldigheten enligt artikel 24.2 k att upprätta och uppdatera en certifikatdatabas, skyldigheten enligt artikel 24.3 att registrera ett återkallande av certifikat i sin certifikatdatabas och offentliggöra återkallandet eller skyldigheten enligt artikel 24.4 att informera om giltigheten eller statusen som återkallad hos kvalificerade certifikat.

46 §

Påföljdsavgift för kvalificerade tillhandahållare av betrodda tjänster som tillhandahåller kvalificerade elektroniska attributsintyg

Påföljdsavgift kan av Transport- och kommunikationsverket påföras en kvalificerad tillhandahållare av betrodda tjänster som tillhandahåller kvalificerade elektroniska attributsintyg och som uppsåtligen eller av oaktsamhet bryter mot eller försummar skyldigheten

enligt artikel 24.1 i eIDAS-förordningen att kontrollera identiteten och eventuella andra attribut för den fysiska eller juridiska person till vilken ett kvalificerat elektroniskt attributsintyg utfärdas, eller skyldigheten enligt artikel 24.4 a att iaktta kraven i artikel 24.3 och 24.4 vid återkallelse av kvalificerade elektroniska attributsintyg.

47 §

Påföljdsavgiftens storlek

Påförandet av påföljdsavgift och påföljdsavgiftens belopp grundar sig på en helhetsbedömning där följande ska beaktas:

1) överträdelsens art, omfattning och varaktighet samt hur allvarlig och återkommande överträdelsen är,

2) det allmänintresse som eftersträvas med påföljden,

3) storleken hos och affärsmodellerna för tillhandahållaren av betrodda tjänster,

4) de åtgärder som tillhandahållaren av betrodda tjänster vidtagit för att lindra eller avhjälpa den skada som överträdelsen orsakat,

5) tillhandahållaren av betrodda tjänsters eventuella tidigare överträdelser,

6) eventuella andra än i 1–5 punkten avsedda faktorer som har påverkat omständigheterna.

Påföljdsavgiftens belopp är minst 1 000 euro om påföljdsavgiften påförs en fysisk person, och i annat fall minst 10 000 euro. Om tillhandahållaren av betrodda tjänster är en fysisk person, får den påföljdsavgift som påförs tillhandahållaren vara högst 5 000 000 euro. Om tillhandahållaren av betrodda tjänster är en juridisk person, får den påföljdsavgift som påförs tillhandahållaren vara högst 5 000 000 euro eller en procent av den globala årsomsättningen för det företag till vilket tillhandahållaren av betrodda tjänster hörde under den räkenskapsperiod som föregått överträdelseåret, beroende på vilket belopp som är störst.

Med omsättning avses omsättning enligt 4 kap. 1 § i bokföringslagen (1336/1997) eller motsvarande omsättning.

48 §

Avstående från påförande av påföljdsavgift

Påföljdsavgift påförs inte, om

1) överträdelsen av en skyldighet ska anses vara ringa, eller

2) påförande av påföljdsavgift ska anses vara uppenbart oskäligt.

Påföljdsavgift får inte påföras den som misstänks för samma gärning i en förundersökning, en åtalsprövning eller ett brottmål som är anhängigt vid domstol. Påföljdsavgift får inte heller påföras den som genom en lagakraftvunnen dom har dömts för samma gärning.

Påföljdsavgift får inte påföras, om mer än fem år har förflutit sedan överträdelsen eller försummelsen inträffade. Om överträdelsen eller försummelsen har varit fortlöpande räknas den femåriga tidsfristen från det att överträdelsen eller försummelsen upphörde.

49 §

Verkställighet av påföljdsavgift

Bestämmelser om verkställighet av påföljdsavgifter som påförts med stöd av denna lag finns i lagen om verkställighet av böter (672/2002).

7 kap.

Särskilda bestämmelser

50 §

Avvikelse från förvaltningslagens procedurbestämmelser

Med avvikelse från förvaltningslagen ges inte något förvaltningsbeslut eller några anvisningar om hur man begär omprövning eller någon upplysning om besvärsförbud när identifieringsuppgifter för fysiska och juridiska personer enligt 3 och 5 § i denna lag utfärdas eller återkallas i enlighet med ansökan.

Med avvikelse från vad som föreskrivs i förvaltningslagen och i 68 § i lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata (661/2009) ges inte något förvaltningsbeslut eller några anvisningar om hur man begär omprövning eller någon upplysning om besvärsförbud i fråga om tillhandahållande av betrodda tjänster för en europeisk digital identitetsplånbok eller avbrytande eller avslutande av tillhandahållandet i enlighet med tjänstemottagarens ansökan.

51 §

Begäran om omprövning

Omprövning får begäras av andra avgöranden som Myndigheten för digitalisering och befolkningsdata och Patent- och registerstyrelsen har meddelat med stöd av denna lag än sådana som avses i 50 §.

Omprövning får begäras av ett beslut av Transport- och kommunikationsverket som gäller en i 41 § avsedd avgift som ska betalas till Transport- och kommunikationsverket.

Omprövning av ett beslut som ett organ för bedömning av överensstämmelse eller en certifierare har fattat med stöd av denna lag eller eIDAS-förordningen eller bestämmelser som utfärdats med stöd av den förordningen får begäras hos Transport- och kommunikationsverket.

Bestämmelser om begäran om omprövning finns i 7 a kap. i förvaltningslagen.

52 §

Besvärsförbud och sökande av ändring i myndighetsbeslut

Bestämmelser om sökande av ändring i förvaltningsdomstol finns i lagen om rättegång i förvaltningsärenden (808/2019). Vid sökande av ändring i beslut som gäller föreläggande och utdömande av vite samt föreläggande och verkställighet av hot om tvångsutförande eller hot om avbrytande tillämpas dock viteslagen.

I avgöranden som avses i 50 § och som fattats av Myndigheten för digitalisering eller befolkningsdata eller Patent- och registerstyrelsen får ändring inte sökas genom besvär.

Bestämmelser om sökande av ändring i Patent- och registerstyrelsens beslut med anledning av begäran om omprövning finns i lagen om Patent- och registerstyrelsen (578/2013).

Transport- och kommunikationsverket får i sitt tillsynsbeslut enligt 38 § eller interimistiska beslut enligt 39 § bestämma att beslutet ska iaktas innan det har vunnit laga kraft.

53 §

Ikraftträdande

Denna lag träder i kraft den 20 .

Myndigheten för digitalisering och befolkningsdata ska anpassa sin verksamhet till 3, 4, 7–9 § samt 17 § 1 mom., 18 § 1 och 2 mom. och 23 § senast den 24 december 2026.

Patent- och registerstyrelsen ska anpassa sin verksamhet till 5 och 6 § senast den 24 december 2026.

Transport- och kommunikationsverket ska anpassa sin verksamhet till 16 § och 17 § 2 mom. senast den 24 december 2026.

Lagens 18 § 3 mom. tillämpas från och med den 1 januari 2028.

2.

Lag

om ändring av lagen om stark autentisering och betrodda elektroniska tjänster

I enlighet med riksdagens beslut
upphävs i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) 30, 32 och 36 §, 4 a kap. samt 42 c §,
sådana de lyder, 30, 32 och 36 § i lag 1009/2018, 4 a kap. i lag 533/2016 och 42 c § i lag 1188/2019,
ändras lagens rubrik, 1, 2 och 7 b §, 17 § 2 mom., 24 § 2 mom., 29 §, 31 § 1 mom., 37, 38, 42 och 42 a §, 45 § 1 mom. samt 45 a, 46, 47 och 49 a §,
sådana de lyder, lagens rubrik, 1 § och 24 § 2 mom. i lag 533/2016, 2 och 7 b §, 17 § 2 mom., 29, 37 och 38 §, 45 § 1 mom., 45 a, 46 och 47 § i lag 1009/2018, 31 § 1 mom. i lag 1188/2019, 42 § i lagarna 1009/2018 och 230/2021, 42 a § i lag 230/2021 och 49 a § i lag 1542/2019, samt
fogas till lagen nya 12 e och 21 a § som följer:

Lag

om stark autentisering

1 §

Tillämpningsområde

Denna lag innehåller bestämmelser om

- 1) stark autentisering,
 - 2) tillhandahållande av identifieringstjänster till tjänsteleverantörer, till allmänheten och till andra leverantörer av identifieringstjänster,
 - 3) bedömning av överensstämmelse av identifieringstjänster.
- Lagen tillämpas inte på
- 1) tillhandahållande av tjänster avsedda för identifiering internt inom en sammanslutning,
 - 2) en sammanslutning som använder en egen metod för identifiering av egna kunder i samband med egna tjänster.

I lagen om vissa tjänster som möjliggör gränsöverskridande e-tjänster (/) föreskrivs det om tillsynen över efterlevnaden av bestämmelserna i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, nedan *eIDAS-förordningen*, sådan den lyder senast ändrad genom förordning (EU) 2024/1183, och utfärdas det bestämmelser som kompletterar förordningen.

2 §

Definitioner

I denna lag avses med

1) *stark autentisering* identifiering av en person, av en juridisk person eller av en fysisk person som företräder en juridisk person och verifiering av identifikatorns autenticitet och riktighet genom tillämpning av en elektronisk metod som motsvarar tillitsnivån väsentlig enligt artikel 8.2 b i eIDAS-förordningen eller tillitsnivån hög enligt artikel 8.2 c i den förordningen,

2) *identifieringsverktyg* ett sådant medel för elektronisk identifiering som avses i artikel 3.2 i eIDAS-förordningen,

3) *leverantör av identifieringstjänster* en leverantör av tjänster för identifieringsförmedling och en leverantör av identifieringsverktyg,

4) *leverantör av identifieringsverktyg* en tjänsteleverantör som tillhandahåller eller ger ut identifieringsverktyg för stark autentisering till allmänheten samt tillhandahåller sitt identifieringsverktyg till leverantörer av tjänster för identifieringsförmedling för förmedling i förtroendenätet,

5) *leverantör av tjänster för identifieringsförmedling* en tjänsteleverantör som förmedlar identifieringstransaktioner baserade på stark autentisering till en part som förlitar sig på en elektronisk identifiering,

6) *innehavare av identifieringsverktyg* en fysisk eller juridisk person som enligt avtal har fått ett identifieringsverktyg av en leverantör av identifieringstjänster,

7) *inledande identifiering* verifiering av identiteten hos den som ansöker om ett identifieringsverktyg, när verifieringen sker i samband med att verktyget skaffas,

8) *certifikat* ett intyg i elektronisk form som verifierar identiteten eller verifierar identiteten och kopplar ihop autentiseringsuppgifter för en betrodd tjänst med en användare av tjänsten och som kan användas vid stark autentisering och betrodda tjänster,

9) *certifikatutfärdare* en fysisk eller juridisk person som tillhandahåller allmänheten certifikat,

10) *förtroendenätet* de leverantörer av identifieringstjänster som har gjort en anmälan till Transport- och kommunikationsverket,

11) *organ för bedömning av överensstämmelse* ett av Transport- och kommunikationsverket godkänt organ enligt artikel 2.13 i Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknads kontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93, som är ackrediterat i enlighet med den förordningen,

12) *europaisk digital identitetsplånbok* en sådan europeisk digital identitetsplånbok som avses i artikel 3.42 i eIDAS-förordningen,

13) *system för elektronisk identifiering* detsamma som i artikel 3.4 i eIDAS-förordningen,

14) *förlitande part* detsamma som i artikel 3.6 i eIDAS-förordningen.

7 b §

Information om giltighet för pass, identitetskort eller e-legitimation

Leverantörer av identifieringstjänster har trots sekretessbestämmelserna rätt att via ett tekniskt gränssnitt eller annars i elektronisk form få information ur polisens informationssystem om giltigheten för pass eller identitetskort som används vid inledande identifiering samt information ur Myndigheten för digitalisering och befolkningsdatas informationssystem om giltigheten för ett kvalificerat elektroniskt attributsintyg som ingår i e-legitimation som avses i lagen om e-legitimation (/) och som och som används vid inledande identifiering.

Leverantörer av identifieringsverktyg är skyldiga att säkerställa den i 1 mom. avsedda informationen om giltigheten för de handlingar som används vid inledande identifiering. Leverantörerna ska säkerställa att ett identifieringsverktyg inte kan användas förrän handlingens giltighet har säkerställts.

12 e §

Förmedling av identifieringstransaktioner baserade på en europeisk digital identitetsplånbok

Leverantörer av tjänster för identifieringsförmedling kan förmedla identifieringstransaktioner som baserar sig på en europeisk digital identitetsplånbok till en part som förlitar sig på elektronisk identifiering, trots att bestämmelserna i denna lag inte tillämpas på plånböcker eller deras tillhandahållare.

17 §

Identifiering av en fysisk person som ansöker om ett identifieringsverktyg

Dokument som godkänns vid inledande identifiering, när identifieringen endast sker utifrån en identitetshandling som utfärdats av en myndighet, är ett giltigt pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet, i Schweiz eller i San Marino. Leverantörer av identifieringsverktyg kan som identitetshandling godkänna också en sådan e-legitimation som avses i lagen om e-legitimation. En leverantör av identifieringsverktyg som så önskar kan vid kontrollen av identiteten dessutom använda ett giltigt pass som har utfärdats av en myndighet i någon annan stat.

21 a §

Återaktivering av identifieringsverktyg

Vid återaktivering av identifieringsverktyg ska kraven i punkt 2.2.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering iakttas.

24 §

Registrering och användning av uppgifter om identifieringstransaktioner och identifieringsverktyg

Leverantörer av identifieringsverktyg ska registrera behövliga uppgifter om den inledande identifiering av sökande som avses i 17 och 17 a § och om de handlingar eller den elektroniska identifiering som använts i den inledande identifieringen. Om det i den inledande identifieringen används ett identifieringsverktyg som levereras av en annan leverantör av identifieringsverktyg, ska information om den inledande identifieringstransaktionen förmedlas till den berörda leverantören av identifieringsverktyg i samband med identifieringstransaktionen.

29 §

Bedömning av överensstämmelse hos en elektronisk identifieringstjänst

En leverantör av identifieringstjänster ska regelbundet låta ett sådant bedömningsorgan som avses i 28 § bedöma om identifieringstjänsten uppfyller kraven på interoperabilitet, informationssäkerhet, dataskydd och annan tillförlitlighet enligt denna lag.

Bestämmelser om Transport- och kommunikationsverkets rätt att meddela närmare föreskrifter om bedömningsgrunderna vid bedömningen av överensstämmelsen hos en

identifieringstjänst finns i 42 §. Som bedömningsgrund kan Transport- och kommunikationsverket utöver de författningar och rättsakter som avses i 1 mom. fastställa bestämmelser eller riktlinjer som antagits av Europeiska unionen eller något annat internationellt organ, publicerade och generellt eller regionalt tillämpade anvisningar för informationssäkerhet samt datasäkerhetsstandarder eller förfaranden som används allmänt.

31 §

Inspektionsberättelse

En leverantör av identifieringstjänster ska över bedömningen av överensstämmelse låta utarbeta en inspektionsberättelse som lämnas in till Transport- och kommunikationsverket.

37 §

Verksamheten vid organ för bedömning av överensstämmelse

Ett organ för bedömning av överensstämmelse får i sitt uppdrag anlita personer som inte hör till organisationen. Organet ansvarar också för det arbete som utförts av personer som organet anlitat.

Bestämmelser om de principer för god förvaltning som organ för bedömning av överensstämmelse ska följa, när det utför offentliga förvaltningsuppgifter som avses i denna lag, finns i förvaltningslagen (434/2003), lagen om offentlighet i myndigheternas verksamhet, lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003), språklagen (423/2003) och samiska språklagen (1086/2003). På personalen vid organ för bedömning av överensstämmelse och vid dotterbolag och underentreprenörer som anlitas av sådana organ tillämpas bestämmelserna om straffrättsligt tjänsteansvar när personalen utför uppgifter som avses i denna paragraf. Bestämmelser om skadeståndsansvar finns i skadeståndslagen (412/1974).

Organ för bedömning av överensstämmelse ska underrätta Transport- och kommunikationsverket om varje ändring som har betydelse för uppfyllandet av villkoren för att godkännas.

38 §

Återkallande av godkännande som organ för bedömning av överensstämmelse

Om Transport- och kommunikationsverket konstaterar att ett organ för bedömning av överensstämmelse inte uppfyller föreskrivna villkor eller att organet i väsentlig grad handlar i strid med gällande bestämmelser, ska Transport- och kommunikationsverket sätta ut en tillräcklig tidsfrist inom vilken saken ska korrigeras.

Transport- och kommunikationsverket kan återkalla ett beslut att godkänna ett bedömningsorgan om organet inte har korrigerat sin verksamhet inom den tid som satts ut enligt 1 mom. och det är fråga om en väsentlig förseelse eller försummelse.

42 §

Transport- och kommunikationsverkets föreskrifter

Transport- och kommunikationsverket får meddela närmare föreskrifter om

- 1) kraven enligt 8 § 1 mom. 4 och 5 punkten på säkerhet och tillförlitlighet hos identifieringssystemet,
- 2) innehållet i de uppgifter som ska anmälas enligt 10 § och inlämnandet av dem till Transport- och kommunikationsverket,
- 3) egenskaperna enligt 12 a § 3 mom. hos förtroendenätets tekniska gränssnitt,
- 4) när störningar som avses i 16 § är betydande och om innehållet i anmälningar enligt 16 § 1 mom. samt anmälningarnas form och inlämnandet av dem,
- 5) de behövliga uppgifter som avses i 24 § 2 mom. och som ska registreras om den inledande identifieringen av sökanden och om de handlingar eller om den elektroniska identifiering som används i den inledande identifieringen,
- 6) de grunder för bedömningen av överensstämmelsen hos en identifieringstjänst som avses i 29 §,
- 7) kompetenskraven enligt 33 § för organ för bedömning av överensstämmelse,
- 8) de uppgifter som ska ingå i en ansökan som avses i 35 § och inlämnandet av dem till Transport- och kommunikationsverket.

42 a §

Transport- och kommunikationsverkets uppgifter

Transport- och kommunikationsverket ska utöva tillsyn över efterlevnaden av denna lag, om inte något annat föreskrivs i denna lag.

Transport- och kommunikationsverket ska årligen samla och föra statistik över information om marknaden för stark autentisering och om tillhandahållandet av, tillgången till och priserna på identifieringstjänster. Den information som verket samlar hos leverantörer av identifieringstjänster ska vara behövlig för uppföljningen av regleringens konsekvenser. Informationen ska omfatta uppgifter om volymen av identifieringstransaktionerna, priserna mellan identifieringstjänsterna, detaljpriser på eller kundmängder inom identifieringstjänsterna, inkomster från identifieringstjänster eller andra motsvarande uppgifter som behövs för att statistikföringen ska vara tillförlitlig.

Transport- och kommunikationsverkets beslutanderätt omfattar inte avtalsförhållanden mellan parter eller frågor om ersättningsskyldighet.

45 §

Administrativa tvångsmedel

Transport- och kommunikationsverket kan ge en anmärkning till den som bryter mot denna lag eller bestämmelser som utfärdats eller föreskrifter eller beslut som har meddelats med stöd av den, samt ålägga denne att avhjälpa felet eller försummelsen inom skälig tid. Beslutet kan förenas med vite eller med hot om att verksamheten kommer att avbrytas helt eller delvis eller att den försummade åtgärden kommer att vidtas på den försumliges bekostnad.

45 a §

Interimistiska beslut

Om ett fel eller en försummelse som gäller denna lag eller bestämmelser som utfärdats eller föreskrifter som meddelats med stöd av den, eller en störning i datasäkerheten, omedelbart och i väsentlig grad äventyrar tillförlitligheten hos en identifieringstjänst, får Transport- och

kommunikationsverket omgående förbjuda eller avbryta tillhandahållandet av identifieringsmetoden som stark autentisering oberoende av den tidsfrist som avses i 45 §.

Transport- och kommunikationsverket ska innan det beslutar om interimistiska åtgärder ge den som är föremål för beslutet tillfälle att bli hörd, utom när detta inte kan ordnas så snabbt som ärendets brådskande natur nödvändigtvis kräver.

De interimistiska åtgärderna kan vara i kraft i högst tre månader. Beslut om interimistiska åtgärder får överklagas separat, på samma sätt som beslut som avses i 45 § 1 mom.

46 §

Inspektionsrätt

Transport- och kommunikationsverket har rätt att utföra inspektioner av leverantörer av identifieringstjänster och av leverantörernas tjänster samt av organ för bedömning av överensstämmelse som avses i 28 § och av organens verksamhet. En inspektion kan genomföras för att övervaka fullgörandet av skyldigheter enligt denna lag samt bestämmelser som utfärdats och föreskrifter och beslut som har meddelats med stöd av den. På inspektioner tillämpas 39 § i förvaltningslagen.

Transport- och kommunikationsverket förordnar en inspektör att utföra de inspektioner som avses i 1 mom. Den som utför inspektionen har rätt att hos en leverantör av identifieringstjänster och hos personer som denne anlitar granska sådan maskinvara och programvara som kan vara av betydelse vid tillsynen över efterlevnaden av denna lag och de bestämmelser som utfärdats och de föreskrifter som meddelats med stöd av den.

Leverantörer av identifieringstjänster och de personer som dessa anlitar ska för inspektionen ge en inspektör som avses i 2 mom. tillträde till alla andra utrymmen än sådana som används för boende av permanent natur.

47 §

Avgifter till Transport- och kommunikationsverket

Leverantören av identifieringstjänster eller sammanslutningen ska betala Transport- och kommunikationsverket en årlig tillsynsavgift på sammanlagt 17 000 euro för tillsynen över alla de identifieringstjänster som leverantören eller sammanslutningen tillhandahåller.

Ett organ för bedömning av överensstämmelse som godkänts enligt 34 § ska betala Transport- och kommunikationsverket en årlig tillsynsavgift på 18 000 euro.

Tillsynsavgiften ska betalas till fullt belopp också under det första verksamhetsåret, även om verksamheten inleds senare under året. Tillsynsavgiften återbetalas inte även om tjänsteleverantören upphör med sin verksamhet under året.

Tillsynsavgiften påförs av Transport- och kommunikationsverket och avgiften är direkt utsökbar. Bestämmelser om sökande av ändring i beslut om påförande av avgift finns i 49 §.

Bestämmelser om indrivning av tillsynsavgifter finns i lagen om verkställighet av skatter och avgifter. Om avgiften inte betalas senast på förfallodagen, tas årlig dröjsmålsränta ut på det obetalda beloppet enligt den räntesats som föreskrivs i 4 § i räntelagen (633/1982). I stället för dröjsmålsränta kan myndigheten ta ut en dröjsmålsavgift på fem euro om dröjsmålsräntan är mindre än detta belopp.

Bestämmelser om den avgift som tas ut för behandling av en anmälan enligt 10 § och en ansökan enligt 35 § samt för en inspektion enligt 46 § 1 mom. finns i lagen om grunderna för avgifter till staten.

49 a §

Sökande av ändring i beslut av organ för bedömning av överensstämmelse

Omprövning av ett beslut som fattats av ett organ för bedömning av överensstämmelse med stöd av denna lag får begäras hos Transport- och kommunikationsverket. Bestämmelser om begäran om omprövning finns i förvaltningslagen.

Bestämmelser om sökande av ändring i förvaltningsdomstol finns i lagen om rättegång i förvaltningsärenden.

Beslut av organ för bedömning av överensstämmelse ska iakttas trots ändringssökande, om inte den myndighet där ändring sökts bestämmer något annat.

Denna lag träder i kraft den 20 .

Lagens 7 b § och 17 § 2 mom. träder dock i kraft först den 1 januari 2027.

3.

Lag

om e-legitimation

I enlighet med riksdagens beslut föreskrivs:

1 §

Lagens syfte

Denna lag innehåller bestämmelser om e-legitimationer som används för styrkande av identiteten eller visande av bestyrkta uppgifter för finska medborgare samt utlänningar som vistas i Finland.

2 §

Definitioner

I denna lag avses med

1) *bestyrkta uppgifter* personuppgifter som en myndighet verifierat elektroniskt och som ingår i det passregister som avses i 29 § i passlagen (671/2006) eller i det identitetskortsregister som avses i 31 § i lagen om identitetskort (663/2016) samt i 4 § i denna lag avsedda andra personuppgifter som en myndighet verifierat elektroniskt,

2) *eIDAS-förordningen* Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, sådan den lyder senast ändrad genom förordning (EU) 2024/1183,

3) *förlitande part* en sådan förlitande part som avses i artikel 3.6 i eIDAS-förordningen,

4) *användare* en fysisk person som Myndigheten för digitalisering och befolkningsdata tillhandahåller ett sådant kvalificerat elektroniskt attributsintyg som avses i denna lag,

5) *teknisk utrustning* en mobil terminal eller annan motsvarande utrustning som användaren av den europeiska digitala identitetsplånboken innehar och i vilken plånboken har tagits i bruk.

6) *europeisk digital identitetsplånbok* en sådan europeisk digital identitetsplånbok som avses i artikel 3.42 i eIDAS-förordningen,

7) *kvalificerat elektroniskt attributsintyg* ett sådant kvalificerat elektroniskt attributsintyg som avses i artikel 3.45 i eIDAS-förordningen,

8) *kvalificerad tillhandahållare av betrodda tjänster* en sådan kvalificerad tillhandahållare av betrodda tjänster som avses i artikel 3.20 i eIDAS-förordningen,

9) *handling som utgör grund för en e-legitimation* ett pass som avses i 3, 3 c och 4 § i passlagen och ett identitetskort som avses i 2 § 1 mom., 14 §, 15 a § och 17 § 3 mom. i lagen om identitetskort,

10) *åldersbevis* ett attributsintyg eller motsvarande intyg som härletts ur de bestyrkta uppgifterna och med vilket användaren kan bekräfta för en förlitande part att användaren hör till en viss åldersgrupp.

3 §

E-legitimation

Med en e-legitimation kan användaren styrka sin identitet eller visa sina bestyrkta uppgifter på motsvarande sätt som med det pass eller identitetskort som utgör grund för e-legitimationen. Användaren kan få e-legitimationen som ett kvalificerat elektroniskt attributsintyg i användarens europeiska digitala identitetsplånbok.

E-legitimationen är inte ett resedokument.

4 §

Uppgifter som ingår i e-legitimationer

Uppgifterna i en e-legitimation ska motsvara uppgifterna i polisens passregister eller identitetskortsregister.

I en e-legitimation ska ingå följande uppgifter:

- 1) efternamn,
- 2) förnamn,
- 3) kön som antecknats i ett giltigt finskt pass eller identitetskort,
- 4) födelsetid,
- 5) personbeteckning,
- 6) uppgift om finskt medborgarskap,
- 7) den myndighet som utfärdat ett giltigt finskt pass eller identitetskort,
- 8) dagen för utfärdande av ett giltigt finskt pass eller identitetskort, sista giltighetsdag och nummer,
- 9) ansiktsbild som har förts in i pass- eller identitetskortsregistret.

Ett kvalificerat elektroniskt attributsintyg som tillhandahålls på basis av de uppgifter som avses i 2 mom. kan också innehålla åldersbevis.

Bestämmelser om andra uppgifter i ett kvalificerat elektroniskt attributsintyg finns i bilaga V till eIDAS-förordningen.

5 §

Förutsättningar för att få tillgång till e-legitimation

En finsk medborgare samt en utlänning som vistas i Finland kan få tillgång till e-legitimation. Personen ska ha en giltig handling som utgör grund för e-legitimationen samt en europeisk digital identitetsplånbok som har tagits i bruk.

En förutsättning för att få tillgång till e-legitimation är att Myndigheten för digitalisering och befolkningsdata har fjärrläst uppgifterna i den tekniska delen av den handling som utgör grund för den digitala identiteten och att uppgifterna motsvarar identifieringsuppgifterna för den fysiska personen i personens europeiska digitala identitetsplånbok.

6 §

Giltigheten för e-legitimationer

En e-legitimation kan vara i kraft lika länge som den handling som utgör grund för den digitala identiteten är i kraft.

Om den handling som utgör grund för e-legitimationen dras in på den grunden att innehavaren har anmält att den har förkommit eller stulits, fortsätter rätten till e-legitimationen 30 dygn efter det att handlingen som utgör grund för e-legitimationen har dragits in, om inte något annat följer av 12 §.

En e-legitimation kan användas som ett kvalificerat elektroniskt attributsintyg samtidigt på två separata tekniska utrustningar.

Giltighetstiden för ett kvalificerat elektroniskt attributsintyg för en e-legitimation bestäms av Myndigheten för digitalisering och befolkningsdata.

7 §

Behöriga myndigheter, myndighetsuppgifter och uppgiftsbehandling

När polisen eller någon annan behörig myndighet utfärdar en handling som utgör grund för en e-legitimation beviljar den samtidigt rätt att få tillgång till en e-legitimation.

Polisen lämnar ut de uppgifter som avses i 4 § 2 mom. till Myndigheten för digitalisering och befolkningsdata för tillhandahållande av ett kvalificerat elektroniskt attributsintyg. Innan uppgifter lämnas ut ska polisen försäkra sig om att uppgifterna är korrekta.

Myndigheten för digitalisering och befolkningsdata ska tillhandahålla ett kvalificerat elektroniskt attributsintyg med iakttagande av eIDAS-förordningen. Dessutom ska Myndigheten för digitalisering och befolkningsdata tillhandahålla de certifikat som behövs för att säkerställa äktheten och integriteten hos uppgifterna i ett kvalificerat elektroniskt attributsintyg och stämpla uppgifterna med en kvalificerad elektronisk stämpel.

I 4 § 2 mom. avsedda uppgifter som polisen lämnar ut ska Myndigheten för digitalisering och befolkningsdata behandla i Finland.

8 §

Register över e-legitimationer

För skötseln av de uppgifter som föreskrivs i denna lag för polisen ett register över e-legitimationer. Registret innehåller de uppgifter som avses i 4 § 2 mom. i fråga om de personer som har tagit i bruk en e-legitimation. Dessutom innehåller registret uppgifter om e-legitimationer och behandlingen av dem vid polisen.

Bestämmelser om behandling av uppgifter i registret finns i 11–15 § i lagen om behandling av personuppgifter i polisens verksamhet (616/2019). Bestämmelser om utlämnande och radering av uppgifter i registret finns i 4 kap. och i 38 § i den lagen.

9 §

Register över kvalificerade elektroniska attributsintyg

För skötseln av de uppgifter som föreskrivs i denna lag för Myndigheten för digitalisering och befolkningsdata ett register över kvalificerade elektroniska attributsintyg för e-legitimationer och europeiska digitala identitetsplånböcker för vilka ett kvalificerat elektroniskt attributsintyg har tagits i bruk.

10 §

Polisens behörighet att dra in rätten till e-legitimation

Polisen ska dra in den rätt till en e-legitimation som avses i 7 § 1 mom. om e-legitimationen används av någon annan än användaren eller om säkerheten vid användningen av den annars har allvarligt äventyrats.

Polisen ska utan dröjsmål underrätta Myndigheten för digitalisering och befolkningsdata om en indragning med stöd av 1 mom.

Den indragna rätten till en e-legitimation kan inte återinföras.

11 §

Indragning av kvalificerade elektroniska attributsintyg

Myndigheten för digitalisering och befolkningsdata ska dra in ett kvalificerat elektroniskt attributsintyg om det används av någon annan än användaren.

Myndigheten för digitalisering och befolkningsdata ska dra in ett kvalificerat elektroniskt attributsintyg om polisen med stöd av 10 § 1 mom. har dragit in rätten till e-legitimationen.

Myndigheten för digitalisering och befolkningsdata ska dra in ett kvalificerat elektroniskt attributsintyg om intyget innehåller ett uppenbart fel. Myndigheten för digitalisering och befolkningsdata ska efter en indragning på grund av ett uppenbart fel utan dröjsmål tillhandahålla användaren ett nytt kvalificerat elektroniskt attributsintyg.

Ett indraget kvalificerat elektroniskt attributsintyg kan inte återinföras.

12 §

Giltighetens upphörande

En e-legitimation och de kvalificerade elektroniska attributsintyg som hänför sig till den upphör utan särskilt beslut att gälla när

1) till personen lämnas ut en ny handling som utgör grund för e-legitimationen och som har använts för fjärravläsning av uppgifter enligt 5 § 2 mom.,

2) den handling som utgör grund för e-legitimationen dras in av någon annan orsak än en sådan som avses i 6 § 2 mom.,

3) identifieringsuppgifterna i e-legitimationen och de identifieringsuppgifter för en fysisk person som utfärdats för den europeiska digitala identitetsplånboken inte motsvarar varandra,

4) användaren återkallar giltigheten för den europeiska digitala identitetsplånboken.

Myndigheten för digitalisering och befolkningsdata ska i andra situationer än de som avses i 1 mom. 4 punkten utan dröjsmål informera användaren om att giltigheten för ett kvalificerat elektroniskt attributsintyg upphör.

13 §

Avvikelse från förvaltningslagens förfarandebestämmelser

Med avvikelse från förvaltningslagen (434/2003) ges inte något förvaltningsbeslut eller någon besväransvisning eller någon upplysning om besvärsförbud vid beviljande av rätten att få tillgång till en e-legitimation enligt 7 § 1 mom. i denna lag.

Med avvikelse från förvaltningslagen ges inte något förvaltningsbeslut eller någon besväransvisning eller någon upplysning om besvärsförbud vid indragning av ett kvalificerat elektroniskt attributsintyg med stöd av 11 § 2 mom. i denna lag.

14 §

Besvärsförbud och sökande av ändring

I situationer som avses i 12 §, när det är fråga om att en e-legitimation och de kvalificerade elektroniska attributsintyg som hänför sig till den upphör att gälla, får ändring inte sökas genom besvär.

Ändring i avgöranden som avses i 13 § får inte sökas genom besvär.

Bestämmelser om sökande av ändring i förvaltningsdomstol finns i lagen om rättegång i förvaltningsärenden (808/2019).

15 §

Ikraftträdande

Denna lag träder i kraft den 20 .
Myndigheterna ska anpassa sin verksamhet till denna lag senast den 24 december 2026.

4.

Lag

om ändring av 3 och 6 § i lagen om tillhandahållande av digitala tjänster

I enlighet med riksdagens beslut
ändras i lagen om tillhandahållande av digitala tjänster (306/2019) 3 § 1 mom. 4 punkten och 6 § 2 mom. som följer:

3 §

Lagens tillämpningsområde

Denna lag tillämpas

4) på identifieringstjänster som tillhandahålls av sådana leverantörer av identifieringstjänster som finns införda i det register som avses i 12 § i lagen om stark autentisering (617/2009) samt på sådana delar av digitala tjänster som används via en i 3 § 1 mom. 8 punkten i lagen om förvaltningens gemensamma stödtjänster för e-tjänster (571/2016) avsedd samlad förvaltningstjänst för internetbetalning och med vilka betalningsuppdrag kan skötas,

6 §

Elektronisk identifiering av tjänsteanvändarna

Om det är möjligt att få se och använda sekretessbelagt datainnehåll i en digital tjänst, ska tjänsteanvändaren identifieras med hjälp av en sådan tjänst för identifiering av fysiska personer som avses i 3 § 1 mom. 4 punkten i lagen om förvaltningens gemensamma stödtjänster för e-tjänster, med hjälp av stark autentisering som avses i 2 § 1 punkten i lagen om stark autentisering, med hjälp av en europeisk digital identitetsplånbok som avses i 2 § 1 punkten i lagen om vissa tjänster som möjliggör gränsöverskridande e-tjänster (/) eller av vägande och motiverande skäl med hjälp av någon annan motsvarande informationssäker identifieringstjänst.

Denna lag träder i kraft den 20 .

5.

Lag

om ändring av 3 § i lagen om förvaltningens gemensamma stödtjänster för e-tjänster

I enlighet med riksdagens beslut
ändras i lagen om förvaltningens gemensamma stödtjänster för e-tjänster (571/2016) 3 § 1 mom. 4 och 5 punkten samt 3 § 2 mom., av dem 3 § 2 mom. sådant det lyder i lag 1314/2019, som följer:

3 §

Stödtjänster

De gemensamma stödtjänsterna för e-tjänster omfattar

4) en sådan tjänst för identifiering av fysiska personer som identifierar en fysisk person som använder den offentliga förvaltningens e-tjänster med hjälp av en tjänst som tillhandahålls av en sådan leverantör av identifieringstjänster som avses i lagen om stark autentisering (617/2009), administrerar identifieringstransaktionen och till användarorganisationen lämnar ut identifieringsuppgifter om en person ur befolkningsdatasystemet,

5) sådana identifieringstjänster och samlade förvaltningstjänster för identifiering där även någon annan metod för identifiering än sådan stark autentisering som avses i lagen om stark autentisering kan användas,

I tjänsten för identifiering av fysiska personer får en person identifieras också med en sådan metod för identifiering som hör till de medel för elektronisk identifiering som ska erkännas ömsesidigt enligt artiklarna 5f eller 6 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, sådan den lyder senast ändrad genom förordning (EU) 2024/1183. I det fallet får det ur tjänsten för identifiering av fysiska personer till användarorganisationen lämnas ut också sådana identifieringsuppgifter om en person som i samband med identifieringstransaktionen förmedlas från en annan medlemsstat.

Denna lag träder i kraft den 20 .

6.

Lag

om ändring av 1 § i lagen om verkställighet av böter

I enlighet med riksdagens beslut
ändras i lagen om verkställighet av böter (672/2002) 1 § 2 mom. 63 punkten, sådan den lyder
i lag 1379/2025, och
fogas till 1 § 2 mom., sådant det lyder i lagarna 416/2025, 860/2025, 979/2025, 1080/2025,
1149/2025 och 1379/2025, en ny 64 punkt som följer:

1 §

Lagens tillämpningsområde

Denna lag innehåller bestämmelser om verkställighet av följande administrativa påföljder av
straffkaraktär:

- 63) påföljdsavgifter enligt 4 kap. i lagen om tillsyn över vissa system för artificiell intelligens
(1377/2025),
64) påföljdsavgift enligt 42–46 § i lagen om vissa tjänster som möjliggör gränsöverskridande
e-tjänster (/).

Denna lag träder i kraft den 20 .

7.

Lag

om ändring av lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata

I enlighet med riksdagens beslut

ändras i lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata (661/2009) 2 § 2 mom. 2 punkten, 28 § 1 mom., 43 § 2 mom. 1 och 2 punkten, 62 §, 63 § 2 mom. 1 punkten, 66 § 2 och 3 mom. och 67 § 1 mom., sådana de lyder, 2 § 2 mom. 2 punkten, 28 § 1 mom. och 66 § 2 och 3 mom. i lag 55/2019, 43 § 2 mom. 1 punkten, 63 § 2 mom. 1 punkten och 67 § 1 mom. i lag 1175/2019, 43 § 2 mom. 2 punkten i lag 538/2016 och 62 § i lagarna 538/2016 och 1175/2019, som följer:

2 §

Lagens tillämpningsområde

Om inte något annat föreskrivs i denna lag, ska följande lagar och rättsakter tillämpas:

2) i fråga om certifierad elektronisk kommunikation och behandling av uppgifter i det certifikatregister som avses i denna lag, lagen om stark autentisering (617/2009).

28 §

Allmänna förutsättningar för utlämnande av uppgifter

Uppgifter i befolkningsdatasystemet får lämnas ut endast om förutsättningarna för utlämnande av uppgifter enligt denna lag är uppfyllda. Det krävs att de uppgifter som lämnas ut ur befolkningsdatasystemet behövs för det ändamål för vilket de lämnas ut. När uppgifter som hör till kategorierna av särskilda personuppgifter lämnas ut ska det säkerställas att mottagaren har rätt att behandla uppgifterna med stöd av dataskyddsförordningen eller dataskyddslagen (1050/2018).

43 §

Utlämnande av identifieringsuppgifter

Elektroniska kommunikationskoder som registrerats i befolkningsdatasystemet får lämnas ut endast om

1) koden används som en uppgift som identifierar innehavaren av ett certifikat eller innehavaren av identifieringsuppgifter för en fysisk person i samband med produktion av tjänster eller prestationer som baserar sig på användningen av medborgarcertifikat eller andra certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för fysiska personer eller på identifieringsuppgifter för fysiska personer som Myndigheten för digitalisering och

befolkningsdata utfärdar med stöd av lagen om vissa tjänster som möjliggör gränsöverskridande e-tjänster (/), eller

2) en annan än i 1 punkten avsedd i Finland etablerad certifikatutfärdare använder koden som en uppgift som identifierar innehavaren av certifikatet i certifikat som avses i lagen om stark autentisering eller i motsvarande certifikat som används i identifieringssyfte.

62 §

Uppgifter som ska ingå i certifikat för certifierad elektronisk kommunikation

Bestämmelser om vilka uppgifter som ska ingå i medborgarcertifikat och andra certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för fysiska personer finns i lagen om stark autentisering och i EU:s förordning om elektronisk identifiering. Medborgarcertifikat ska innehålla en elektronisk kommunikationskod som identifierar innehavaren av certifikatet. Andra certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för fysiska personer ska innehålla en elektronisk kommunikationskod som identifierar innehavaren av certifikatet eller någon annan identifieringsuppgift som identifierar personen och som inte innehåller information om personen. Även andra nödvändiga tekniska uppgifter som behövs vid användningen av ett certifikat kan ingå i medborgarcertifikat och andra certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för fysiska personer. Beslut om dessa uppgifter fattas av Myndigheten för digitalisering och befolkningsdata.

En elektronisk kommunikationskod kan också ingå i andra i lagen om stark autentisering avsedda certifikat för fysiska personer som en uppgift som identifierar innehavaren av certifikatet.

63 §

Tekniska identifieringskoder och elektroniska kommunikationskoder samt skapande av dessa

Myndigheten för digitalisering och befolkningsdata ska ändra en teknisk identifieringskod till en individuell elektronisk kommunikationskod när

1) ett medborgarcertifikat eller ett annat certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för fysiska personer eller identifieringsuppgifter för fysiska personer som Myndigheten för digitalisering och befolkningsdata utfärdar med stöd av lagen om vissa tjänster som möjliggör gränsöverskridande e-tjänster första gången utfärdas för en person, eller

66 §

Ansökan om och utfärdande av medborgarcertifikat

På ansökan om medborgarcertifikat som ingår i ett identitetskort tillämpas lagen om identitetskort. På ansökan om medborgarcertifikat som ingår i en annan myndighetshandling eller ett tekniskt underlag tillämpas förfarandet enligt 67 § 2 och 3 mom. i denna lag, de krav i dataskyddsförordningen och dataskyddslagen som gäller behandlingen av personuppgifter samt de krav i lagen om stark autentisering som gäller utfärdande av certifikat.

Den som tar emot ansökan ska iaktta de krav i dataskyddsförordningen och dataskyddslagen som gäller behandlingen av personuppgifter och de krav i lagen om stark autentisering och i EU:s förordning om elektronisk identifiering som gäller utfärdande av certifikat.

Ansökan om och utfärdande av andra certifikat

Andra certifikat för fysiska personer som Myndigheten för digitalisering och befolkningsdata producerar och som inte är medborgarcertifikat kan utfärdas endast för finska medborgare samt för utlänningar som enligt lagen om hemkommun är stadigvarande bosatta i Finland och vars uppgifter har registrerats i befolkningsdatasystemet och vars identitet har kunnat konstateras på ett tillförlitligt sätt. Andra certifikat än medborgarcertifikat som Myndigheten för digitalisering och befolkningsdata producerar för fysiska personer kan av särskilda och motiverade skäl också beviljas personer vars identitet har kunnat konstateras tillförlitligt även om de inte uppfyller övriga ovannämnda förutsättningar för att få certifikat. Sådana certifikat kan på sökandens begäran ingå i handlingar, kort och tekniska underlag som används vid elektronisk kommunikation och som utfärdas av en myndighet, ett företag eller en organisation. Myndigheten för digitalisering och befolkningsdata kan komma överens med en myndighet, ett företag eller en organisation som utfärdar handlingar eller tekniska underlag om att ansökningar om certifikat personligen kan lämnas in till myndigheten, företaget eller organisationen för vidarebefordran till Myndigheten för digitalisering och befolkningsdata. Myndigheten för digitalisering och befolkningsdata ska då se till att den som tar emot ansökan iakttar vad som i dataskyddsförordningen och dataskyddslagen föreskrivs om behandlingen av personuppgifter och vad som i lagen om stark autentisering och i EU:s förordning om elektronisk identifiering föreskrivs om utfärdande av certifikat.

Denna lag träder i kraft den 20 .

8.

Lag

om ändring av 8 och 65 § i lagen om behandling av kunduppgifter inom social- och hälsovården

I enlighet med riksdagens beslut
ändras i lagen om behandling av kunduppgifter inom social- och hälsovården (703/2023) 8 § 2 mom. och 65 § 3 mom., av dem 65 § 3 mom. sådant det lyder i lag 764/2025, som följer:

8 §

Identifiering av dem som deltar i behandlingen av kunduppgifter

Tjänstetillhandahållaren, apoteket, Folkpensionsanstalten samt producenten av informationssystemtjänsten och tillverkaren av informationssystemet samt mellanhanden ska kontrollera att identifieringsverktygen för personer som behandlar kunduppgifter och som används för identifiering av informationstekniska enheter är i kraft med iakttagande av 25 § 4–6 mom. i lagen om stark autentisering (617/2009), nedan *autentiseringslagen*.

65 §

De riksomfattande informationssystemtjänsterna inom social- och hälsovården

Myndigheten för digitalisering och befolkningsdata är certifikatutfärdare i enlighet med autentiseringslagen för yrkesutbildade personer inom social- och hälsovården och annan personal inom social- och hälsovården, tjänstetillhandahållare inom social- och hälsovården samt organisationer som deltar i tillhandahållandet av dessa tjänster, deras personal och datatekniska enheter. Myndigheten för digitalisering och befolkningsdata har rätt att för skötseln av dessa uppgifter av Tillstånds- och tillsynsverket få den information som behövs för utfärdande och återkallande av certifikat, för certifikat, för det tekniska underlaget för certifikat och för sändande av certifikat, ur centralregistret över yrkesutbildade personer inom hälso- och sjukvården som verket upprätthåller.

Denna lag träder i kraft den 20 .

9.

Lag

om ändring av 3 kap. 11 § i lagen om förhindrande av penningtvätt och av finansiering av terrorism

I enlighet med riksdagens beslut
ändras i lagen om förhindrande av penningtvätt och av finansiering av terrorism (444/2017)
3 kap. 11 § 3 punkten som följer:

3 kap.

Kundkontroll

11 §

Skärpta åtgärder för kundkontroll vid identifiering på distans

Om kunden inte är närvarande vid identifieringen och identitetskontrollen (*identifiering på distans*) ska den rapporteringsskyldiga vidta följande åtgärder för att minska risken för penningtvätt och finansiering av terrorism:

3) kontrollera en kunds identitet med ett identifieringsverktyg enligt lagen om stark autentisering (617/2009) eller med ett kvalificerat certifikat för elektroniska underskrifter enligt artikel 28 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, sådan den lyder senast ändrad genom förordning (EU) 2024/1183, eller med någon annan elektronisk identifieringsteknik som är datasäker och bevislig.

Denna lag träder i kraft den 20 .

10.

Lag

om ändring av 9 a kap. 1 § i jordabalken

I enlighet med riksdagens beslut
ändras i jordabalken (540/1995) 9 a kap. 1 § 1 mom., sådant det lyder i lag 536/2016, som följer:

9 a kap.

Elektroniska ärendehanteringssystem och deras användning

1 §

Användning av ärendehanteringssystem och elektronisk identifiering i ett ärendehanteringssystem

En förutsättning för att upprätta och godkänna elektroniska dokument i ett ärendehanteringssystem samt för att i övrigt använda ärendehanteringssystemet är att användaren identifieras på ett tillförlitligt sätt med hjälp av en sådan identifieringsmetod, tillhandahållen av en leverantör av tjänster för stark autentisering, som avses i lagen om stark autentisering (617/2009) eller ett sådant kvalificerat certifikat för elektronisk underskrift som föreskrivs i artikel 28 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, sådan den lyder senast ändrad genom förordning (EU) 2024/1183, eller med hjälp av någon annan identifieringsteknik som är datatekniskt tillförlitlig och bevislig.

Denna lag träder i kraft den 20 .

11.

Lag

om ändring av 7 § i lagen om medborgarinitiativ

I enlighet med riksdagens beslut
ändras i lagen om medborgarinitiativ (12/2012) 7 § 1 mom. 1 punkten, sådan den lyder i lag 1276/2019, som följer:

7 §

Tekniska krav på elektroniskt förfarande

Elektronisk insamling av stödförklaringar i ett datanät ska ske med utnyttjande av datasystem som har godkänts av Transport- och kommunikationsverket. En förutsättning för godkännande är att

1) insamlingen av stödförklaringar sker genom utnyttjande av sådan stark autentisering som avses i lagen om stark autentisering (617/2009),

Denna lag träder i kraft den 20 . _____

12.

Lag

om ändring av 4 § i lagen om förfarandet vid rådgivande folkomröstningar i velfärdsområden och kommuner

I enlighet med riksdagens beslut
ändras i lagen om förfarandet vid rådgivande folkomröstningar i velfärdsområden och
kommuner (656/1990) 4 § 3 mom., sådant det lyder i lag 652/2021, som följer:

4 §

Initiativ till folkomröstning

Insamlingen av stödförklaringar på elektronisk väg i ett datanät ska ske med hjälp av stark
autentisering enligt lagen om stark autentisering (617/2009).

Denna lag träder i kraft den 20 .

13.

Lag

om ändring av 15 och 26 § i lagen om fonderna inom området för inrikes frågor under programperioden 2021–2027

I enlighet med riksdagens beslut
ändras i lagen om fonderna inom området för inrikes frågor under programperioden 2021–2027 (1125/2021) 15 § 4 mom. och 26 § 3 mom., sådana de lyder i lag 1293/2022, som följer:

15 §

Ansökan om understöd

På undertecknandet av ansökan tillämpas vad som i lagen om stark autentisering (617/2009) föreskrivs om identifiering och autentisering av en person. Om ansökan har gjorts på en blankett som godkänts av den förvaltande myndigheten, ska ansökan undertecknas.

26 §

E-tjänst- och behandlingssystemet för programmet för fonderna inom området för inrikes frågor samt behandling av uppgifter

Varje användare av informationssystemet ska identifiera sig med hjälp av sådan stark autentisering som avses i 2 § 1 punkten i lagen om stark autentisering.

Denna lag träder i kraft den 20 .

14.

Lag

om ändring av lagen om identitetskort

I enlighet med riksdagens beslut
ändras i lagen om identitetskort (663/2016) 11 § 4 mom. och
fogas till lagen en ny 1 a § som följer:

1 a §

E-legitimation

I identitetskort som avses i 2 § 1 mom., 14 och 15 a § samt 17 § 3 mom. ingår en rätt att få tillgång till en e-legitimation som avses i lagen om e-legitimation (/).

11 §

Identifiering av sökanden och verifiering av sökandens identitet

Elektronisk kommunikation förutsätter ett sådant identifieringsverktyg som avses i lagen om stark autentisering (617/2009).

Denna lag träder i kraft den 20 .
Rätten att få tillgång till en e-legitimation ingår i sådana identitetskort som avses i 1 a § och som har utfärdats före ikraftträdandet av denna lag.

15.

Lag

om ändring av 3 § i partilagen

I enlighet med riksdagens beslut
ändras i partilagen (10/1969) 3 § 1 mom., sådant det lyder i lag 904/2020, som följer:

3 §

Registreringsansökan

En förening kan göra en registreringsansökan i en webbtjänst som drivs av justitieministeriet, i vilken det används stark autentisering enligt lagen om stark autentisering (617/2009), eller på annat sätt skriftligen.

Denna lag träder i kraft den 20 .

16.

Lag

om ändring av 52 § i lagen om finansiering av projekt inom regionutveckling och Europeiska unionens regional- och strukturpolitik

I enlighet med riksdagens beslut
ändras i lagen om finansiering av projekt inom regionutveckling och Europeiska unionens regional- och strukturpolitik (757/2021) 52 § som följer:

52 §

Stark autentisering vid användning av informationssystemet för Europeiska unionens regional- och strukturpolitiska program

Varje användare av det informationssystem som avses i 50 § ska identifiera sig med hjälp av stark autentisering. Bestämmelser om stark autentisering finns i lagen om stark autentisering (617/2009). Offentliga uppgifter som avses i 54 § 2 mom. får dock granskas utan stark autentisering.

Denna lag träder i kraft den 20 . _____

17.

Lag

om ändring av passlagen

I enlighet med riksdagens beslut
ändras i passlagen (671/2006) 6 § 4 mom., sådant det lyder i lag 966/2014, och
fogas till lagen en ny 3 d § som följer:

3 d §

E-legitimation

I pass som avses i 3 och 3 c samt 4 § ingår en rätt att få tillgång till en e-legitimation som avses i lagen om e-legitimation (/).

6 §

Ansökan om pass

Till ansökan ska fogas sökandens ansiktsbild, på vilken sökanden utan svårighet kan kännas igen. Sökanden ska som identifieringshandling uppvisa en giltig handling där sökandens identitet framgår. Om sökanden inte kan uppvisa en identifieringshandling, utförs identifieringen av den myndighet som utfärdar passet. Elektronisk kommunikation förutsätter ett sådant identifieringsverktyg som avses i lagen om stark autentisering (617/2009).

Denna lag träder i kraft den 20 .
Rätten att få tillgång till en e-legitimation ingår också i pass som har utfärdats före ikraftträdandet av denna lag och som avses i 3 d §.

18.

Lag

om ändring av 31 § i lagen om stödjande av landsbygdens utveckling under finansieringsperioden 2023–2027

I enlighet med riksdagens beslut
ändras i lagen om stödjande av landsbygdens utveckling under finansieringsperioden 2023–2027 (1325/2022) 31 § 1 mom. enligt följande:

31 §

Ansökan om stöd

Ansökan om stöd görs elektroniskt via en nättjänst som utgör en del av den informationsresurs för livsmedelsförvaltningen som avses i lagen om livsmedelsförvaltningens informationsresurs (560/2021). Sökanden identifieras genom stark autentisering i enlighet med lagen om stark autentisering (617/2009).

Denna lag träder i kraft den 20 . _____

19.

Lag

om ändring av 12 § i lagen om verkställighet av vissa av Europeiska unionens jordbruksstöd och vissa nationella jordbruksstöd

I enlighet med riksdagens beslut
ändras i lagen om verkställighet av vissa av Europeiska unionens jordbruksstöd och vissa nationella jordbruksstöd (1334/2022) 12 § 1 mom. som följer:

12 §

Ansökan om stöd

Ansökningar om stöd görs elektroniskt i en nättjänst som utgör en del av livsmedelsförvaltningens informationsresurs, som avses i lagen om livsmedelsförvaltningens informationsresurs (560/2021). Sökanden eller sökandena identifieras genom stark autentisering i enlighet med lagen om stark autentisering (617/2009). Vad som i denna lag föreskrivs om ansökan om stöd gäller även anmälan som gäller stöd.

Denna lag träder i kraft den 20 . _____

20.

Lag

om ändring av 32 § i lagen om det nationella genomförandet av Europeiska unionens gemensamma fiskeripolitik

I enlighet med riksdagens beslut
ändras i lagen om det nationella genomförandet av Europeiska unionens gemensamma
fiskeripolitik (1048/2016) 32 § 2 mom., sådant det lyder i lag 3/2023, som följer:

32 §

Innehavarens rätt att använda uppgifterna i fiskekvotsregistret

För att ta del av uppgifter samt för överföringar i den elektroniska tjänsten krävs det sådan
stark autentisering som avses i 2 § 1 punkten i lagen om stark autentisering (617/2009).

Denna lag träder i kraft den 20 .

21.

Lag

om ändring av 41 § i lagen om behandling av personuppgifter i polisens verksamhet

I enlighet med riksdagens beslut
ändras i lagen om behandling av personuppgifter i polisens verksamhet (616/2019) 41 § 2 mom. som följer:

41 §

Tillgödoseende av den registrerades rätt till insyn

En registrerad som vill utöva sin rätt till insyn ska framställa en personlig begäran om detta till den personuppgiftsansvarige eller någon annan i 1 mom. avsedd polisenhet samt styrka sin identitet. En begäran kan också framställas genom att använda sådan stark autentisering som avses i lagen om stark autentisering (617/2009), om en sådan tjänst är tillgänglig.

Denna lag träder i kraft den 20 .

22.

Lag

om ändring av 35 § i lagen om behandling av personuppgifter inom Tullen

I enlighet med riksdagens beslut
ändras i lagen om behandling av personuppgifter inom Tullen (650/2019) 35 § 2 mom. som följer:

35 §

Tillgodoseende av den registrerades rätt till insyn

En registrerad som vill utöva sin rätt till insyn ska framställa en personlig begäran om detta till den personuppgiftsansvarige eller en i 1 mom. avsedd verksamhetsenhet inom Tullen samt styrka sin identitet. En begäran kan också framställas genom att använda sådan stark autentisering som avses i lagen om stark autentisering (617/2009), om en sådan tjänst är tillgänglig.

Denna lag träder i kraft den 20 . _____

23.

Lag

om ändring av 29 § i lagen om strukturstöd till jordbruket

I enlighet med riksdagens beslut
ändras i lagen om strukturstöd till jordbruket (1476/2007) 29 § 1 mom., sådant det lyder i lag
1328/2022, som följer:

29 §

Ansökan om stöd

Stöd ska sökas elektroniskt via en nättjänst som utgör en del av den informationsresurs för
livsmedelsförvaltningen som avses i lagen om livsmedelsförvaltningens informationsresurs
(560/2021). Sökanden identifieras genom stark autentisering i enlighet med lagen om stark
autentisering (617/2009).

Denna lag träder i kraft den 20 .

24.

Lag

om ändring av 50 § i lagen om behandling av personuppgifter vid Gränsbevakningsväsendet

I enlighet med riksdagens beslut
ändras i lagen om behandling av personuppgifter vid Gränsbevakningsväsendet (639/2019)
50 § 2 mom. som följer:

50 §

Tillgodoseende av den registrerades rätt till insyn

En registrerad som vill utöva sin rätt till insyn ska framställa en personlig begäran om detta till den personuppgiftsansvarige eller någon annan i 1 mom. avsedd myndighet samt styrka sin identitet. En begäran kan också framställas med användning av stark autentisering enligt lagen om stark autentisering (617/2009), om en sådan tjänst är tillgänglig.

Denna lag träder i kraft den 20 .

25.

Lag

om ändring av 70 a § i lagen om en marknadsordning för jordbruksprodukter

I enlighet med riksdagens beslut
ändras i lagen om en marknadsordning för jordbruksprodukter (999/2012) 70 a § 1 mom.,
sådant det lyder i lag 1336/2022, som följer:

70 a §

Elektronisk ansökan

Det kan förutsättas att stöd söks elektroniskt i en nättjänst som utgör en del av livsmedelsförvaltningens informationsresurs, som avses i lagen om livsmedelsförvaltningens informationsresurs. Sökanden identifieras genom stark autentisering i enlighet med lagen om stark autentisering (617/2009). Genom förordning av statsrådet föreskrivs om sådana stöd enligt denna lag beträffande vilka ansökan kan göras bara på det sätt som avses i denna paragraf.

Denna lag träder i kraft den 20 . _____

26.

Lag

om ändring av konsumentkyddslagen

I enlighet med riksdagens beslut
ändras i konsumentkyddslagen (38/1978) 6 kap. 12 c § 1 mom., 7 kap. 15 § 1 mom., 7 a kap. 33 § 2 mom. och 10 kap. 6 § 1 mom., sådana de lyder, 6 kap. 12 c § 1 mom. och 7 kap. 15 § 1 mom. i lag 449/2023, 7 a kap. 33 § 2 mom. i lag 851/2016 samt 10 kap. 6 § 1 mom. i lag 227/2011, som följer:

6 kap.

Hemförsäljning och distansförsäljning

12 c §

Kontroll av identiteten hos konsumenter och bevarande av uppgifterna om kontrollen i vissa fall

Om konsumenten vid köp av nyttigheter på nätet väljer ett betalningssätt som innebär betalningsanstånd, ska den näringsidkare som tillhandahåller betalningssättet i fråga kontrollera konsumentens identitet i samband med godkännandet av betalningssättet med hjälp av en identifieringsmetod som uppfyller kraven på system för elektronisk identifiering enligt 8 § i lagen om stark autentisering (617/2009) eller kraven på stark kundautentisering enligt 8 § 24 punkten och 85 c § 4 mom. i betaltjänstlagen (290/2010).

7 kap.

Konsumentkrediter

15 §

Kontroll av kreditsökandens identitet

I samband med att ett avtal om konsumentkredit ingås och i samband med att kreditbeloppet eller kreditgränsen höjs ska kreditgivaren noggrant kontrollera konsumentens identitet. Om identiteten kontrolleras elektroniskt, ska kreditgivaren använda en identifieringsmetod som uppfyller kraven i 8 § i lagen om stark autentisering eller kraven på stark kundautentisering i 8 § 24 punkten och 85 c § 4 mom. i betaltjänstlagen.

7 a kap.

Konsumentkrediter som har samband med bostadsegendom

33 §

Tillsynsmyndigheter

Tillsynsmyndigheterna ska samarbeta på lämpligt sätt. När efterlevnaden av 7 kap. 15 § övervakas med stöd av 31 § i detta kapitel ger Transport- och kommunikationsverket på begäran tillsynsmyndigheten ett utlåtande om huruvida den metod för elektronisk identitetskontroll som kreditgivaren använder uppfyller kraven i 8 § i lagen om stark autentisering.

10 kap.

Tidsdelat boende och långfristiga semesterprodukter

6 §

Avtalets form och språk

Avtalet ska upprättas skriftligt och undertecknas av parterna. Konsumenten ska få ett exemplar av avtalet. Avtalet kan upprättas även elektroniskt så att konsumenten kan bevara och återge avtalet i oförändrad form. På elektronisk signering av avtalet tillämpas Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, sådan den lyder senast ändrad genom förordning (EU) 2024/1183. I 7 och 7 a kap. i denna lag föreskrivs det om formen för och innehållet i eventuella kreditavtal som anknyter till huvudavtalet.

Denna lag träder i kraft den 20 .

27.

Lag

om ändring av 48 § i lagen om strukturstöd för renhushållning och naturnäringar

I enlighet med riksdagens beslut
ändras i lagen om strukturstöd för renhushållning och naturnäringar (986/2011) 48 § 1 mom.,
sådant det lyder i lag 1329/2022, som följer:

48 §

Ansökan om stöd

Stöd ska sökas elektroniskt via en nättjänst som utgör en del av den informationsresurs för livsmedelsförvaltningen som avses i lagen om livsmedelsförvaltningens informationsresurs (560/2021). Sökanden identifieras genom stark autentisering i enlighet med lagen om stark autentisering (617/2009). En stödansökan kan också göras med en blankett som fastställts för ändamålet. Blanketten kan lämnas in via en skyddad e-postförbindelse i form av en ifyllbar pdf-blankett eller i pappersformat. Det sistnämnda ska undertecknas.

Denna lag träder i kraft den 20 . _____

28.

Lag

om ändring av 119 a § i skjutvapenlagen

I enlighet med riksdagens beslut

ändras i skjutvapenlagen (1/1998) 119 a §, sådan den lyder i lag 89/2020, som följer:

119 a §

Elektroniska tjänster

I 22 och 25 §, 42 § 2 mom., 42 c § 1 och 3 mom., 70 § 3 mom. och 89 § avsedda elektroniska tjänster förutsätter ett identifieringsverktyg som avses i lagen om stark autentisering (617/2009).

Denna lag träder i kraft den 20 .

29.

Lag

om ändring av 84 § i fordonslagen

I enlighet med riksdagens beslut
ändras i fordonslagen (82/2021) 84 § 3 mom. som följer:

84 §

Bestämmelser om registreringsanmälan

Den som gör en registreringsanmälan ska identifieras när denne personligen lämnar in en anmälan till en avtalsregistrerare. Den som gör anmälan i den elektroniska tjänst som tillhandahålls av den som utför registreringar ska identifieras med sådan stark autentisering som avses i 2 § 1 punkten i lagen om stark autentisering (617/2009).

Denna lag träder i kraft den 20 .

30.

Lag

om ändring av 39 § i konkurrenslagen

I enlighet med riksdagens beslut
ändras i konkurrenslagen (948/2011) 39 § 1 mom. 9 punkten, sådan den lyder i lag 721/2019,
som följer:

39 §

Informationsutbytet mellan myndigheter

Konkurrens- och konsumentverket kan på eget initiativ, trots bestämmelserna om sekretess, om det behövs lämna ut en uppgift eller handling som verket har fått eller upprättat i samband med skötseln av uppgifter enligt denna lag,

9) till Transport- och kommunikationsverket för uppgifter enligt lagen om tjänster inom elektronisk kommunikation (917/2014), postlagen (415/2011), lagen om stöd för byggande av fast bredband (1262/2020), lagen om stark autentisering (617/2009) och lagen om sambyggnad och samutnyttjande av nätinфраstruktur (276/2016).

Denna lag träder i kraft den 20 .

Helsingfors den 5 mars 2026

Statsminister

Petteri Orpo

Kommun- och regionminister Anna-Kaisa Ikonen

2.

Lag

om ändring av lagen om stark autentisering och betrodda elektroniska tjänster

I enlighet med riksdagens beslut
upphävs i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) 30, 32 och 36 §, 4 a kap. samt 42 c §,
sådana de lyder, 30, 32 och 36 § i lag 1009/2018, 4 a kap. i lag 533/2016 och 42 c § i lag 1188/2019,
ändras lagens rubrik, 1, 2 och 7 b §, 17 § 2 mom., 24 § 2 mom., 29 §, 31 § 1 mom., 37, 38, 42 och 42 a §, 45 § 1 mom. samt 45 a, 46, 47 och 49 a §,
sådana de lyder, lagens rubrik, 1 § och 24 § 2 mom. i lag 533/2016, 2 och 7 b §, 17 § 2 mom., 29, 37 och 38 §, 45 § 1 mom., 45 a, 46 och 47 § i lag 1009/2018, 31 § 1 mom. i lag 1188/2019, 42 § i lagarna 1009/2018 och 230/2021, 42 a § i lag 230/2021 och 49 a § i lag 1542/2019, samt
fogas till lagen nya 12 e och 21 a § som följer:

Gällande lydelse

Föreslagen lydelse

Lag

om stark autentisering och betrodda elektroniska tjänster

1 §

Tillämpningsområde

Denna lag innehåller bestämmelser om stark autentisering och om tillhandahållande av identifieringstjänster till tjänsteleverantörer, till allmänheten och till andra leverantörer av identifieringstjänster.

Lagen innehåller bestämmelser om tillsynen över efterlevnaden av Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, nedan EU:s förordning om elektronisk identifiering, samt bestämmelser som kompletterar den förordningen. Dessutom innehåller lagen bestämmelser om bedömning av överensstämmelsen med

Lag

om stark autentisering

1 §

Tillämpningsområde

Denna lag innehåller bestämmelser om

- 1) stark autentisering,
- 2) tillhandahållande av identifieringstjänster till tjänsteleverantörer, till allmänheten och till andra leverantörer av identifieringstjänster,
- 3) bedömning av överensstämmelse av identifieringstjänster.

Lagen tillämpas inte på

- 1) tillhandahållande av tjänster avsedda för identifiering internt inom en sammanslutning,
- 2) en sammanslutning som använder en egen metod för identifiering av egna kunder i samband med egna tjänster.

I lagen om vissa tjänster som möjliggör gränsöverskridande e-tjänster (/) föreskrivs det om tillsynen över efterlevnaden av

Gällande lydelse

kraven när det gäller identifieringstjänster och betrodda tjänster.

På gränsöverskridande identifieringssystem som anmäls till Europeiska kommissionen tillämpas denna lag endast om inte något annat följer av EU:s förordning om elektronisk identifiering.

Lagen tillämpas inte på tillhandahållande av tjänster avsedda för identifiering internt inom en sammanslutning. Lagen tillämpas inte heller på en sammanslutning som använder en egen metod för identifiering av egna kunder i samband med egna tjänster.

2 §

Definitioner

I denna lag avses med

1) *stark autentisering* identifiering av en person, av en juridisk person eller av en fysisk person som företräder en juridisk person och verifiering av identifikatorns autenticitet och riktighet genom tillämpning av en elektronisk metod som motsvarar tillitsnivån väsentlig enligt artikel 8.2 b i EU:s förordning om elektronisk identifiering eller tillitsnivån hög enligt artikel 8.2 c i den förordningen,

2) *identifieringsverktyg* ett sådant medel för elektronisk identifiering som avses i artikel 3.2 i EU:s förordning om elektronisk identifiering,

3) *leverantör av identifieringstjänster* en leverantör av tjänster för identifieringsförmedling eller en leverantör av identifieringsverktyg,

4) *leverantör av identifieringsverktyg* en tjänsteleverantör som tillhandahåller eller ger ut identifieringsverktyg för stark autentisering till allmänheten samt tillhandahåller sitt identifieringsverktyg till leverantörer av tjänster för identifieringsförmedling för förmedling i förtroendenätet,

5) *leverantör av tjänster för identifieringsförmedling* en tjänsteleverantör som förmedlar identifieringstransaktioner baserade på stark autentisering till en part som förlitar sig på en elektronisk identifiering,

6) *innehavare av identifieringsverktyg* en fysisk eller juridisk person som enligt avtal

Föreslagen lydelse

bestämmelserna i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, nedan eIDAS-förordningen, sådan den lyder senast ändrad genom förordning (EU) 2024/1183, och utfärdas det bestämmelser som kompletterar förordningen.

2 §

Definitioner

I denna lag avses med

1) ***stark autentisering*** identifiering av en person, av en juridisk person eller av en fysisk person som företräder en juridisk person och verifiering av identifikatorns autenticitet och riktighet genom tillämpning av en elektronisk metod som motsvarar tillitsnivån väsentlig enligt artikel 8.2 b i eIDAS-förordningen eller tillitsnivån hög enligt artikel 8.2 c i den förordningen,

2) ***identifieringsverktyg*** ett sådant medel för elektronisk identifiering som avses i artikel 3.2 i eIDAS-förordningen,

3) ***leverantör av identifieringstjänster*** en leverantör av tjänster för identifieringsförmedling och en leverantör av identifieringsverktyg,

4) ***leverantör av identifieringsverktyg*** en tjänsteleverantör som tillhandahåller eller ger ut identifieringsverktyg för stark autentisering till allmänheten samt tillhandahåller sitt identifieringsverktyg till leverantörer av tjänster för identifieringsförmedling för förmedling i förtroendenätet,

5) ***leverantör av tjänster för identifieringsförmedling*** en tjänsteleverantör som förmedlar identifieringstransaktioner baserade på stark autentisering till en part som förlitar sig på en elektronisk identifiering,

6) ***innehavare av identifieringsverktyg*** en fysisk eller juridisk person som enligt avtal

Gällande lydelse

har fått ett identifieringsverktyg av en leverantör av identifieringstjänster,

7) *inledande identifiering* verifiering av identiteten hos den som ansöker om ett identifieringsverktyg, när verifieringen sker i samband med att verktyget skaffas,

8) *certifikat* ett intyg i elektronisk form som verifierar identiteten eller verifierar identiteten och kopplar ihop autentiseringsuppgifter för en betrodd tjänst med en användare av tjänsten och som kan användas vid stark autentisering och betrodda tjänster,

9) *certifikatutfärdare* en fysisk eller juridisk person som tillhandahåller allmänheten certifikat,

10) *förtroendenätet* de leverantörer av identifieringstjänster som har gjort en anmälan till Transport- och kommunikationsverket,

11) *organ för bedömning av överensstämmelse* ett av Transport- och kommunikationsverket godkänt organ enligt artikel 2.13 i Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93, som är ackrediterat i enlighet med den förordningen.

Termerna elektronisk underskrift, betrodd tjänst, avancerad elektronisk underskrift, system för elektronisk identifiering och förlitande part har i denna lag samma betydelse som i artikel 3 i EU:s förordning om elektronisk identifiering.

7 b §

Information om giltighet för pass eller identitetskort

Leverantörer av identifieringstjänster har trots sekretessbestämmelserna rätt att via ett gränssnitt eller annars i elektronisk form få information ur polisens informationssystem om giltighet för pass eller identitetskort som används vid inledande identifiering.

Föreslagen lydelse

har fått ett identifieringsverktyg av en leverantör av identifieringstjänster,

7) ***inledande identifiering*** verifiering av identiteten hos den som ansöker om ett identifieringsverktyg, när verifieringen sker i samband med att verktyget skaffas,

8) ***certifikat*** ett intyg i elektronisk form som verifierar identiteten eller verifierar identiteten och kopplar ihop autentiseringsuppgifter för en betrodd tjänst med en användare av tjänsten och som kan användas vid stark autentisering och betrodda tjänster,

9) ***certifikatutfärdare*** en fysisk eller juridisk person som tillhandahåller allmänheten certifikat,

10) ***förtroendenätet*** de leverantörer av identifieringstjänster som har gjort en anmälan till Transport- och kommunikationsverket,

11) ***organ för bedömning av överensstämmelse*** ett av Transport- och kommunikationsverket godkänt organ enligt artikel 2.13 i Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93, som är ackrediterat i enlighet med den förordningen,

12) ***europaisk digital identitetsplånbok*** en sådan europeisk digital identitetsplånbok som avses i artikel 3.42 i eIDAS-förordningen,

13) ***system för elektronisk identifiering*** detsamma som i artikel 3.4 i eIDAS-förordningen,

14) ***förlitande part*** detsamma som i artikel 3.6 i eIDAS-förordningen.

7 b §

Information om giltighet för pass, identitetskort eller e-legitimation

Leverantörer av identifieringstjänster har trots sekretessbestämmelserna rätt att via ett tekniskt gränssnitt eller annars i elektronisk form få information ur polisens informationssystem om giltigheten för pass eller identitetskort som används vid inledande

Gällande lydelse

Föreslagen lydelse

identifiering samt information ur Myndigheten för digitalisering och befolkningsdatas informationssystem om giltigheten för ett kvalificerat elektroniskt attributsintyg som ingår i e-legitimation som avses i lagen om e-legitimation (/) och som och som används vid inledande identifiering.

Leverantörer av identifieringsverktyg är skyldiga att säkerställa den i 1 mom. avsedda informationen om giltigheten för de handlingar som används vid inledande identifiering. Leverantörerna ska säkerställa att ett identifieringsverktyg inte kan användas förrän handlingens giltighet har säkerställts.

12 e §

***Förmedling av identifieringstransaktioner
baserade på en europeisk digital
identitetsplånbok***

Leverantörer av tjänster för identifieringsförmedling kan förmedla identifieringstransaktioner som baserar sig på en europeisk digital identitetsplånbok till en part som förlitar sig på elektronisk identifiering, trots att bestämmelserna i denna lag inte tillämpas på plånböcker eller deras tillhandahållare.

17 §

*Identifiering av en fysisk person som ansöker
om ett identifieringsverktyg*

Dokument som godkänns vid inledande identifiering, när identifieringen endast sker utifrån en identitetshandling som utfärdats av en myndighet, är ett giltigt pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet, i Schweiz eller i San Marino. En leverantör av identifieringsverktyg som så önskar kan också vid kontrollen av identiteten använda ett giltigt pass som har utfärdats av en myndighet i någon annan stat.

17 §

*Identifiering av en fysisk person som ansöker
om ett identifieringsverktyg*

Dokument som godkänns vid inledande identifiering, när identifieringen endast sker utifrån en identitetshandling som utfärdats av en myndighet, är ett giltigt pass eller identitetskort som har utfärdats av en myndighet i en medlemsstat inom Europeiska ekonomiska samarbetsområdet, i Schweiz eller i San Marino. Leverantörer av identifieringsverktyg kan som identitetshandling godkänna också en sådan e-legitimation som avses i lagen om e-legitimation. En leverantör av identifieringsverktyg som så önskar kan vid kontrollen av identiteten dessutom använda

Gällande lydelse

Föreslagen lydelse

ett giltigt pass som har utfärdats av en myndighet i någon annan stat.

21 a §

Återaktivering av identifieringsverktyg

Vid återaktivering av identifieringsverktyg ska kraven i punkt 2.2.3 i bilagan till förordningen om tillitsnivåer vid elektronisk identifiering iakttas.

24 §

Registrering och användning av uppgifter om identifieringstransaktioner och identifieringsverktyg

Leverantörer av identifieringsverktyg ska registrera behövliga uppgifter om den inledande identifiering av sökande som avses i 17 och 17 a § och om de handlingar eller den elektroniska identifiering som använts i den inledande identifieringen.

24 §

Registrering och användning av uppgifter om identifieringstransaktioner och identifieringsverktyg

Leverantörer av identifieringsverktyg ska registrera behövliga uppgifter om den inledande identifiering av sökande som avses i 17 och 17 a § och om de handlingar eller den elektroniska identifiering som använts i den inledande identifieringen. *Om det i den inledande identifieringen används ett identifieringsverktyg som levereras av en annan leverantör av identifieringsverktyg, ska information om den inledande identifieringstransaktionen förmedlas till den berörda leverantören av identifieringsverktyg i samband med identifieringstransaktionen.*

29 §

Bedömning av överensstämmelse hos en elektronisk identifieringstjänst

En leverantör av identifieringstjänster ska regelbundet låta ett sådant bedömningsorgan som nämns i 28 § bedöma om identifieringstjänsten uppfyller kraven på interoperabilitet, informationssäkerhet, dataskydd och annan tillförlitlighet enligt denna lag.

Bestämmelser om bedömning av överensstämmelse hos system för elektronisk identifiering som ska anmälas till Europeiska

29 §

Bedömning av överensstämmelse hos en elektronisk identifieringstjänst

En leverantör av identifieringstjänster ska regelbundet låta ett sådant bedömningsorgan som *avses* i 28 § bedöma om identifieringstjänsten uppfyller kraven på interoperabilitet, informationssäkerhet, dataskydd och annan tillförlitlighet enligt denna lag.

Bestämmelser om Transport- och kommunikationsverkets rätt att meddela närmare föreskrifter om

Gällande lydelse

kommissionen finns i EU:s förordning om elektronisk identifiering och i förordningen om tillitsnivåer vid elektronisk identifiering.

Bestämmelser om Transport- och kommunikationsverkets rätt att meddela närmare föreskrifter om bedömningsgrunderna vid bedömningen av överensstämmelsen hos en identifieringstjänst finns i 42 §. Som bedömningsgrund kan Transport- och kommunikationsverket utöver de författningar och rättsakter som avses i 1 och 2 mom. fastställa bestämmelser eller riktlinjer som antagits av Europeiska unionen eller något annat internationellt organ, publicerade och generellt eller regionalt tillämpade anvisningar för informationssäkerhet samt datasäkerhetsstandarder eller förfaranden som används allmänt.

Föreslagen lydelse

bedömningsgrunderna vid bedömningen av överensstämmelsen hos en identifieringstjänst finns i 42 §. Som bedömningsgrund kan Transport- och kommunikationsverket utöver de författningar och rättsakter som avses i 1 mom. fastställa bestämmelser eller riktlinjer som antagits av Europeiska unionen eller något annat internationellt organ, publicerade och generellt eller regionalt tillämpade anvisningar för informationssäkerhet samt datasäkerhetsstandarder eller förfaranden som används allmänt.

30 §

Bedömning av överensstämmelse hos den nationella noden för elektronisk identifiering

Överensstämmelse hos det nationella gränssnitt som hör till EU:s interoperabilitetsramverk för elektronisk identifiering (den nationella noden) ska påvisas genom en bedömning som görs av ett organ för bedömning av överensstämmelse eller ett annat utomstående bedömningsorgan.

Bestämmelser om kraven på den nationella noden finns i kommissionens genomförandeförordning (EU) 2015/1501 om interoperabilitetsramverket enligt artikel 12.8 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden. Bestämmelser om Transport- och kommunikationsverkets rätt att meddela närmare föreskrifter om bedömningsgrunderna vid bedömningen av överensstämmelse hos den nationella noden finns i 42 §.

(upphävs)

31 §

31 §

Gällande lydelse

Inspektionsberättelse

En leverantör av identifieringstjänster och Myndigheten för digitalisering och befolkningsdata ska över bedömningen av överensstämmelse låta utarbeta en inspektionsberättelse som lämnas in till Transport- och kommunikationsverket.

Föreslagen lydelse

Inspektionsberättelse

En leverantör av identifieringstjänster ska över bedömningen av överensstämmelse låta utarbeta en inspektionsberättelse som lämnas in till Transport- och kommunikationsverket.

32 §

Fastställande av överensstämmelse hos betrodda tjänster

Ett organ för bedömning av överensstämmelse ska inspektera en kvalificerad tillhandahållare av betrodda tjänster och överensstämmelsen hos en kvalificerad betrodd tjänst med iakttagande av bestämmelserna i EU:s förordning om elektronisk identifiering.

Bestämmelser om Transport- och kommunikationsverkets rätt att meddela närmare föreskrifter om bedömningsgrunderna vid bedömningen av överensstämmelse finns i 42 §. Som bedömningsgrund kan Transport- och kommunikationsverket fastställa bestämmelser eller riktlinjer som antagits av Europeiska unionen eller något annat internationellt organ, publicerade och generellt eller regionalt tillämpade anvisningar för informationssäkerhet samt datasäkerhetsstandarder eller förfaranden som används allmänt.

(upphävs)

36 §

Certifiering av anordningar för skapande av kvalificerade elektroniska underskrifter eller kvalificerade elektroniska stämplat

Transport- och kommunikationsverket får efter ansökan utse offentliga eller privata certifieringsorgan enligt artiklarna 30 och 39.2 i EU:s förordning om elektronisk identifiering som har i uppgift att certifiera anordningar för skapande av kvalificerade

(upphävs)

Gällande lydelse

elektroniska underskrifter eller kvalificerade elektroniska stämplat. Certifieringsorganet kan utses för viss tid. I sin ansökan ska certifieringsorganet ange de uppgifter som Transport- och kommunikationsverket begär och som behövs för behandlingen av ansökan.

Certifieringsorganet ska vara funktionellt och ekonomiskt oberoende av tillverkarna av anordningar för skapande av elektroniska underskrifter eller elektroniska stämplat. Organet ska ha en ansvarsförsäkring som är tillräcklig med hänsyn till verksamhetens omfattning, eller något annat motsvarande arrangemang, och det ska ha tillgång till en tillräckligt stor yrkeskunnig personal och de system, den utrustning och de redskap som behövs för verksamheten.

37 §

Verksamheten vid organ för bedömning av överensstämmelse och certifieringsorgan

Ett organ för bedömning av överensstämmelse och ett certifieringsorgan får i sitt uppdrag anlita personer som inte hör till organisationen. Organen ansvarar också för det arbete som utförts av personer de anlitat.

Organ för bedömning av överensstämmelse och certifieringsorgan ska följa bestämmelserna i förvaltningslagen (434/2003), lagen om offentlighet i myndigheternas verksamhet, lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003), språklagen (423/2003) och samiska språklagen (1086/2003) när de utför offentliga förvaltningsuppgifter som avses i denna lag. På personalen vid organ för bedömning av överensstämmelse och vid certifieringsorgan och vid dotterbolag och underentreprenörer som anlitas av sådana organ tillämpas bestämmelserna om straffrättsligt tjänsteansvar när den sköter uppgifter som avses i denna paragraf. Bestämmelser om skadeståndsansvar finns i skadeståndslagen (412/1974).

Organ för bedömning av överensstämmelse och certifieringsorgan ska underrätta Transport- och kommunikationsverket om

Föreslagen lydelse

37 §

Verksamheten vid organ för bedömning av överensstämmelse

Ett organ för bedömning av överensstämmelse får i sitt uppdrag anlita personer som inte hör till organisationen. Organet ansvarar också för det arbete som utförts av personer som organet anlitat.

Bestämmelser om de principer för god förvaltning som organ för bedömning av överensstämmelse ska följa, när det utför offentliga förvaltningsuppgifter som avses i denna lag, finns i förvaltningslagen (434/2003), lagen om offentlighet i myndigheternas verksamhet, lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003), språklagen (423/2003) och samiska språklagen (1086/2003). På personalen vid organ för bedömning av överensstämmelse och vid dotterbolag och underentreprenörer som anlitas av sådana organ tillämpas bestämmelserna om straffrättsligt tjänsteansvar när personalen utför uppgifter som avses i denna paragraf. Bestämmelser om skadeståndsansvar finns i skadeståndslagen (412/1974).

Organ för bedömning av överensstämmelse ska underrätta Transport- och kommunikationsverket om varje ändring som

Gällande lydelse

varje ändring som har betydelse för uppfyllandet av villkoren för att godkännas eller utses.

38 §

Återkallande av godkännande som organ för bedömning av överensstämmelse eller utseende till certifieringsorgan

Om Transport- och kommunikationsverket konstaterar att ett organ för bedömning av överensstämmelse eller ett certifieringsorgan inte uppfyller föreskrivna villkor eller att organet i väsentlig grad handlar i strid med gällande bestämmelser, ska Transport- och kommunikationsverket sätta ut en tillräcklig tidsfrist inom vilken saken ska rättas till.

Transport- och kommunikationsverket kan återkalla ett beslut att godkänna ett bedömningsorgan eller utse ett certifieringsorgan om organet inte har korrigerat sin verksamhet inom den tid som satts ut enligt 1 mom. och det är fråga om en väsentlig förseelse eller försummelse.

4 a kap.

Betrodda tjänster

39 §

Återkallande av certifikat

En undertecknare eller en innehavare av en elektronisk stämpel ska utan dröjsmål begära att den certifikatutfärdare som har utfärdat ett kvalificerat certifikat ska återkalla det, om undertecknaren eller innehavaren har grundad anledning att misstänka att framställningsdata för underteckningen eller den elektroniska stämpeln används på obehörigt sätt.

En certifikatutfärdare som tillhandahåller kvalificerade certifikat ska utan dröjsmål återkalla ett kvalificerat certifikat, om undertecknaren eller innehavaren av den elektroniska stämpeln begär det. En begäran om återkallande av ett certifikat anses ha kommit in till certifikatutfärdaren när den har

Föreslagen lydelse

har betydelse för uppfyllandet av villkoren för att godkännas.

38 §

Återkallande av godkännande som organ för bedömning av överensstämmelse

Om Transport- och kommunikationsverket konstaterar att ett organ för bedömning av överensstämmelse inte uppfyller föreskrivna villkor eller att organet i väsentlig grad handlar i strid med gällande bestämmelser, ska Transport- och kommunikationsverket sätta ut en tillräcklig tidsfrist inom vilken saken ska korrigeras.

Transport- och kommunikationsverket kan återkalla ett beslut att godkänna ett bedömningsorgan om organet inte har korrigerat sin verksamhet inom den tid som satts ut enligt 1 mom. och det är fråga om en väsentlig förseelse eller försummelse.

(upphävs 4 a kap.)

(upphävs)

Gällande lydelse

stått till utfärdarens förfogande så att begäran har kunnat behandlas.

Föreslagen lydelse

40 §

Ansvar för obehörig användning av framställningsdata för en underteckning eller elektronisk stämpel

En undertecknare och en innehavare av en elektronisk stämpel ansvarar för skada som orsakats av obehörig användning av framställningsdata för en avancerad elektronisk underskrift eller elektronisk stämpel som är baserad på ett kvalificerat certifikat tills en begäran om återkallande av certifikatet har kommit in till certifikatutfärdaren så som anges i 39 § 2 mom.

(upphävs)

En konsument har dock ansvar enligt 1 mom. endast om

1) konsumenten har överlåtit framställningsdata till någon annan,

2) någon som är obehörig att använda framställningsdata kommit åt dem på grund av att konsumenten varit vårdslös på ett sätt som inte är lindrigt, eller

3) konsumenten på annat sätt än det som nämns i 2 punkten har förlorat besittningen till framställningsdata och därefter har underlåtit att begära att det certifikatet ska återkallas så som anges i 39 § 1 mom.

41 §

Det ansvar som vilar på tillhandahållare av betrodda tjänster

Bestämmelser om det ansvar som vilar på tillhandahållare av betrodda tjänster finns i artikel 13 i EU:s förordning om elektronisk identifiering.

Den certifikatutfärdare som tillhandahållit ett kvalificerat certifikat är ansvarig för skada som den som förlitat sig på det kvalificerade certifikatet orsakats genom att certifikatutfärdaren eller en person som denne anlitat inte har återkallat certifikatet på det sätt som anges i 39 §. Certifikatutfärdaren är fri från ansvar, om den visar att skadan inte

(upphävs)

Gällande lydelse

har berott på oaktsamhet hos certifikatutfärdaren eller en person som denne anlitat.

42 §

Allmän styrning samt Transport- och kommunikationsverkets föreskrifter

Kommunikationsministeriet svarar för den allmänna styrningen och utvecklingen av stark autentisering och betrodda tjänster.

Transport- och kommunikationsverket får meddela närmare föreskrifter om

1) kraven enligt 8 § 1 mom. 4 och 5 punkten på säkerhet och tillförlitlighet hos identifieringssystemet,

2) innehållet i de uppgifter som ska anmälas enligt 10 § och inlämnandet av dem till Transport- och kommunikationsverket,

3) egenskaperna enligt 12 a § 3 mom. hos förtroendenätets gränssnitt, (26.3.2021/230)

4) när störningar som avses i 16 § är betydande och om innehållet i anmälningar enligt 16 § 1 mom. samt anmälningarnas form och inlämnandet av dem,

5) grunderna för bedömningen enligt 29, 30 och 32 § av överensstämelsen hos en identifieringstjänst, en betrodd tjänst och den nationella noden,

6) kompetenskraven enligt 33 § för organ för bedömning av överensstämmelse med beaktande av vad som föreskrivs i EU:s förordning om elektronisk identifiering,

7) de uppgifter som ska ingå i en ansökan enligt 35 § och inlämnandet av dem till Transport- och kommunikationsverket,

8) de krav som ställs på certifieringsorgan som avses i 36 §, förfarandet vid certifiering och kraven på anordningar för skapande av elektroniska underskrifter och elektroniska stämplat med beaktande av vad som föreskrivs i EU:s förordning om elektronisk identifiering.

42 a §

Transport- och kommunikationsverkets uppgifter

Föreslagen lydelse

42 §

Transport- och kommunikationsverkets föreskrifter

Transport- och kommunikationsverket får meddela närmare föreskrifter om

1) kraven enligt 8 § 1 mom. 4 och 5 punkten på säkerhet och tillförlitlighet hos identifieringssystemet,

2) innehållet i de uppgifter som ska anmälas enligt 10 § och inlämnandet av dem till Transport- och kommunikationsverket,

3) egenskaperna enligt 12 a § 3 mom. hos förtroendenätets tekniska gränssnitt,

4) när störningar som avses i 16 § är betydande och om innehållet i anmälningar enligt 16 § 1 mom. samt anmälningarnas form och inlämnandet av dem,

5) *de behövliga uppgifter som avses i 24 § 2 mom. och som ska registreras om den inledande identifieringen av sökanden och om de handlingar eller om den elektroniska identifiering som används i den inledande identifieringen,*

6) *de grunder för bedömningen av överensstämelsen hos en identifieringstjänst som avses i 29 §,*

7) *kompetenskraven enligt 33 § för organ för bedömning av överensstämmelse,*

8) *de uppgifter som ska ingå i en ansökan som avses i 35 § och inlämnandet av dem till Transport- och kommunikationsverket.*

42 a §

Transport- och kommunikationsverkets uppgifter

Gällande lydelse

Transport- och kommunikationsverket ska utöva tillsyn över efterlevnaden av denna lag, om inte något annat föreskrivs i denna lag.

Transport- och kommunikationsverket ska årligen samla och föra statistik över information om marknaden för stark autentisering och om tillhandahållandet av, tillgången till och priserna på identifieringstjänster. Den information som verket samlar hos leverantörer av identifieringstjänster ska vara behövlig för uppföljningen av regleringens konsekvenser *eller för skötseln av den styrnings- och utvecklingsuppgift som avses i 42 § 1 mom.* Informationen ska omfatta uppgifter om volymen av identifieringstransaktionerna, priserna mellan identifieringstjänsterna, detaljpriser på eller kundmängder inom identifieringstjänsterna, inkomster från identifieringstjänster eller andra motsvarande uppgifter som behövs för att statistikföringen ska vara tillförlitlig.

Transport- och kommunikationsverket ska i enlighet med EU:s förordning om elektronisk identifiering

1) delta i samarbetet mellan Europeiska unionens medlemsstater i det interoperabilitetsramverk för elektronisk identifiering som avses i artikel 12 i förordningen och i det samarbetsnätverk som upprättats för detta ändamål,

2) anmäla system för elektronisk identifiering till Europeiska kommissionen i enlighet med artiklarna 7–10 i förordningen,

3) vara tillsynsorgan enligt artikel 17 i förordningen och sköta tillsynsorganets uppgifter enligt förordningen,

4) i enlighet med artikel 22 i förordningen föra och publicera förteckningar över kvalificerade tillhandahållare av betrodda tjänster i Finland och över de kvalificerade betrodda tjänster som dessa tillhandahåller.

Transport- och kommunikationsverkets beslutanderätt omfattar inte avtalsförhållanden mellan parter eller frågor om ersättningsskyldighet.

Föreslagen lydelse

Transport- och kommunikationsverket ska utöva tillsyn över efterlevnaden av denna lag, om inte något annat föreskrivs i denna lag.

Transport- och kommunikationsverket ska årligen samla och föra statistik över information om marknaden för stark autentisering och om tillhandahållandet av, tillgången till och priserna på identifieringstjänster. Den information som verket samlar hos leverantörer av identifieringstjänster ska vara behövlig för uppföljningen av regleringens konsekvenser. Informationen ska omfatta uppgifter om volymen av identifieringstransaktionerna, priserna mellan identifieringstjänsterna, detaljpriser på eller kundmängder inom identifieringstjänsterna, inkomster från identifieringstjänster eller andra motsvarande uppgifter som behövs för att statistikföringen ska vara tillförlitlig.

Transport- och kommunikationsverkets beslutanderätt omfattar inte avtalsförhållanden mellan parter eller frågor om ersättningsskyldighet.

Gällande lydelse

*Uppgifter som ankommer på Myndigheten
för digitalisering och befolkningsdata*

Myndigheten för digitalisering och
befolkningsdata ska upprätthålla den
nationella nod som avses i 30 § 1 mom.

45 §

Administrativa tvångsmedel

Transport- och kommunikationsverket kan ge en anmärkning till den som bryter mot denna lag eller bestämmelser som utfärdats eller föreskrifter eller beslut som har meddelats med stöd av den, *eller mot EU:s förordning om elektronisk identifiering eller bestämmelser som har utfärdats med stöd av den*, samt ålägga denne att avhjälpa felet eller försummelsen inom skälig tid. Beslutet kan förenas med vite eller med hot om att verksamheten kommer att avbrytas helt eller delvis eller att den försummade åtgärden kommer att vidtas på den försumliges bekostnad. *Bestämmelser om vite, hot om avbrytande och hot om tvångsutförande finns i viteslagen (1113/1990).*

45 a §

Interimistiska beslut

Om ett fel eller en försummelse som gäller *EU:s förordning om elektronisk identifiering*, denna lag eller bestämmelser som utfärdats eller föreskrifter som meddelats med stöd av den, eller en störning i datasäkerheten, omedelbart och i väsentlig grad äventyrar tillförlitligheten hos en identifieringstjänst *eller betrodde tjänst*, får Transport- och kommunikationsverket omgående besluta om behövliga interimistiska åtgärder oberoende av den tidsfrist som avses i 45 §.

Transport- och kommunikationsverket ska innan det beslutar om interimistiska åtgärder ge den som är föremål för beslutet tillfälle att bli hörd, utom när detta inte kan ordnas så

Föreslagen lydelse

(upphävs)

45 §

Administrativa tvångsmedel

Transport- och kommunikationsverket kan ge en anmärkning till den som bryter mot denna lag eller bestämmelser som utfärdats eller föreskrifter eller beslut som har meddelats med stöd av den, samt ålägga denne att avhjälpa felet eller försummelsen inom skälig tid. Beslutet kan förenas med vite eller med hot om att verksamheten kommer att avbrytas helt eller delvis eller att den försummade åtgärden kommer att vidtas på den försumliges bekostnad.

45 a §

Interimistiska beslut

Om ett fel eller en försummelse som gäller denna lag eller bestämmelser som utfärdats eller föreskrifter som meddelats med stöd av *den*, eller en störning i datasäkerheten, omedelbart och i väsentlig grad äventyrar tillförlitligheten hos en identifieringstjänst, får Transport- och kommunikationsverket omgående *förbjuda eller avbryta tillhandahållandet av identifieringsmetoden som stark autentisering* oberoende av den tidsfrist som avses i 45 §.

Transport- och kommunikationsverket ska innan det beslutar om interimistiska åtgärder ge den som är föremål för beslutet tillfälle att bli hörd, utom när detta inte kan ordnas så

Gällande lydelse

snabbt som ärendets brådskande natur nödvändigtvis kräver.

Som interimistisk åtgärd kan Transport- och kommunikationsverket förbjuda eller avbryta

1) tillhandahållandet av en identifieringsmetod som stark autentisering,

2) tillhandahållandet av en sådan kvalificerad betrodd tjänst som avses i artikel 3.17 i EU:s förordning om elektronisk identifiering,

3) tillhandahållandet av ett system för elektronisk identifiering som anmälts enligt artikel 9.1 i EU:s förordning om elektronisk identifiering,

4) tillhandahållandet av autentisering enligt artikel 7 f i EU:s förordning om elektronisk identifiering.

De interimistiska åtgärderna kan vara i kraft i högst tre månader. Beslut om interimistiska åtgärder får överklagas separat, på samma sätt som beslut som avses i 45 § 1 mom.

46 §

Inspektionsrätt

Transport- och kommunikationsverket har rätt att utföra inspektioner av leverantörer av identifieringstjänster och av leverantörernas tjänster, av organ för bedömning av överensstämmelse som avses i 28 §, *av certifieringsorgan enligt 36 § för anordningar för skapande av kvalificerade elektroniska underskrifter och elektroniska stämplatser och dessa organs verksamhet, av certifikatutfärdare som tillhandahåller kvalificerade certifikat samt av tillhandahållare av betrodda tjänster och deras tjänster.* En inspektion kan genomföras för att övervaka fullgörandet av skyldigheter enligt denna lag *och EU:s förordning om elektronisk identifiering* samt bestämmelser som utfärdats och föreskrifter och beslut som har meddelats med stöd av dem. Bestämmelser om inspektioner finns i 39 § i förvaltningslagen.

Transport- och kommunikationsverket förordnar en inspektör att utföra de inspektioner som avses i 1 mom. Den som utför inspektionen har rätt att hos en

Föreslagen lydelse

snabbt som ärendets brådskande natur nödvändigtvis kräver.

De interimistiska åtgärderna kan vara i kraft i högst tre månader. Beslut om interimistiska åtgärder får överklagas separat, på samma sätt som beslut som avses i 45 § 1 mom.

46 §

Inspektionsrätt

Transport- och kommunikationsverket har rätt att utföra inspektioner av leverantörer av identifieringstjänster och av leverantörernas tjänster samt av organ för bedömning av överensstämmelse som avses i 28 § *och av organens verksamhet.* En inspektion kan genomföras för att övervaka fullgörandet av skyldigheter enligt denna lag samt bestämmelser som utfärdats och föreskrifter och beslut som har meddelats med stöd av den. *På inspektioner tillämpas 39 § i förvaltningslagen.*

Transport- och kommunikationsverket förordnar en inspektör att utföra de inspektioner som avses i 1 mom. Den som utför inspektionen har rätt att hos en

Gällande lydelse

leverantör av identifieringstjänster, *hos en certifikatutfärdare som tillhandahåller kvalificerade certifikat* och hos en tillhandahållare av betrodda tjänster samt hos personer som dessa anlitar granska sådan maskinvara och programvara som kan vara av betydelse vid tillsynen över efterlevnaden av denna lag och de bestämmelser som utfärdats och de föreskrifter som meddelats med stöd av den.

Leverantörer av identifieringstjänster, *certifikatutfärdare som tillhandahåller kvalificerade certifikat, tillhandahållare av betrodda tjänster* och de personer som dessa anlitar ska för inspektionen ge en inspektör som avses i 2 mom. tillträde till alla andra utrymmen än sådana som används för boende av permanent natur.

47 §

Avgifter till Transport- och kommunikationsverket

När en leverantör av identifieringstjänster eller en sammanslutning av tjänsteleverantörer som har gjort en anmälan enligt 10 § registreras första gången ska den betala Transport- och kommunikationsverket en registreringsavgift på 5 000 euro. Leverantören av identifieringstjänster eller sammanslutningen ska dessutom betala Transport- och kommunikationsverket en årlig tillsynsavgift på sammanlagt 14 000 euro för tillsynen över alla de identifieringstjänster som leverantören eller sammanslutningen tillhandahåller.

En kvalificerad tillhandahållare av betrodda tjänster som gjort en anmälan enligt artikel 21 i EU:s förordning om elektronisk identifiering och en certifikatutfärdare som tillhandahåller kvalificerade betrodda tjänster ska betala Transport- och kommunikationsverket en registreringsavgift på 5 000 euro för varje betrodd tjänst de tillhandahåller. Dessutom ska de betala Transport- och kommunikationsverket en årlig tillsynsavgift på 14 000 euro för den första kvalificerade betrodda tjänst som de tillhandahåller och en årlig tillsynsavgift på 9 000 euro för varje

Föreslagen lydelse

leverantör av identifieringstjänster och hos personer som denne anlitar granska sådan maskinvara och programvara som kan vara av betydelse vid tillsynen över efterlevnaden av denna lag och de bestämmelser som utfärdats och de föreskrifter som meddelats med stöd av den.

Leverantörer av identifieringstjänster och de personer som dessa anlitar ska för inspektionen ge en inspektör som avses i 2 mom. tillträde till alla andra utrymmen än sådana som används för boende av permanent natur.

47 §

Avgifter till Transport- och kommunikationsverket

Leverantören av identifieringstjänster eller sammanslutningen ska betala Transport- och kommunikationsverket en årlig tillsynsavgift på sammanlagt 17 000 euro för tillsynen över alla de identifieringstjänster som leverantören eller sammanslutningen tillhandahåller.

Ett organ för bedömning av överensstämmelse som godkänts enligt 34 § ska betala Transport- och kommunikationsverket en årlig tillsynsavgift på 18 000 euro.

Tillsynsavgiften ska betalas till fullt belopp också under det första verksamhetsåret, även om verksamheten inleds senare under året. Tillsynsavgiften återbetalas inte även om tjänsteleverantören upphör med sin verksamhet under året.

Gällande lydelse

därpå följande kvalificerade betrodda tjänst som de tillhandahåller. Om en certifikatutfärdare som tillhandahåller betrodda tjänster även gör en anmälan enligt 10 §, ska certifikatutfärdaren dessutom betala den registreringsavgift som anges i 1 mom.

Ett organ för bedömning av överensstämmelse som godkänts enligt 34 § ska betala Transport- och kommunikationsverket en utnämningsavgift på 10 000 euro. Dessutom ska organet betala Transport- och kommunikationsverket en årlig tillsynsavgift på 15 000 euro.

Ett certifieringsorgan som utsetts enligt 36 § ska betala Transport- och kommunikationsverket en utnämningsavgift på 10 000 euro. Dessutom ska organet betala Transport- och kommunikationsverket en årlig tillsynsavgift på 15 000 euro.

Registreringsavgiften, utnämningsavgiften och tillsynsavgiften täcker Transport- och kommunikationsverkets kostnader för att utföra uppgifterna enligt denna lag, med undantag för de uppgifter som avses i 46 § 1 mom. Tillsynsavgiften ska betalas till fullt belopp också under det första verksamhetsåret, även om verksamheten inleds under året. Tillsynsavgiften återbetalas inte, även om tjänsteleverantören upphör med sin verksamhet under året.

Registreringsavgiften, utnämningsavgiften och tillsynsavgiften påförs av Transport- och kommunikationsverket och avgifterna är direkt utsökbara. I Transport- och kommunikationsverkets beslut om påförande av avgift får ändring sökas i enlighet med 49 § 1 mom. Närmare bestämmelser om verkställigheten av avgifterna får utfärdas genom förordning av kommunikationsministeriet.

Bestämmelser om indrivning av registreringsavgiften, utnämningsavgiften och tillsynsavgiften finns i lagen om verkställighet av skatter och avgifter. Om avgifterna inte betalas senast på förfallodagen, tas årlig dröjsmålsränta ut på det obetalda beloppet enligt den räntesats som avses i 4 § i räntelagen (633/1982). I stället för dröjsmålsränta kan myndigheten ta ut en

Föreslagen lydelse

Tillsynsavgiften påförs av Transport- och kommunikationsverket och avgiften är direkt utsökbar. Bestämmelser om sökande av ändring i beslut om påförande av avgift finns i 49 §.

Bestämmelser om indrivning av tillsynsavgifter finns i lagen om verkställighet av skatter och avgifter. Om avgiften inte betalas senast på förfallodagen, tas årlig dröjsmålsränta ut på det obetalda beloppet enligt den räntesats som föreskrivs i 4 § i räntelagen (633/1982). I stället för dröjsmålsränta kan myndigheten ta ut en dröjsmålsavgift på fem euro om dröjsmålsräntan är mindre än detta belopp.

Bestämmelser om den avgift som tas ut för behandling av en anmälan enligt 10 § och en ansökan enligt 35 § samt för en inspektion enligt 46 § 1 mom. finns i lagen om grunderna för avgifter till staten.

Gällande lydelse

dröjsmålsavgift på fem euro om dröjsmålsrättan är mindre än detta belopp.

För en inspektion som avses i 46 § 1 mom. tas kostnaderna för inspektionen ut av föremålet för inspektionen med iakttagande av lagen om grunderna för avgifter till staten.

49 a §

Sökande av ändring i beslut av organ för bedömning av överensstämmelse och beslut av certifieringsorgan

Omrövning av ett beslut som fattats av ett organ för bedömning av överensstämmelse eller av ett certifieringsorgan med stöd av denna lag får begäras hos Transport- och kommunikationsverket. Bestämmelser om begäran om omrövning finns i förvaltningslagen.

Bestämmelser om sökande av ändring i förvaltningsdomstol finns i lagen om rättegång i förvaltningsärenden.

Beslut av organ för bedömning av överensstämmelse och beslut av certifieringsorgan ska iakttas trots ändringssökande, om inte den myndighet där ändring söks bestämmer något annat.

Föreslagen lydelse

49 a §

Sökande av ändring i beslut av organ för bedömning av överensstämmelse

Omrövning av ett beslut som fattats av ett organ för bedömning av överensstämmelse med stöd av denna lag får begäras hos Transport- och kommunikationsverket. Bestämmelser om begäran om omrövning finns i förvaltningslagen.

Bestämmelser om sökande av ändring i förvaltningsdomstol finns i lagen om rättegång i förvaltningsärenden.

Beslut av organ för bedömning av överensstämmelse ska iakttas trots ändringssökande, om inte den myndighet där ändring söks bestämmer något annat.

*Denna lag träder i kraft den 20 .
Lagens 7 b § och 17 § 2 mom. träder dock i
kraft först den 1 januari 2027.*

4.

Lag

om ändring av 3 och 6 § i lagen om tillhandahållande av digitala tjänster

I enlighet med riksdagens beslut
ändras i lagen om tillhandahållande av digitala tjänster (306/2019) 3 § 1 mom. 4 punkten och 6 § 2 mom. som följer:

Gällande lydelse

3 §

Lagens tillämpningsområde

Denna lag tillämpas

4) på identifieringstjänster som tillhandahålls av sådana leverantörer av identifieringstjänster som finns införda i det register som avses i 12 § i lagen om stark autentisering *och betrodda elektroniska tjänster* (617/2009) samt på sådana delar av digitala tjänster som används via en i 3 § 1 mom. 8 punkten i lagen om förvaltningens gemensamma stödtjänster för e-tjänster (571/2016) avsedd samlad förvaltningstjänst för internetbetalning och med vilka betalningsuppdrag kan skötas,

6 §

Elektronisk identifiering av tjänsteanvändarna

Om det är möjligt att få se och använda sekretessbelagt datainnehåll i en digital tjänst, ska tjänsteanvändaren identifieras med hjälp av en sådan tjänst för identifiering av fysiska personer som avses i 3 § 1 mom. 4 punkten i lagen om förvaltningens gemensamma stödtjänster för e-tjänster, med hjälp av stark autentisering som avses i 2 § 1 mom. 1 punkten i lagen om stark autentisering och betrodda elektroniska tjänster eller av vägande och motiverande skäl med hjälp av

Föreslagen lydelse

3 §

Lagens tillämpningsområde

Denna lag tillämpas

4) på identifieringstjänster som tillhandahålls av sådana leverantörer av identifieringstjänster som finns införda i det register som avses i 12 § i lagen om stark autentisering (617/2009) samt på sådana delar av digitala tjänster som används via en i 3 § 1 mom. 8 punkten i lagen om förvaltningens gemensamma stödtjänster för e-tjänster (571/2016) avsedd samlad förvaltningstjänst för internetbetalning och med vilka betalningsuppdrag kan skötas,

6 §

Elektronisk identifiering av tjänsteanvändarna

Om det är möjligt att få se och använda sekretessbelagt datainnehåll i en digital tjänst, ska tjänsteanvändaren identifieras med hjälp av en sådan tjänst för identifiering av fysiska personer som avses i 3 § 1 mom. 4 punkten i lagen om förvaltningens gemensamma stödtjänster för e-tjänster, med hjälp av stark autentisering som avses i 2 § 1 punkten i lagen om stark autentisering, *med hjälp av en europeisk digital identitetsplånbok som avses i 2 § 1 punkten i lagen om vissa tjänster som*

Gällande lydelse

någon annan motsvarande informationssäker
identifieringstjänst.

Föreslagen lydelse

*möjliggör gränsöverskridande e-tjänster (/)
eller av vägande och motiverande skäl med
hjälp av någon annan motsvarande
informationssäker identifieringstjänst.*

Denna lag träder i kraft den 20 .

5.

Lag

om ändring av 3 § i lagen om förvaltningens gemensamma stödtjänster för e-tjänster

I enlighet med riksdagens beslut
ändras i lagen om förvaltningens gemensamma stödtjänster för e-tjänster (571/2016) 3 § 1 mom. 4 och 5 punkten samt 3 § 2 mom., av dem 3 § 2 mom. sådant det lyder i lag 1314/2019, som följer:

Gällande lydelse

3 §

Stödtjänster

De gemensamma stödtjänsterna för e-tjänster omfattar

4) en sådan tjänst för identifiering av fysiska personer som identifierar en fysisk person som använder den offentliga förvaltningens e-tjänster med hjälp av en tjänst som tillhandahålls av en sådan leverantör av identifieringstjänster som avses i lagen om stark autentisering *och betrodda elektroniska tjänster* (533/2016), administrerar identifieringstransaktionen och till användarorganisationen lämnar ut identifieringsuppgifter om en person ur befolkningsdatasystemet,

5) sådana identifieringstjänster och samlade förvaltningstjänster för identifiering där även någon annan metod för identifiering än sådan stark autentisering som avses i lagen om stark autentisering *och betrodda elektroniska tjänster* kan användas,

I tjänsten för identifiering av fysiska personer får en person identifieras också med en sådan metod för identifiering som hör till de medel för elektronisk identifiering som ska erkännas ömsesidigt enligt artikel 6 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG. I det

Föreslagen lydelse

3 §

Stödtjänster

De gemensamma stödtjänsterna för e-tjänster omfattar

4) en sådan tjänst för identifiering av fysiska personer som identifierar en fysisk person som använder den offentliga förvaltningens e-tjänster med hjälp av en tjänst som tillhandahålls av en sådan leverantör av identifieringstjänster som avses i lagen om stark autentisering (617/2009), administrerar identifieringstransaktionen och till användarorganisationen lämnar ut identifieringsuppgifter om en person ur befolkningsdatasystemet,

5) sådana identifieringstjänster och samlade förvaltningstjänster för identifiering där även någon annan metod för identifiering än sådan stark autentisering som avses i lagen om stark autentisering kan användas,

I tjänsten för identifiering av fysiska personer får en person identifieras också med en sådan metod för identifiering som hör till de medel för elektronisk identifiering som ska erkännas ömsesidigt enligt *artiklarna 5f eller* 6 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, *sådan*

Gällande lydelse

fallet får det ur tjänsten för identifiering av fysiska personer till användarorganisationen lämnas ut också sådana identifieringsuppgifter om en person som i samband med identifieringstransaktionen förmedlas från en annan medlemsstat.

— — — — —

Föreslagen lydelse

den lyder senast ändrad genom förordning (EU) 2024/1183. I det fallet får det ur tjänsten för identifiering av fysiska personer till användarorganisationen lämnas ut också sådana identifieringsuppgifter om en person som i samband med identifieringstransaktionen förmedlas från en annan medlemsstat.

— — — — —

Denna lag träder i kraft den 20 .

6.

Lag

om ändring av 1 § i lagen om verkställighet av böter

I enlighet med riksdagens beslut
ändras i lagen om verkställighet av böter (672/2002) 1 § 2 mom. 63 punkten, sådan den lyder
i lag 1379/2025, och
fogas till 1 § 2 mom., sådant det lyder i lagarna 416/2025, 860/2025, 979/2025, 1080/2025,
1149/2025 och 1379/2025, en ny 64 punkt som följer:

Gällande lydelse

1 §

Lagens tillämpningsområde

Denna lag innehåller bestämmelser om
verkställighet av följande administrativa
påföljder av straffkaraktär:

63) påföljdsavgifter enligt 4 kap. i lagen om
tillsyn över vissa system för artificiell
intelligens (1377/2025).

Föreslagen lydelse

1 §

Lagens tillämpningsområde

Denna lag innehåller bestämmelser om
verkställighet av följande administrativa
påföljder av straffkaraktär:

63) påföljdsavgifter enligt 4 kap. i lagen om
tillsyn över vissa system för artificiell
intelligens (1377/2025),

64) påföljdsavgift enligt 42–46 § i lagen om
vissa tjänster som möjliggör
gränsöverskridande e-tjänster (/).

Denna lag träder i kraft den 20 .

7.

Lag

om ändring av lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata

I enlighet med riksdagens beslut

ändras i lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata (661/2009) 2 § 2 mom. 2 punkten, 28 § 1 mom., 43 § 2 mom. 1 och 2 punkten, 62 §, 63 § 2 mom. 1 punkten, 66 § 2 och 3 mom. och 67 § 1 mom., sådana de lyder, 2 § 2 mom. 2 punkten, 28 § 1 mom. och 66 § 2 och 3 mom. i lag 55/2019, 43 § 2 mom. 1 punkten, 63 § 2 mom. 1 punkten och 67 § 1 mom. i lag 1175/2019, 43 § 2 mom. 2 punkten i lag 538/2016 och 62 § i lagarna 538/2016 och 1175/2019, som följer:

Gällande lydelse

2 §

Lagens tillämpningsområde

Om inte något annat föreskrivs i denna lag, ska följande lagar och rättsakter tillämpas:

2) i fråga om certifierad elektronisk kommunikation och behandlingen av uppgifter i det certifikatregister som avses i denna lag, lagen om stark autentisering och betrodda elektroniska tjänster (617/2009).

28 §

Allmänna förutsättningar för utlämnande av uppgifter

Uppgifter i befolkningsdatasystemet får lämnas ut endast om förutsättningarna för utlämnande av uppgifter enligt denna lag är uppfyllda. Det krävs att de uppgifter som lämnas ut ur befolkningsdatasystemet behövs för det ändamål för vilket de lämnas ut. När uppgifter som hör till kategorierna av särskilda personuppgifter lämnas ut ska det säkerställas att mottagaren har rätt att behandla uppgifterna med stöd av dataskyddsförordningen eller dataskyddslagen.

Föreslagen lydelse

2 §

Lagens tillämpningsområde

Om inte något annat föreskrivs i denna lag, ska följande lagar och rättsakter tillämpas:

2) i fråga om certifierad elektronisk kommunikation och behandling av uppgifter i det certifikatregister som avses i denna lag, lagen om stark autentisering (617/2009).

28 §

Allmänna förutsättningar för utlämnande av uppgifter

Uppgifter i befolkningsdatasystemet får lämnas ut endast om förutsättningarna för utlämnande av uppgifter enligt denna lag är uppfyllda. Det krävs att de uppgifter som lämnas ut ur befolkningsdatasystemet behövs för det ändamål för vilket de lämnas ut. När uppgifter som hör till kategorierna av särskilda personuppgifter lämnas ut ska det säkerställas att mottagaren har rätt att behandla uppgifterna med stöd av dataskyddsförordningen eller dataskyddslagen (1050/2018).

Gällande lydelse

43 §

Utlämnande av identifieringsuppgifter

Elektroniska kommunikationskoder som registrerats i befolkningsdatasystemet får lämnas ut endast om

1) koden används som en uppgift som identifierar innehavaren av ett certifikat i samband med produktion av tjänster eller prestationer som baserar sig på användningen av medborgarcertifikat eller andra certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för fysiska personer, eller

2) en annan i Finland etablerad certifikatutfärdare använder koden som en uppgift som identifierar innehavaren av certifikatet i certifikat som avses i lagen om stark autentisering och betrodda tjänster eller i motsvarande certifikat som används i identifieringssyfte.

62 §

Uppgifter som ska ingå i certifikat för certifierad elektronisk kommunikation

Bestämmelser om vilka uppgifter som ska ingå i medborgarcertifikat och andra certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för fysiska personer finns i lagen om stark autentisering och betrodda elektroniska tjänster och i EU:s förordning om elektronisk identifiering. Medborgarcertifikat ska innehålla en elektronisk kommunikationskod som identifierar innehavaren av certifikatet. Andra certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för fysiska personer ska innehålla en elektronisk kommunikationskod som identifierar

Föreslagen lydelse

43 §

Utlämnande av identifieringsuppgifter

Elektroniska kommunikationskoder som registrerats i befolkningsdatasystemet får lämnas ut endast om

1) koden används som en uppgift som identifierar innehavaren av ett certifikat *eller innehavaren av identifieringsuppgifter för en fysisk person i samband med produktion av tjänster* eller prestationer som baserar sig på användningen av medborgarcertifikat eller andra certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för fysiska personer eller på identifieringsuppgifter för fysiska personer som Myndigheten för digitalisering och befolkningsdata utfärdar med stöd av lagen om vissa tjänster som möjliggör gränsoverskridande e-tjänster (/), eller

2) en annan *än i 1 punkten avsedd* i Finland etablerad certifikatutfärdare använder koden som en uppgift som identifierar innehavaren av certifikatet i certifikat som avses i lagen om stark autentisering eller i motsvarande certifikat som används i identifieringssyfte.

62 §

Uppgifter som ska ingå i certifikat för certifierad elektronisk kommunikation

Bestämmelser om vilka uppgifter som ska ingå i medborgarcertifikat och andra certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för fysiska personer finns i lagen om stark autentisering och i EU:s förordning om elektronisk identifiering. Medborgarcertifikat ska innehålla en elektronisk kommunikationskod som identifierar innehavaren av certifikatet. Andra certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för fysiska personer ska innehålla en elektronisk kommunikationskod som identifierar innehavaren av certifikatet eller någon annan

Gällande lydelse

innehavaren av certifikatet eller någon annan identifieringsuppgift som identifierar personen och som inte innehåller information om personen. Även andra nödvändiga tekniska uppgifter som behövs vid användningen av ett certifikat kan ingå i medborgarcertifikat och andra certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för fysiska personer. Beslut om dessa uppgifter fattas av Myndigheten för digitalisering och befolkningsdata.

En elektronisk kommunikationskod kan också ingå i andra i lagen om stark autentisering och betrodda tjänster avsedda certifikat för fysiska personer som en uppgift som identifierar innehavaren av certifikatet.

63 §

Tekniska identifieringskoder och elektroniska kommunikationskoder samt skapande av dessa

Myndigheten för digitalisering och befolkningsdata ska ändra en teknisk identifieringskod till en individuell elektronisk kommunikationskod när

1) ett medborgarcertifikat eller ett annat certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för fysiska personer första gången utfärdas för en person, eller

66 §

Ansökan om och utfärdande av medborgarcertifikat

På ansökan om medborgarcertifikat som ingår i ett identitetskort tillämpas lagen om identitetskort. På ansökan om medborgarcertifikat som ingår i en annan

Föreslagen lydelse

identifieringsuppgift som identifierar personen och som inte innehåller information om personen. Även andra nödvändiga tekniska uppgifter som behövs vid användningen av ett certifikat kan ingå i medborgarcertifikat och andra certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för fysiska personer. Beslut om dessa uppgifter fattas av Myndigheten för digitalisering och befolkningsdata.

En elektronisk kommunikationskod kan också ingå i andra i lagen om stark autentisering avsedda certifikat för fysiska personer som en uppgift som identifierar innehavaren av certifikatet.

63 §

Tekniska identifieringskoder och elektroniska kommunikationskoder samt skapande av dessa

Myndigheten för digitalisering och befolkningsdata ska ändra en teknisk identifieringskod till en individuell elektronisk kommunikationskod när

1) ett medborgarcertifikat eller ett annat certifikat som Myndigheten för digitalisering och befolkningsdata utfärdar för fysiska personer eller identifieringsuppgifter för fysiska personer som Myndigheten för digitalisering och befolkningsdata utfärdar med stöd av lagen om vissa tjänster som möjliggör gränsöverskridande e-tjänster första gången utfärdas för en person, eller

66 §

Ansökan om och utfärdande av medborgarcertifikat

På ansökan om medborgarcertifikat som ingår i ett identitetskort tillämpas lagen om identitetskort. På ansökan om medborgarcertifikat som ingår i en annan

Gällande lydelse

myndighetshandling eller ett tekniskt underlag tillämpas förfarandet enligt 67 § 2 och 3 mom., de krav i dataskyddsförordningen och dataskyddslagen som gäller behandlingen av personuppgifter samt de krav i lagen om stark autentisering och betrodda elektroniska tjänster som gäller utfärdande av certifikat.

Den som tar emot ansökan ska iaktta de krav i dataskyddsförordningen och dataskyddslagen som gäller behandlingen av personuppgifter och de krav i lagen om stark autentisering och betrodda elektroniska tjänster och i EU:s förordning om elektronisk identifiering som gäller utfärdande av certifikat.

67 §

Ansökan om och utfärdande av andra certifikat

Andra certifikat för fysiska personer som Myndigheten för digitalisering och befolkningsdata producerar och som inte är medborgarcertifikat kan utfärdas endast för finska medborgare samt för utlänningar som enligt lagen om hemkommun är stadigvarande bosatta i Finland och vars uppgifter har registrerats i befolkningsdatasystemet och vars identitet har kunnat konstateras på ett tillförlitligt sätt. Andra certifikat än medborgarcertifikat som Myndigheten för digitalisering och befolkningsdata producerar för fysiska personer kan av särskilda och motiverade skäl också beviljas personer vars identitet har kunnat konstateras tillförlitligt även om de inte uppfyller övriga ovannämnda förutsättningar för att få certifikat. Sådana certifikat kan på sökandens begäran ingå i handlingar, kort och tekniska underlag som används vid elektronisk kommunikation och som utfärdas av en myndighet, ett företag eller en organisation. Myndigheten för digitalisering och befolkningsdata kan komma överens med en myndighet, ett företag eller en organisation som utfärdar handlingar eller tekniska underlag om att ansökningar om certifikat personligen kan lämnas in till myndigheten, företaget eller organisationen för vidarebefordran till Myndigheten för

Föreslagen lydelse

myndighetshandling eller ett tekniskt underlag tillämpas förfarandet enligt 67 § 2 och 3 mom. i denna lag, de krav i dataskyddsförordningen och dataskyddslagen som gäller behandlingen av personuppgifter samt de krav i lagen om stark autentisering som gäller utfärdande av certifikat.

Den som tar emot ansökan ska iaktta de krav i dataskyddsförordningen och dataskyddslagen som gäller behandlingen av personuppgifter och de krav i lagen om stark autentisering och i EU:s förordning om elektronisk identifiering som gäller utfärdande av certifikat.

67 §

Ansökan om och utfärdande av andra certifikat

Andra certifikat för fysiska personer som Myndigheten för digitalisering och befolkningsdata producerar och som inte är medborgarcertifikat kan utfärdas endast för finska medborgare samt för utlänningar som enligt lagen om hemkommun är stadigvarande bosatta i Finland och vars uppgifter har registrerats i befolkningsdatasystemet och vars identitet har kunnat konstateras på ett tillförlitligt sätt. Andra certifikat än medborgarcertifikat som Myndigheten för digitalisering och befolkningsdata producerar för fysiska personer kan av särskilda och motiverade skäl också beviljas personer vars identitet har kunnat konstateras tillförlitligt även om de inte uppfyller övriga ovannämnda förutsättningar för att få certifikat. Sådana certifikat kan på sökandens begäran ingå i handlingar, kort och tekniska underlag som används vid elektronisk kommunikation och som utfärdas av en myndighet, ett företag eller en organisation. Myndigheten för digitalisering och befolkningsdata kan komma överens med en myndighet, ett företag eller en organisation som utfärdar handlingar eller tekniska underlag om att ansökningar om certifikat personligen kan lämnas in till myndigheten, företaget eller organisationen för vidarebefordran till Myndigheten för

Gällande lydelse

digitalisering och befolkningsdata. Myndigheten för digitalisering och befolkningsdata ska då se till att den som tar emot ansökan iakttar vad som i dataskyddsförordningen och dataskyddslagen föreskrivs om behandlingen av personuppgifter och vad som i lagen om stark autentisering och betrodda elektroniska tjänster och i EU:s förordning om elektronisk identifiering föreskrivs om utfärdande av certifikat.

Föreslagen lydelse

digitalisering och befolkningsdata. Myndigheten för digitalisering och befolkningsdata ska då se till att den som tar emot ansökan iakttar vad som i dataskyddsförordningen och dataskyddslagen föreskrivs om behandlingen av personuppgifter och vad som i lagen om stark autentisering och i EU:s förordning om elektronisk identifiering föreskrivs om utfärdande av certifikat.

Denna lag träder i kraft den 20 .

8.

Lag

om ändring av 8 och 65 § i lagen om behandling av kunduppgifter inom social- och hälsovården

I enlighet med riksdagens beslut
ändras i lagen om behandling av kunduppgifter inom social- och hälsovården (703/2023) 8 § 2 mom. och 65 § 3 mom., av dem 65 § 3 mom. sådant det lyder i lag 764/2025, som följer:

Gällande lydelse

8 §

*Identifiering av dem som deltar i
behandlingen av kunduppgifter*

Tjänstetillhandahållaren, apoteket, Folkpensionsanstalten samt producenten av informationssystemtjänsten och tillverkaren av informationssystemet samt mellanhanden ska kontrollera att identifieringsverktygen för personer som behandlar kunduppgifter och som används för identifiering av informationstekniska enheter är i kraft med iakttagande av 25 § 4–6 mom. i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009), nedan *autentiseringslagen*.

65 §

*De riksomfattande
informationssystemtjänsterna inom social-
och hälsovården*

Myndigheten för digitalisering och befolkningsdata är certifikatutfärdare i enlighet med lagen om stark autentisering och betrodda elektroniska tjänster för yrkesutbildade personer inom social- och hälsovården och annan personal inom social- och hälsovården, tjänstetillhandahållare inom social- och hälsovården samt organisationer som deltar i tillhandahållandet av dessa tjänster, deras personal och datatekniska

Föreslagen lydelse

8 §

*Identifiering av dem som deltar i
behandlingen av kunduppgifter*

Tjänstetillhandahållaren, apoteket, Folkpensionsanstalten samt producenten av informationssystemtjänsten och tillverkaren av informationssystemet samt mellanhanden ska kontrollera att identifieringsverktygen för personer som behandlar kunduppgifter och som används för identifiering av informationstekniska enheter är i kraft med iakttagande av 25 § 4–6 mom. i lagen om stark autentisering (617/2009), nedan *autentiseringslagen*.

65 §

*De riksomfattande
informationssystemtjänsterna inom social-
och hälsovården*

Myndigheten för digitalisering och befolkningsdata är certifikatutfärdare i enlighet med *autentiseringslagen* för yrkesutbildade personer inom social- och hälsovården och annan personal inom social- och hälsovården, tjänstetillhandahållare inom social- och hälsovården samt organisationer som deltar i tillhandahållandet av dessa tjänster, deras personal och datatekniska enheter. Myndigheten för digitalisering och

Gällande lydelse

enheter. Myndigheten för digitalisering och befolkningsdata har rätt att för skötseln av dessa uppgifter av Tillstånds- och tillsynsverket få den information som behövs för utfärdande och återkallande av certifikat, för certifikat, för det tekniska underlaget för certifikat och för sändande av certifikat, ur centralregistret över yrkesutbildade personer inom hälso- och sjukvården som verket upprätthåller.

Föreslagen lydelse

befolkningsdata har rätt att för skötseln av dessa uppgifter av Tillstånds- och tillsynsverket få den information som behövs för utfärdande och återkallande av certifikat, för certifikat, för det tekniska underlaget för certifikat och för sändande av certifikat, ur centralregistret över yrkesutbildade personer inom hälso- och sjukvården som verket upprätthåller.

Denna lag träder i kraft den 20 .

9.

Lag

om ändring av 3 kap. 11 § i lagen om förhindrande av penningtvätt och av finansiering av terrorism

I enlighet med riksdagens beslut
ändras i lagen om förhindrande av penningtvätt och av finansiering av terrorism (444/2017)
3 kap. 11 § 3 punkten som följer:

Gällande lydelse

3 kap.

Kundkontroll

11 §

Skärpta åtgärder för kundkontroll vid identifiering på distans

Om kunden inte är närvarande vid identifieringen och identitetskontrollen (identifiering på distans) ska den rapporteringsskyldiga vidta följande åtgärder för att minska risken för penningtvätt och finansiering av terrorism:

3) kontrollera en kunds identitet med ett identifieringsverktyg enligt lagen om stark autentisering *och elektroniska signaturer* (617/2009) eller med ett kvalificerat certifikat för elektroniska underskrifter enligt artikel 28 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG eller med någon annan elektronisk identifieringsteknik som är datasäker och bevislig.

Föreslagen lydelse

3 kap.

Kundkontroll

11 §

Skärpta åtgärder för kundkontroll vid identifiering på distans

Om kunden inte är närvarande vid identifieringen och identitetskontrollen (*identifiering på distans*) ska den rapporteringsskyldiga vidta följande åtgärder för att minska risken för penningtvätt och finansiering av terrorism:

3) kontrollera en kunds identitet med ett identifieringsverktyg enligt lagen om stark autentisering (617/2009) eller med ett kvalificerat certifikat för elektroniska underskrifter enligt artikel 28 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, *sådan den lyder senast ändrad genom förordning (EU) 2024/1183*, eller med någon annan elektronisk identifieringsteknik som är datasäker och bevislig.

Denna lag träder i kraft den 20 .

10.

Lag

om ändring av 9 a kap. 1 § i jordabalken

I enlighet med riksdagens beslut
ändras i jordabalken (540/1995) 9 a kap. 1 § 1 mom., sådant det lyder i lag 536/2016, som
följer:

Gällande lydelse

9 a kap.

Elektroniska ärendehanteringssystem och deras användning

1 §

Användning av ärendehanteringssystem och elektronisk identifiering i ett ärendehanteringssystem

En förutsättning för att upprätta och godkänna elektroniska dokument i ett ärendehanteringssystem samt för att i övrigt använda ärendehanteringssystemet är att användaren identifieras på ett tillförlitligt sätt med hjälp av en sådan identifieringsmetod, tillhandahållen av en leverantör av tjänster för stark autentisering, som avses i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) eller ett sådant kvalificerat certifikat för elektronisk underskrift som föreskrivs i artikel 28 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, eller med hjälp av någon annan identifieringsteknik som är datatekniskt tillförlitlig och bevislig.

Föreslagen lydelse

9 a kap.

Elektroniska ärendehanteringssystem och deras användning

1 §

Användning av ärendehanteringssystem och elektronisk identifiering i ett ärendehanteringssystem

En förutsättning för att upprätta och godkänna elektroniska dokument i ett ärendehanteringssystem samt för att i övrigt använda ärendehanteringssystemet är att användaren identifieras på ett tillförlitligt sätt med hjälp av en sådan identifieringsmetod, tillhandahållen av en leverantör av tjänster för stark autentisering, som avses i lagen om stark autentisering (617/2009) eller ett sådant kvalificerat certifikat för elektronisk underskrift som föreskrivs i artikel 28 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, sådan den lyder senast ändrad genom förordning (EU) 2024/1183, eller med hjälp av någon annan identifieringsteknik som är datatekniskt tillförlitlig och bevislig.

Gällande lydelse

Föreslagen lydelse

Denna lag träder i kraft den 20 .

11.

Lag

om ändring av 7 § i lagen om medborgarinitiativ

I enlighet med riksdagens beslut
ändras i lagen om medborgarinitiativ (12/2012) 7 § 1 mom. 1 punkten, sådan den lyder i lag
1276/2019, som följer:

Gällande lydelse

7 §

Tekniska krav på elektroniskt förfarande

Elektronisk insamling av stödförklaringar i ett datanät ska ske med utnyttjande av datasystem som har godkänts av Transport- och kommunikationsverket. En förutsättning för godkännande är att

1) insamlingen av stödförklaringar sker genom utnyttjande av sådan stark autentisering som avses i lagen om stark autentisering *och betrodda elektroniska tjänster* (617/2009),

Föreslagen lydelse

7 §

Tekniska krav på elektroniskt förfarande

Elektronisk insamling av stödförklaringar i ett datanät ska ske med utnyttjande av datasystem som har godkänts av Transport- och kommunikationsverket. En förutsättning för godkännande är att

1) insamlingen av stödförklaringar sker genom utnyttjande av sådan stark autentisering som avses i lagen om stark autentisering (617/2009),

Denna lag träder i kraft den 20 .

12.

Lag

om ändring av 4 § i lagen om förfarandet vid rådgivande folkomröstningar i velfärdsområden och kommuner

I enlighet med riksdagens beslut
ändras i lagen om förfarandet vid rådgivande folkomröstningar i velfärdsområden och
kommuner (656/1990) 4 § 3 mom., sådant det lyder i lag 652/2021, som följer:

Gällande lydelse

4 §

Initiativ till folkomröstning

Insamlingen av stödförklaringar på
elektronisk väg i ett datanät ska ske med hjälp
av stark autentisering enligt lagen om stark
autentisering *och betrodda elektroniska
tjänster* (617/2009).

Föreslagen lydelse

4 §

Initiativ till folkomröstning

Insamlingen av stödförklaringar på
elektronisk väg i ett datanät ska ske med hjälp
av stark autentisering enligt lagen om stark
autentisering (617/2009).

Denna lag träder i kraft den 20 .

13.

Lag

om ändring av 15 och 26 § i lagen om fonderna inom området för inrikes frågor under programperioden 2021–2027

I enlighet med riksdagens beslut
ändras i lagen om fonderna inom området för inrikes frågor under programperioden 2021–2027 (1125/2021) 15 § 4 mom. och 26 § 3 mom., sådana de lyder i lag 1293/2022, som följer:

Gällande lydelse

15 §

Ansökan om understöd

På undertecknandet av ansökan tillämpas vad som i lagen om stark autentisering *och betrodda elektroniska tjänster* (617/2009) föreskrivs om identifiering och autentisering. Om ansökan har gjorts på en blankett som godkänts av den förvaltande myndigheten, ska ansökan undertecknas.

26 §

E-tjänst- och behandlingssystemet för programmet för fonderna inom området för inrikes frågor samt behandling av uppgifter

Varje användare av informationssystemet ska identifiera sig med hjälp av sådan stark autentisering som avses i 2 § 1 mom. 1 punkten i lagen om stark autentisering *och betrodda elektroniska tjänster*.

Föreslagen lydelse

15 §

Ansökan om understöd

På undertecknandet av ansökan tillämpas vad som i lagen om stark autentisering (617/2009) föreskrivs om identifiering och autentisering av en person. Om ansökan har gjorts på en blankett som godkänts av den förvaltande myndigheten, ska ansökan undertecknas.

26 §

E-tjänst- och behandlingssystemet för programmet för fonderna inom området för inrikes frågor samt behandling av uppgifter

Varje användare av informationssystemet ska identifiera sig med hjälp av sådan stark autentisering som avses i 2 § 1 punkten i lagen om stark autentisering.

Denna lag träder i kraft den 20 .

14.

Lag

om ändring av lagen om identitetskort

I enlighet med riksdagens beslut
ändras i lagen om identitetskort (663/2016) 11 § 4 mom. och
fogas till lagen en ny 1 a § som följer:

Gällande lydelse

Föreslagen lydelse

1 a §

E-legitimation

*I identitetskort som avses i 2 § 1 mom., 14
och 15 a § samt 17 § 3 mom. ingår en rätt att
få tillgång till en e-legitimation som avses i
lagen om e-legitimation (/).*

11 §

11 §

*Identifiering av sökanden och verifiering av
sökandens identitet*

*Identifiering av sökanden och verifiering av
sökandens identitet*

Elektronisk kommunikation förutsätter ett
sådan identifieringsverktyg som avses i lagen
om stark autentisering och betrodda
elektroniska tjänster (617/2009).

Elektronisk kommunikation förutsätter ett
sådan identifieringsverktyg som avses i lagen
om stark autentisering (617/2009).

*Denna lag träder i kraft den 20 .
Rätten att få tillgång till en e-legitimation
ingår i sådana identitetskort som avses i 1 a §
och som har utfärdats före ikraftträdandet av
denna lag.*

15.

Lag

om ändring av 3 § i partilagen

I enlighet med riksdagens beslut
ändras i partilagen (10/1969) 3 § 1 mom., sådant det lyder i lag 904/2020, som följer:

Gällande lydelse

3 §

Registreringsansökan

En förening kan göra en registreringsansökan i en webbtjänst som drivs av justitieministeriet, i vilken det används stark autentisering enligt lagen om stark autentisering *och betrodda elektroniska tjänster* (617/2009), eller på annat sätt skriftligen.

Föreslagen lydelse

3 §

Registreringsansökan

En förening kan göra en registreringsansökan i en webbtjänst som drivs av justitieministeriet, i vilken det används stark autentisering enligt lagen om stark autentisering (617/2009), eller på annat sätt skriftligen.

Denna lag träder i kraft den 20 .

16.

Lag

om ändring av 52 § i lagen om finansiering av projekt inom regionutveckling och Europeiska unionens regional- och strukturpolitik

I enlighet med riksdagens beslut
ändras i lagen om finansiering av projekt inom regionutveckling och Europeiska unionens regional- och strukturpolitik (757/2021) 52 § som följer:

Gällande lydelse

52 §

Stark autentisering vid användning av informationssystemet för Europeiska unionens regional- och strukturpolitiska program

Varje användare av det informationssystem som avses i 50 § ska identifiera sig med hjälp av stark autentisering. Bestämmelser om stark autentisering finns i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009). Offentliga uppgifter som avses i 54 § 2 mom. får dock granskas utan stark autentisering.

Föreslagen lydelse

52 §

Stark autentisering vid användning av informationssystemet för Europeiska unionens regional- och strukturpolitiska program

Varje användare av det informationssystem som avses i 50 § ska identifiera sig med hjälp av stark autentisering. Bestämmelser om stark autentisering finns i lagen om stark autentisering (617/2009). Offentliga uppgifter som avses i 54 § 2 mom. får dock granskas utan stark autentisering.

Denna lag träder i kraft den 20 .

17.

Lag

om ändring av passlagen

I enlighet med riksdagens beslut
ändras i passlagen (671/2006) 6 § 4 mom., sådant det lyder i lag 966/2014, och
fogas till lagen en ny 3 d § som följer:

Gällande lydelse

Föreslagen lydelse

3 d §

E-legitimation

*I pass som avses i 3 och 3 c samt 4 § ingår
en rätt att få tillgång till en e-legitimation som
avses i lagen om e-legitimation (/).*

6 §

6 §

Ansökan om pass

Ansökan om pass

Till ansökan ska fogas sökandens
ansiktsbild, på vilken sökanden utan svårighet
kan kännas igen. Sökanden ska som
identifieringshandling uppvisa en giltig
handling där sökandens identitet framgår. Om
sökanden inte kan uppvisa en
identifieringshandling, utförs identifieringen
av den myndighet som utfärdar passet.
Elektronisk kommunikation förutsätter ett
sådant identifieringsverktyg som avses i lagen
om stark autentisering och elektroniska
signaturer (617/2009).

Till ansökan ska fogas sökandens
ansiktsbild, på vilken sökanden utan svårighet
kan kännas igen. Sökanden ska som
identifieringshandling uppvisa en giltig
handling där sökandens identitet framgår. Om
sökanden inte kan uppvisa en
identifieringshandling, utförs identifieringen
av den myndighet som utfärdar passet.
Elektronisk kommunikation förutsätter ett
sådant identifieringsverktyg som avses i lagen
om stark autentisering (617/2009).

*Denna lag träder i kraft den 20 .
Rätten att få tillgång till en e-legitimation
ingår också i pass som har utfärdats före
ikraftträdandet av denna lag och som avses i
3 d §.*

18.

Lag

om ändring av 31 § i lagen om stödjande av landsbygdens utveckling under finansieringsperioden 2023–2027

I enlighet med riksdagens beslut
ändras i lagen om stödjande av landsbygdens utveckling under finansieringsperioden 2023–2027 (1325/2022) 31 § 1 mom. enligt följande:

Gällande lydelse

31 §

Ansökan om stöd

Ansökan om stöd görs elektroniskt via en nättjänst som utgör en del av den informationsresurs för livsmedelsförvaltningen som avses i lagen om livsmedelsförvaltningens informationsresurs (560/2021). Sökanden identifieras genom stark autentisering på det sätt som föreskrivs i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009).

Föreslagen lydelse

31 §

Ansökan om stöd

Ansökan om stöd görs elektroniskt via en nättjänst som utgör en del av den informationsresurs för livsmedelsförvaltningen som avses i lagen om livsmedelsförvaltningens informationsresurs (560/2021). Sökanden identifieras genom stark autentisering *i enlighet med lagen om stark autentisering* (617/2009).

Denna lag träder i kraft den 20 .

19.

Lag

om ändring av 12 § i lagen om verkställighet av vissa av Europeiska unionens jordbruksstöd och vissa nationella jordbruksstöd

I enlighet med riksdagens beslut
ändras i lagen om verkställighet av vissa av Europeiska unionens jordbruksstöd och vissa nationella jordbruksstöd (1334/2022) 12 § 1 mom. som följer:

Gällande lydelse

12 §

Ansökan om stöd

Ansökningar om stöd görs elektroniskt i en nättjänst som utgör en del av livsmedelsförvaltningens informationsresurs, som avses i lagen om livsmedelsförvaltningens informationsresurs (560/2021). Sökanden eller sökandena identifieras genom stark autentisering på det sätt som föreskrivs i lagen om stark autentisering *och betrodda elektroniska tjänster* (617/2009). Vad som i denna lag föreskrivs om ansökan om stöd gäller även anmälan som gäller stöd.

Föreslagen lydelse

12 §

Ansökan om stöd

Ansökningar om stöd görs elektroniskt i en nättjänst som utgör en del av livsmedelsförvaltningens informationsresurs, som avses i lagen om livsmedelsförvaltningens informationsresurs (560/2021). Sökanden eller sökandena identifieras genom stark autentisering *i enlighet med lagen om stark autentisering* (617/2009). Vad som i denna lag föreskrivs om ansökan om stöd gäller även anmälan som gäller stöd.

Denna lag träder i kraft den 20 .

20.

Lag

om ändring av 32 § i lagen om det nationella genomförandet av Europeiska unionens gemensamma fiskeripolitik

I enlighet med riksdagens beslut
ändras i lagen om det nationella genomförandet av Europeiska unionens gemensamma fiskeripolitik (1048/2016) 32 § 2 mom., sådant det lyder i lag 3/2023, som följer:

Gällande lydelse

32 §

*Innehavarens rätt att använda uppgifterna i
fiskekvotsregistret*

För att ta del av uppgifter samt för
överföringar i den elektroniska tjänsten krävs
det sådan stark autentisering som avses i 2 § 1
mom. I punkten i lagen om stark autentisering
och *betrodda elektroniska tjänster*
(617/2009).

Föreslagen lydelse

32 §

*Innehavarens rätt att använda uppgifterna i
fiskekvotsregistret*

För att ta del av uppgifter samt för
överföringar i den elektroniska tjänsten krävs
det sådan stark autentisering som avses i 2 § *1*
punkten i lagen om stark autentisering
(617/2009).

Denna lag träder i kraft den 20 .

21.

Lag

om ändring av 41 § i lagen om behandling av personuppgifter i polisens verksamhet

I enlighet med riksdagens beslut
ändras i lagen om behandling av personuppgifter i polisens verksamhet (616/2019) 41 § 2 mom. som följer:

Gällande lydelse

41 §

*Tillgodoseende av den registrerades rätt till
insyn*

En registrerad som vill utöva sin rätt till insyn ska framställa en personlig begäran om detta till den personuppgiftsansvarige eller någon annan i 1 mom. avsedd polisenhet samt styrka sin identitet. En begäran kan också framställas genom att använda sådan stark autentisering som avses i lagen om stark autentisering *och betrodde elektroniska tjänster* (617/2009), om en sådan tjänst är tillgänglig.

Föreslagen lydelse

41 §

*Tillgodoseende av den registrerades rätt till
insyn*

En registrerad som vill utöva sin rätt till insyn ska framställa en personlig begäran om detta till den personuppgiftsansvarige eller någon annan i 1 mom. avsedd polisenhet samt styrka sin identitet. En begäran kan också framställas genom att använda sådan stark autentisering som avses i lagen om stark autentisering (617/2009), om en sådan tjänst är tillgänglig.

Denna lag träder i kraft den 20 .

22.

Lag

om ändring av 35 § i lagen om behandling av personuppgifter inom Tullen

I enlighet med riksdagens beslut
ändras i lagen om behandling av personuppgifter inom Tullen (650/2019) 35 § 2 mom. som följer:

Gällande lydelse

35 §

Tillgodoseende av den registrerades rätt till insyn

En registrerad som vill utöva sin rätt till insyn ska framställa en personlig begäran om detta till den personuppgiftsansvarige eller *någon annan* i 1 mom. avsedd verksamhetsenhet inom Tullen samt styrka sin identitet. En begäran kan också framställas genom att använda sådan stark autentisering som avses i lagen om stark autentisering *och betrodda elektroniska tjänster* (617/2009), om en sådan tjänst är tillgänglig.

Föreslagen lydelse

35 §

Tillgodoseende av den registrerades rätt till insyn

En registrerad som vill utöva sin rätt till insyn ska framställa en personlig begäran om detta till den personuppgiftsansvarige eller en i 1 mom. avsedd verksamhetsenhet inom Tullen samt styrka sin identitet. En begäran kan också framställas genom att använda sådan stark autentisering som avses i lagen om stark autentisering (617/2009), om en sådan tjänst är tillgänglig.

Denna lag träder i kraft den 20 .

23.

Lag

om ändring av 29 § i lagen om strukturstöd till jordbruket

I enlighet med riksdagens beslut
ändras i lagen om strukturstöd till jordbruket (1476/2007) 29 § 1 mom., sådant det lyder i lag 1328/2022, som följer:

Gällande lydelse

29 §

Ansökan om stöd

Stöd ska sökas elektroniskt via en nättjänst som utgör en del av den informationsresurs för livsmedelsförvaltningen som avses i lagen om livsmedelsförvaltningens informationsresurs (560/2021). Sökanden identifieras genom stark autentisering på det sätt som föreskrivs i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009).

Föreslagen lydelse

29 §

Ansökan om stöd

Stöd ska sökas elektroniskt via en nättjänst som utgör en del av den informationsresurs för livsmedelsförvaltningen som avses i lagen om livsmedelsförvaltningens informationsresurs (560/2021). Sökanden identifieras genom stark autentisering *i enlighet med lagen om stark autentisering* (617/2009).

Denna lag träder i kraft den 20 .

24.

Lag

om ändring av 50 § i lagen om behandling av personuppgifter vid Gränsbevakningsväsendet

I enlighet med riksdagens beslut
ändras i lagen om behandling av personuppgifter vid Gränsbevakningsväsendet (639/2019)
50 § 2 mom. som följer:

Gällande lydelse

50 §

*Tillgodoseende av den registrerades rätt till
insyn*

En registrerad som vill utöva sin rätt till insyn ska framställa en personlig begäran om detta till den personuppgiftsansvarige eller någon annan i 1 mom. avsedd myndighet samt styrka sin identitet. En begäran kan också framställas med användning av stark autentisering enligt lagen om stark autentisering *och betrodda elektroniska tjänster* (617/2009), om en sådan tjänst är tillgänglig.

Föreslagen lydelse

50 §

*Tillgodoseende av den registrerades rätt till
insyn*

En registrerad som vill utöva sin rätt till insyn ska framställa en personlig begäran om detta till den personuppgiftsansvarige eller någon annan i 1 mom. avsedd myndighet samt styrka sin identitet. En begäran kan också framställas med användning av stark autentisering enligt lagen om stark autentisering (617/2009), om en sådan tjänst är tillgänglig.

Denna lag träder i kraft den 20 .

25.

Lag

om ändring av 70 a § i lagen om en marknadsordning för jordbruksprodukter

I enlighet med riksdagens beslut
ändras i lagen om en marknadsordning för jordbruksprodukter (999/2012) 70 a § 1 mom.,
sådant det lyder i lag 1336/2022, som följer:

Gällande lydelse

70 a §

Elektronisk ansökan

Det kan förutsättas att stöd söks elektroniskt i en nättjänst som utgör en del av livsmedelsförvaltningens informationsresurs, som avses i lagen om livsmedelsförvaltningens informationsresurs. Sökanden identifieras genom stark autentisering på det sätt som föreskrivs i lagen om stark autentisering *och betrodda elektroniska tjänster* (617/2009). Genom förordning av statsrådet föreskrivs om sådana stöd enligt denna lag beträffande vilka ansökan kan göras bara på det sätt som avses i denna paragraf.

Föreslagen lydelse

70 a §

Elektronisk ansökan

Det kan förutsättas att stöd söks elektroniskt i en nättjänst som utgör en del av livsmedelsförvaltningens informationsresurs, som avses i lagen om livsmedelsförvaltningens informationsresurs. Sökanden identifieras genom stark autentisering *i enlighet med lagen om stark autentisering* (617/2009). Genom förordning av statsrådet föreskrivs om sådana stöd enligt denna lag beträffande vilka ansökan kan göras bara på det sätt som avses i denna paragraf.

Denna lag träder i kraft den 20 .

26.

Lag

om ändring av konsumentskyddslagen

I enlighet med riksdagens beslut
ändras i konsumentskyddslagen (38/1978) 6 kap. 12 c § 1 mom., 7 kap. 15 § 1 mom., 7 a kap. 33 § 2 mom. och 10 kap. 6 § 1 mom., sådana de lyder, 6 kap. 12 c § 1 mom. och 7 kap. 15 § 1 mom. i lag 449/2023, 7 a kap. 33 § 2 mom. i lag 851/2016 samt 10 kap. 6 § 1 mom. i lag 227/2011, som följer:

Gällande lydelse

6 kap.

Hemförsäljning och distansförsäljning

12 c §

Kontroll av identiteten hos konsumenter och bevarande av uppgifterna om kontrollen i vissa fall

Om konsumenten vid köp av nyttigheter på nätet väljer ett betalningssätt som innebär betalningsanstånd, ska den näringsidkare som tillhandahåller betalningssättet i fråga kontrollera konsumentens identitet i samband med godkännandet av betalningssättet med hjälp av en identifieringsmetod som uppfyller kraven på system för elektronisk identifiering enligt 8 § i lagen om stark autentisering *och betrodda elektroniska tjänster* (617/2009) eller kraven på stark kundautentisering enligt 8 § 24 punkten och 85 c § 4 mom. i betaltjänstlagen (290/2010).

7 kap.

Konsumentkrediter

15 §

Kontroll av creditsökandens identitet

I samband med att ett avtal om konsumentkredit ingås och i samband med att

Föreslagen lydelse

6 kap.

Hemförsäljning och distansförsäljning

12 c §

Kontroll av identiteten hos konsumenter och bevarande av uppgifterna om kontrollen i vissa fall

Om konsumenten vid köp av nyttigheter på nätet väljer ett betalningssätt som innebär betalningsanstånd, ska den näringsidkare som tillhandahåller betalningssättet i fråga kontrollera konsumentens identitet i samband med godkännandet av betalningssättet med hjälp av en identifieringsmetod som uppfyller kraven på system för elektronisk identifiering enligt 8 § i lagen om stark autentisering (617/2009) eller kraven på stark kundautentisering enligt 8 § 24 punkten och 85 c § 4 mom. i betaltjänstlagen (290/2010).

7 kap.

Konsumentkrediter

15 §

Kontroll av creditsökandens identitet

I samband med att ett avtal om konsumentkredit ingås och i samband med att

Gällande lydelse

kreditbeloppet eller kreditgränsen höjs ska kreditgivaren noggrant kontrollera konsumentens identitet. Om identiteten kontrolleras elektroniskt, ska kreditgivaren använda en identifieringsmetod som uppfyller kraven i 8 § i lagen om stark autentisering och betrodde elektroniska tjänster eller kraven på stark kundautentisering i 8 § 24 punkten och 85 c § 4 mom. i betaltjänstlagen.

7 a kap.

Konsumentkrediter som har samband med bostadsegendom

33 §

Tillsynsmyndigheter

Tillsynsmyndigheterna ska samarbeta på lämpligt sätt. När efterlevnaden av 7 kap. 15 § övervakas med stöd av 31 § i detta kapitel ger Kommunikationsverket på begäran tillsynsmyndigheten ett utlåtande om huruvida den metod för elektronisk identitetskontroll som kreditgivaren använder uppfyller kraven i 8 § i lagen om stark autentisering och betrodde elektroniska tjänster.

10 kap.

Tidsdelat boende och långfristiga semesterprodukter

6 §

Avtalets form och språk

Avtalet ska upprättas skriftligt och undertecknas av parterna. Konsumenten ska få ett exemplar av avtalet. Avtalet kan upprättas även elektroniskt så att konsumenten kan bevara och återge avtalet i oförändrad form. På elektronisk signering av avtalet tillämpas lagen om stark autentisering och elektroniska signaturer (617/2009). I 7

Föreslagen lydelse

kreditbeloppet eller kreditgränsen höjs ska kreditgivaren noggrant kontrollera konsumentens identitet. Om identiteten kontrolleras elektroniskt, ska kreditgivaren använda en identifieringsmetod som uppfyller kraven i 8 § i lagen om stark autentisering eller kraven på stark kundautentisering i 8 § 24 punkten och 85 c § 4 mom. i betaltjänstlagen.

7 a kap.

Konsumentkrediter som har samband med bostadsegendom

33 §

Tillsynsmyndigheter

Tillsynsmyndigheterna ska samarbeta på lämpligt sätt. När efterlevnaden av 7 kap. 15 § övervakas med stöd av 31 § i detta kapitel ger *Transport- och kommunikationsverket* på begäran tillsynsmyndigheten ett utlåtande om huruvida den metod för elektronisk identitetskontroll som kreditgivaren använder uppfyller kraven i 8 § i lagen om stark autentisering.

10 kap.

Tidsdelat boende och långfristiga semesterprodukter

6 §

Avtalets form och språk

Avtalet ska upprättas skriftligt och undertecknas av parterna. Konsumenten ska få ett exemplar av avtalet. Avtalet kan upprättas även elektroniskt så att konsumenten kan bevara och återge avtalet i oförändrad form. På elektronisk signering av avtalet tillämpas *Europaparlamentets och rådets förordning (EU) nr 910/2014 om*

Gällande lydelse

kap. i den här lagen föreskrivs om formen för och innehållet i eventuella kreditavtal som anknyter till huvudavtalet.

Föreslagen lydelse

elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, sådan den lyder senast ändrad genom förordning (EU) 2024/1183. I 7 och 7 a kap. i denna lag föreskrivs det om formen för och innehållet i eventuella kreditavtal som anknyter till huvudavtalet.

Denna lag träder i kraft den 20 .

27.

Lag

om ändring av 48 § i lagen om strukturstöd för renhushållning och naturnäringar

I enlighet med riksdagens beslut
ändras i lagen om strukturstöd för renhushållning och naturnäringar (986/2011) 48 § 1 mom.,
sådant det lyder i lag 1329/2022, som följer:

Gällande lydelse

48 §

Ansökan om stöd

Stöd ska sökas elektroniskt via en nättjänst som utgör en del av den informationsresurs för livsmedelsförvaltningen som avses i lagen om livsmedelsförvaltningens informationsresurs (560/2021). Sökanden identifieras genom stark autentisering på det sätt som föreskrivs i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009). En stödansökan kan också göras med en blankett som fastställts för ändamålet. Blanketten kan lämnas in via en skyddad e-postförbindelse i form av en ifyllbar pdf-blankett eller i pappersformat. Den sistnämnda ska undertecknas.

Föreslagen lydelse

48 §

Ansökan om stöd

Stöd ska sökas elektroniskt via en nättjänst som utgör en del av den informationsresurs för livsmedelsförvaltningen som avses i lagen om livsmedelsförvaltningens informationsresurs (560/2021). Sökanden identifieras genom stark autentisering *i enlighet med lagen om stark autentisering* (617/2009). En stödansökan kan också göras med en blankett som fastställts för ändamålet. Blanketten kan lämnas in via en skyddad e-postförbindelse i form av en ifyllbar pdf-blankett eller i pappersformat. Det sistnämnda ska undertecknas.

Denna lag träder i kraft den 20 .

28.

Lag

om ändring av 119 a § i skjutvapenlagen

I enlighet med riksdagens beslut

ändras i skjutvapenlagen (1/1998) 119 a §, sådan den lyder i lag 89/2020, som följer:

Gällande lydelse

119 a §

Elektroniska tjänster

I 22 och 25 §, 42 § 2 mom., 42 c § 1 och 3 mom., 70 § 3 mom. och 89 § avsedda elektroniska tjänster förutsätter ett identifieringsverktyg som avses i lagen om stark autentisering *och betrodda elektroniska tjänster* (617/2009).

Föreslagen lydelse

119 a §

Elektroniska tjänster

I 22 och 25 §, 42 § 2 mom., 42 c § 1 och 3 mom., 70 § 3 mom. och 89 § avsedda elektroniska tjänster förutsätter ett identifieringsverktyg som avses i lagen om stark autentisering (617/2009).

Denna lag träder i kraft den 20 .

29.

Lag

om ändring av 84 § i fordonslagen

I enlighet med riksdagens beslut
ändras i fordonslagen (82/2021) 84 § 3 mom. som följer:

Gällande lydelse

84 §

Bestämmelser om registreringsanmälan

Den som gör en registreringsanmälan ska identifieras när han eller hon personligen lämnar in en anmälan till en avtalsregistrerare. Den som gör anmälan i den elektroniska tjänst som tillhandahålls av den som utför registreringar ska identifieras med sådan stark autentisering som avses i 2 § 1 punkten i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009).

Föreslagen lydelse

84 §

Bestämmelser om registreringsanmälan

Den som gör en registreringsanmälan ska identifieras när denne personligen lämnar in en anmälan till en avtalsregistrerare. Den som gör anmälan i den elektroniska tjänst som tillhandahålls av den som utför registreringar ska identifieras med sådan stark autentisering som avses i 2 § 1 punkten i lagen om stark autentisering (617/2009).

Denna lag träder i kraft den 20 .

30.

Lag

om ändring av 39 § i konkurrenslagen

I enlighet med riksdagens beslut
ändras i konkurrenslagen (948/2011) 39 § 1 mom. 9 punkten, sådan den lyder i lag 721/2019,
som följer:

Gällande lydelse

39 §

Informationsutbytet mellan myndigheter

Konkurrens- och konsumentverket kan på eget initiativ, trots bestämmelserna om sekretess, om det behövs lämna ut en uppgift eller handling som verket har fått eller upprättat i samband med skötseln av uppgifter enligt denna lag.

9) till Transport- och kommunikationsverket för uppgifter enligt lagen om tjänster inom elektronisk kommunikation (917/2014), postlagen (415/2011), lagen om stöd för byggande av bredband i glesbygdsområden (1186/2009), lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) och lagen om sambyggnad och samutnyttjande av nätinфраstruktur (276/2016).

Föreslagen lydelse

39 §

Informationsutbytet mellan myndigheter

Konkurrens- och konsumentverket kan på eget initiativ, trots bestämmelserna om sekretess, om det behövs lämna ut en uppgift eller handling som verket har fått eller upprättat i samband med skötseln av uppgifter enligt denna lag.

9) till Transport- och kommunikationsverket för uppgifter enligt lagen om tjänster inom elektronisk kommunikation (917/2014), postlagen (415/2011), lagen om stöd för byggande av fast bredband (1262/2020), lagen om stark autentisering (617/2009) och lagen om sambyggnad och samutnyttjande av nätinфраstruktur (276/2016).

Denna lag träder i kraft den 20 .