U 81/2025 rd

Statsrådets skrivelse till riksdagen om kommissionens förslag till ändring av Europaparlamentets och rådets förordningar och direktiv vad gäller förenkling av lagstiftningsramen på det digitala området (digital omnibus) och förenkling av genomförandet av de harmoniserade reglerna om artificiell intelligens (AI-omnibus)

I enlighet med 96 § 2 mom. i grundlagen översänds till riksdagen kommissionens förslag av den 19 november 2025 till Europaparlamentets och rådets förordning om ändring av förordningarna (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 och direktiven 2002/58/EG, (EU) 2022/2555 och (EU) 2022/2557 vad gäller förenkling av lagstiftningsramen på det digitala området och om upphävande av förordningarna (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 och direktiv (EU) 2019/1024 (digital omnibus, COM(2025) 837 final) och förslag till Europaparlamentets och rådets förordning om ändring av förordningarna (EU) 2024/1689 och (EU) 2018/1139 vad gäller förenkling av genomförandet av de harmoniserade reglerna om artificiell intelligens (AI-omnibus, COM(2025) 836 final) samt en promemoria om dessa.

Helsingfors den 29 januari 2026

Kommunikationsminister Lulu Ranne

Specialsakkunnig Pauliina Penttilä

KOMMUNIKATIONSMINISTERIET | PROMEMORIA | EU/1152/2025

15.1.2026

EUROPEISKA KOMMISSIONENS FÖRSLAG OM ÄNDRING AV FÖRORDNINGARNA (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 OCH DIREKTIVEN 2002/58/EG, (EU) 2022/2555 OCH (EU) 2022/2557 VAD GÄLLER FÖRENKLING AV LAGSTIFTNINGSRAMEN PÅ DET DIGITALA OMRÅDET SAMT FÖRSLAGET OM UPPHÄVANDE AV FÖRORDNINGARNA (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 OCH DIREKTIVET (EU) 2019/1024 (DIGITAL OMNIBUS) OCH FÖRSLAGET TILL FÖRORDNING OM ÄNDRING AV FÖRORDNINGARNA (EU) 2024/1689 OCH (EU) 2018/1139 VAD GÄLLER FÖRENKLING AV GENOMFÖRANDET AV DE HARMONISERADE REGLERNA OM ARTIFICIELL INTELLIGENS (AI-OMNIBUS)

1 Bakgrund

Den 19 november 2025 lämnade Europeiska kommissionen förslag till Europaparlamentets och rådets förordningar om förenkling av lagstiftningsramen på det digitala området (Digital Omnibus Regulation Proposal COM(2025) 837 final, nedan digital omnibus) och förenkling av genomförandet av reglerna om artificiell intelligens (Digital Omnibus on AI Regulation Proposal COM(2025) 836 final, nedan AI-omnibus).

Kommissionens förslag kom som en del av det digitala paketet (Digital Package), som även innehöll strategin för en dataunion (COM/2025/835 final) och förslaget till en förordning om europeiska företagsplånböcker (COM(2025) 838 final). Riksdagen kommer att informeras om övriga förslag i paketet genom separata E-utredningar och U-skrivelser. Kommissionen inledde också ett offentligt samråd om en kontroll av den digitala ändamålsenligheten (Digital Fitness Check) som innebär en bredare granskning av enhetligheten och den kumulativa inverkan av EU:s digitala regelverk för företag. Det offentliga samrådet är öppet till den 11 mars 2026.

Våren 2025 anordnade kommissionen flera samråd i frågor som rör genomförande och förenkling av regleringen på det digitala området (strategin för AI-tillämpningar, översyn av cybersäkerhetsförordningen och strategin för en europeisk dataunion). Kommissionen öppnade ett offentligt samråd om digital omnibus-förslaget i september 2025. Kommissionen har också fört flera temadiskussioner med företrädare för företag och civilsamhället om utmaningar och kostnader som genomförandet av reglerna innebär.

Behandlingen av förslagen inleddes i rådets förenklingsunderarbetsgrupp Antici under det danska ordförandeskapet. Cypern har sagt sig prioritera särskilt AI-omnibusbehandlingen under sitt rådsordförandeskap.

2 Förslagets syfte

Förslagen om digital omnibus och AI-omnibus är det första steget mot att förenkla EU:s digitala regler för data, dataskydd, cybersäkerhet och AI. Förslagen ingår i kommissionens bredare granskning av EU-regleringen med sikte på att minska den administrativa bördan av regleringen med minst 25 % och 35 % för små och medelstora företag.

Förslagen till förordningar fokuserar enligt kommissionen på direkta anpassningar inom sektorer där regleringens mål tydligt kan uppnås med lägre kostnader för företag, myndigheter och medborgare utan att äventyra skyddet för grundläggande rättigheter. Förslagen till ändringar återspeglar det som framhölls i kommissionens samråd.

3 Förslagets huvudsakliga innehåll

Digital omnibus omfattar ändringar i fem EU-förordningar:

- Europaparlamentets och rådets förordning (EU) 2023/2854 (dataförordningen)
- Europaparlamentets och rådets förordning (EU) 2018/1724 (förordningen om inrättande av en gemensam digital ingång)
- Europaparlamentets och rådets förordning (EU) 2016/679 (den allmänna dataskyddsförordningen)
- Europaparlamentets och rådets förordning (EU) 2018/1725 (dataskyddsförordningen för EU-institutioner)
- Europaparlamentets och rådets förordning (EU) 910/2014 (eIDAS-förordningen)
- Europaparlamentets och rådets förordning (EU) 2022/2554 (förordningen om digital operativ motståndskraft för finanssektorn)

Digital omnibus ändrar också tre direktiv:

- Europaparlamentets och rådets direktiv 2002/58/EG (direktivet om integritet och elektronisk kommunikation)
- Europaparlamentets och rådets direktiv (EU) 2022/2555 (NIS 2-direktivet)
- Europaparlamentets och rådets direktiv (EU) 2022/2557 (CER-direktivet)

Digital omnibus upphäver följande rättsakter:

- Europaparlamentets och rådets förordning (EU) 2022/868 (dataförvaltningsakten)
- Europaparlamentets och rådets förordning (EU) 2018/1807 (förordningen om det fria flödet av andra data än personuppgifter)
- Europaparlamentets och rådets förordning (EU) 2019/1150 (om främjande av rättvisa villkor och transparens för företagsanvändare av onlinebaserade förmedlingstjänster, P2B-förordningen)
- Europaparlamentets och rådets direktiv (EU) 2019/1024 (direktivet om öppna data)

AI-omnibus berör i sin tur

- Europaparlamentets och rådets förordning (EU) 2024/1689 (förordningen om artificiell intelligens)
- Europaparlamentets och rådets förordning (EU) 2018/1139 (EASA-förordningen)

3.1 Digital omnibus

Dataförordningen

Kommissionen föreslår att följande tre rättsakter upphävs och införlivas i dataförordningen: förordningen om det fria flödet av andra data än personuppgifter, dataförvaltningsakten och direktivet om öppna data. Därtill föreslås riktade ändringar i dataförordningen och de bestämmelser som förs dit för att skapa ett enhetligt regelverk.

Tillägg i artikel 4 och 5 i dataförordningens II kapitel ger en datahållare större rätt att vägra dela uppgifter innehållande företagshemligheter till användare av IoT-enheter eller tredjeparter om denne visar att det finns en hög risk för att företagshemligheter trots skyddsåtgärder förs utanför EU till tredjeländer eller företag under kontroll av dessa där skyddsmekanismerna är svagare än EU-regleringen. Datahållaren ska underrätta den berörda användaren eller tredjeparten samt den utsedda behöriga nationella myndigheten om vägran och motivera denna.

Offentliga organs rätt att få åtkomst till data från privata datahållare enligt kapitel V i dataförordningen begränsas så att begäran endast är motiverad om organet visar att det föreligger ett behov av att använda vissa data från en privat datahållare för att hantera, mildra eller stödja återhämtningen från ett allmänt nödläge. Uppgifterna får endast begäras om de inte kan inhämtas effektivt på annat sätt och på likvärdiga villkor.

Bestämmelserna om byte av databehandlingstjänster i kapitel VI i dataförordningen får fler undantag. Dessa lättnader tillämpas på databehandlingstjänster som är skräddarsydda eller tillhandahålls av små och medelstora företag, om avtalen har ingåtts före den 12 september 2025. Därtill klargörs att dessa leverantörer av databehandlingstjänster får införa bestämmelser om proportionerliga sanktioner för förtida uppsägning i sina tidsbegränsade avtal så länge de inte utgör ett hinder för byte av tjänsteleverantör. Ändringarna ska inte påverka skyldigheten att gradvis avskaffa bytesavgifterna.

Vad gäller bestämmelserna i dataförordningens VII kapitel om att förhindra olaglig åtkomst till icke-personuppgifter för tredjeländers myndigheter och begränsa internationell överföring av sådana uppgifter utökas tillämpningsområdet från databehandlingstjänster till att även omfatta offentliga organ som tillhandahåller skyddade data enligt avsnitt 3 i det nya kapitlet VIIc, fysiska eller juridiska personer som har rätt att vidareutnyttja dessa i enlighet med samma avsnitt samt dataförmedlingstjänster och erkända dataaltruismorganisationer.

Kapitel III och IV i dataförvaltningsakten införlivas i dataförordningen som det nya kapitlet VIIa. Dataförmedlingstjänstdefinitionen förtydligas och den obligatoriska ordningen för dataförmedlingstjänster blir frivillig. Skyldigheten att hålla dataförmedlingstjänster juridiskt åtskilda från företagets andra tjänster ersätts med en skyldighet att hålla dem funktionellt åtskilda. Kraven på dataförmedlingstjänster minskar betydligt. För dataaltruismorganisationer upphävs rapporterings- och transparenskraven och planerna på ett mer detaljerat dataaltruismregelverk slopas. Kommissionen ska föra ett offentligt register om tjänsterna, och varje medlemsstat ska utse en behörig myndighet för tillämpning och övervakning av kapitel VIIa avseende organisationer etablerade i det egna landet. I Finland är Transport- och kommunikationsverket behörig myndighet enligt dataförvaltningsakten och har även huvudansvaret för att övervaka dataförordningen.

Förbudet mot nationella lokaliseringskrav för andra data än personuppgifter upprätthålls genom att VIIb införs som nytt kapitel i dataförordningen, och skyldigheten att underrätta kommissionen om kraven av säkerhetsskäl bibehålls. Skyldigheten att upprätthålla en gemensam nationell informationspunkt om datalokaliseringskraven avskaffas.

De centrala bestämmelserna om skyddade data från direktivet om öppna data och kapitel II i dataförvaltningsakten förs till det nya kapitlet VIIc i dataförordningen. Regleringen av vidareutnyttjande av skyddade data som innehas av offentliga organ bibehålls till innehållet och tillämpningsområdet. Vidareutnyttjandet av anonymiserade uppgifter förtydligas emellertid. Förslaget inbegriper en ny bestämmelse om att offentliga organ får ta ut en rimlig avkastning utöver marginalkostnaden för vidareutnyttjande av skyddade data som dessa innehar. Det här gäller när data vidareutnyttjas av mycket stora företag, särskilt företag som har stort ekonomiskt

inflytande såsom en grindvakt enligt definitionen i förordningen om digitala marknader (DMA). Offentliga organ ska också kunna fastställa särskilda villkor för sådana mycket stora företag när data från den offentliga sektorn vidareutnyttjas, men villkoren ska vara motiverade och proportionerliga. I fortsättningen ska artikel 37 i dataförordningen tillämpas på utnämning av nationella myndigheter som stöder vidareutnyttjande av skyddade data.

Direktivet om öppna data, som gäller öppna data som innehas av offentliga organ och vissa företag som producerar allmännyttiga tjänster samt forskningsdata genererade med offentliga medel, införlivas i det nya kapitlet VIIc i dataförordningen och ändras innehållsmässigt så att definitionen av data motsvarar den i dataförordningen och dataförvaltningsakten. Handlingsdefinitionen förblir densamma och tillämpningsområdet avses inte bli ändrat. Avgifterna för vidareutnyttjande av handlingar ska kunna betalas online med hjälp av gränsöverskridande betalningstjänster. Det blir också möjligt att utöver marginalkostnaden ta ut en rimlig avkastning för vidareutnyttjandet av handlingar, om ett mycket stort företag vidareutnyttjar data. Offentliga organ ska även ha möjlighet att fastställa särskilda men motiverade och proportionerliga villkor för dessa mycket stora företags vidareutnyttjande av data.

I dataförordningens kapitel VIII om interoperabilitet upphävs artikel 36, dvs. att smarta kontrakt för genomförande av datadelningsavtal ska uppfylla vissa krav. Kraven ersätts med kommissionens befogenhet att införa standarder.

Dataförordningens kapitel IX om genomförande- och tillsynsmekanismer ska även tillämpas på de nya bestämmelserna i förordningen. Nuvarande artikel 38 om rätt att lämna in klagomål till behörig myndighet ersätts med en ny bestämmelse som beaktar att en myndighet i landet där dataförmedlingstjänsten eller dataaltruismorganisationen är registrerad har behörighet att behandla klagomål om dessa aktörer.

Nya kapitlet VIIc utesluts helt från tillämpningsområdet för artikel 40 (sanktioner) i dataförordningen. Offentliga aktörer ska dock enligt kapitel VIIc ha skyldighet att informera dem som efterfrågar vidareutnyttjande om tillgängliga möjligheter till prövning i samband med beslut eller förfaranden som påverkar dem.

I dataförordningen införs nya kapitlet IXa, där ändrade bestämmelser om och dataförvaltningsaktens viktigaste bestämmelser om Europeiska datainnovationsstyrelsen (EDIB) och dess uppdrag ska samlas. Enligt förslaget ska kommissionen framöver besluta om EDIB:s sammansättning och undergrupper medan dagens reglering förutsätter minst tre lagstadgade undergrupper. Ändringarna innebär att kommissionen kan utöka EDIB-medlemskapet från behöriga myndigheter till företrädare för organ, såsom ministerier, med behörighet inom den nationella politiken för dataekonomi. EDIB:s uppgifter renodlas betydligt så att dess roll blir att fungera som ett diskussionsforum i datafrågor, bistå kommissionen vid utveckling av genomförandet av dataförordningen, främja samarbetet mellan medlemsstaternas behöriga myndigheter samt dela god praxis för vidareutnyttande av offentliga data. Ändringsförslaget har inga detaljerade bestämmelser om till exempel EDIB:s arbetsordning som ska ersätta de tidigare.

Lättnaderna i kraven på små och medelstora företag utökas till att omfatta små midcapföretag (SMC). Med midcapföretag avses företag med en personalstyrka på minst 250 personer men under 750 och en omsättning på högst 150 miljoner euro eller en balansomslutning på högst 129 miljoner euro.

Den allmänna dataskyddsförordningen, dataskyddsförordningen för institutioner och direktivet om integritet och elektronisk kommunikation

Den allmänna dataskyddsförordningen

Kommissionen föreslår riktade ändringar i den allmänna dataskyddsförordningen för att bland annat harmonisera och förenkla tolkningen av den samt lätta på kraven för personuppgiftsansvariga vid lågriskbehandling av personuppgifter. Enligt förslaget är kommissionens mål att ändå säkerställa dagens nivå av skydd för personuppgifter.

Kommissionen föreslår ändringar i artikel 4 om definitioner. Syftet med ändringarna är framförallt att minska osäkerheten kring anonymisering, pseydonymisering och vetenskaplig forskning. Avseende anonymisering och pseudonymisering föreslås en bestämmelse som förtydligar definitionen av personuppgifter så att det inte är en personuppgift enbart på grund av att någon annan kan identifiera den registrerade med hjälp av informationen utan det avgörande är om den personuppgiftsansvarige kan identifiera denne med rimlig sannolikhet. Ändringen motsvarar rättspraxis från Europeiska unionens domstol Vidare föreslås att en definition av vetenskaplig forskning införs i förordningen och att principen om ändamålsbegränsning förtydligas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål.

Vad gäller anonymisering och pseudonymisering föreslår kommissionen också reglering som bistår personuppgiftsansvariga när kriterier och metoder för anonymisering och pseudonymisering utformas. Härvid föreslås en ny artikel, 41a, där kommissionen ges befogenhet att anta genomförandeakter. Enligt artikeln får kommissionen bedöma användningen av den senaste tillgängliga tekniken och utveckla kriterier som personuppgiftsansvariga kan använda för att visa att uppgifterna inte kan leda till avanonymisering av de registrerade.

För behandling av särskilda kategorier av personuppgifter föreslås en ny grund för undantag (nytt led l i artikel 9.2) om behandlingen av biometriska uppgifter är nödvändig för att bekräfta en registrerad persons identitet (kontroll). Här förutsätter förslaget att den registrerade har ensam kontroll över de biometriska uppgifter eller de medel som krävs för kontrollen.

Därtill föreslås ändringar i artikel 12 och 13 i dataskyddsförordningen med syftet att lätta kraven på personuppgiftsansvariga att informera registrerade om behandlingen av deras personuppgifter, särskilt vid lågriskbehandling och när registrerade missbrukar sina rättigheter. Artikel 22 om enskilda beslut med automatik (inkl. profilering) förtydligas så att det tydligt framgår att automatiserade beslut endast kan fattas enligt artikelns ramvillkor.

Andra lättnader i kraven på personuppgiftsansvariga är att anmälningströskeln vid personuppgiftsincidenter höjs till hög risk och att tidsfristen för anmälan förlängs från dagens 72 timmar till 96 timmar (artikel 33). Enligt förslaget ska uppgiftsincidenter i fortsättningen anmälas via en ny gemensam kontaktpunkt (Single-Entry Point).

Kommissionen föreslår att regleringen av terminalutrustningens integritet eller s.k. kakor (lagring och användning av personuppgifter i den registrerades terminal) flyttas från direktivet om integritet och elektronisk kommunikation till den allmänna dataskyddsförordningen vad gäller personuppgifter. Härvid läggs nya definitioner till artikel 4 i den allmänna dataskyddsförordningen. Därtill föreslås en ny artikel, 88a, om tillgång till uppgifter såsom kakor i terminalutrustning vid behandling av personuppgifter. Förslaget innebär att lagring och användning av personuppgifter kräver den registrerades samtycke i likhet med kraven i

direktivet om integritet och elektronisk kommunikation. Utöver nu gällande undantag i direktivet om integritet och elektronisk kommunikation föreslås att registrerades samtycke inte behöver begäras då en personuppgiftsansvarig enligt vissa villkor definierar målgruppen för en onlinetjänst för eget bruk eller om behandlingen är nödvändig för att upprätthålla eller återställa säkerheten hos en tjänst som tillhandahålls av den personuppgiftsansvarige och som begärs av den registrerade eller den terminalutrustning som används för att tillhandahålla tjänsten. I den nya artikeln 88b åläggs personuppgiftsansvariga att respektera det samtycke som en registrerad gett automatiskt och i maskinläsbart format till exempel via en webbläsare i enlighet med standarder som utarbetas separat.

För utveckling och drift av AI-system skapar förslaget framförallt klarhet om behandlingens rättsliga grund och behandlingen av särskilda kategorier av personuppgifter (artikel 9 och nya artikeln 88c). Förslaget ger möjlighet att behandla personuppgifter för att tillgodose den personuppgiftsansvariges eller en tredje parts berättigade intressen vid utveckling och drift av AI-system. Behandling tillåts dock inte ifall den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn. För behandlingen av personuppgifter krävs dock ett samtycke av den registrerade ifall ett sådant krav finns i unionsrätten eller medlemsstatens lagstiftning. Avseende utveckling och drift av AI-system föreslår kommissionen också en ny grund för undantag från förbudet mot behandling av särskilda kategorier av personuppgifter (nytt led k i artikel 9.2) och särskilda skyddsåtgärder för behandlingen (nya artikeln 9.5).

Dataskyddsförordningen för institutioner

Kommissionen föreslår liknande ändringar i dataskyddsförordningen för institutioner som i den allmänna dataskyddsförordningen. Förslaget syftar till att harmonisera och förenkla regleringen i dataskyddsförordningen för institutioner, med bibehållande av dagens skyddsnivå för personuppgifter. Ändringsförslagen berör framförallt anonymisering, pseudonymisering, vetenskaplig forskning, utveckling och drift av AI-system samt lättnader och förtydliganden i kraven på personuppgiftsansvariga. Ändringarna i dataskyddsförordningen för institutioner avser artikel 3 (definitioner), 4 (principer för behandling), 10 (behandling av särskilda kategorier av personuppgifter), 14 och 15 (information till registrerade), 24 (automatiserat beslutsfattande), 34 (anmälningar om personuppgiftsincidenter), 37 (reglering av kakor), 39 (konsekvensbedömning) och nya 45 a (kriterier för pseudonymisering). Till skillnad från ändringar som föreslås i den allmänna dataskyddsförordningen övervakas behandlingen av personuppgifter av Europeiska datatillsynsmannen, dit unionens institutioner, organ och byråer bland annat ska anmäla personuppgiftsincidenter. Således ska till exempel anmälningar av uppgiftsincidenter enligt artikel 34 göras till EDPS. Användning av en gemensam kontaktpunkt föreslås inte i fråga om dataskyddsförordningen för institutioner.

Direktivet om integritet och elektronisk kommunikation

Kommissionen föreslår att regleringen kring uppgifter i användarens terminalutrustning enligt direktivet om integritet och elektronisk kommunikation reformeras så att 88a och 88b införs som nya artiklar i den allmänna dataskyddsförordningen.

Förslaget till artikel 5 har bestämmelser om ändringar i direktivet om integritet och elektronisk kommunikation. Artikel 4 i direktivet (säkerhet i samband med behandlingen) upphävs. Efter artikel 5.3 i direktivet införs ett nytt stycke enligt vilket den allmänna dataskyddsförordningen ska tillämpas på lagring eller användning av personuppgifter i en fysisk persons terminalutrustning. Bestämmelserna om sådan lagring och användning kommer att finnas i nya artikel 88a i den allmänna dataskyddsförordningen.

EU-gemensam kontaktpunkt för incidentrapportering

Kommissionen föreslår att en gemensam kontaktpunkt (Single-Entry Point for Incident Reporting) inrättas för anmälningar av olika störningar och incidenter. Därtill ändras incidentrapporteringskraven som följer av vissa rättsakter så att dessa anmälningar i fortsättningen ska göras via den EU-gemensamma kontaktpunkten för att uppfylla rapporteringsskyldigheten.

Kommissionen föreslår att den gemensamma kontaktpunkten tillämpas på anmälningar enligt NIS 2-direktivet, den allmänna dataskyddsförordningen, DORA-förordningen, eIDAS-förordningen och CER-direktivet. Genom förslaget ändras dessa rättsakter så att där avsedda anmälningar framöver ska göras via den EU-gemensamma kontaktpunkten. I övrigt föreslås inga ändringar i anmälningar enligt dessa rättsakter såsom tröskeln för anmälan eller vilka uppgifter som ska lämnas. Den EU-gemensamma kontaktpunkten kan i framtiden utökas till att omfatta anmälningar enligt andra rättsakter.

Bestämmelserna om den EU-gemensamma kontaktpunkten föreslås bli införda i NIS 2-direktivet genom den nya artikeln 23a. Kontaktpunkten ska inrättas och upprätthållas av Europeiska unionens cybersäkerhetsbyrå Enisa. Användandet av den EU-gemensamma kontaktpunkten föreskrivs i anslutning till de bestämmelser som fastställer rapporteringsskyldigheten.

Enligt förslaget ska Enisa vidta nödvändiga tekniska, operativa och organisatoriska åtgärder för kontaktpunktens säkerhet och tillförlitlighet (riskhantering) när den utvecklas och upprätthålls. Enisa ska se till att behöriga myndigheter har tillgång till och kan behandla informationen i kontaktpunkten samt ta hänsyn till känsligheten hos den. Genomförandet och utvecklingen av den gemensamma kontaktpunkten ska ske i ett samarbete mellan Enisa, kommissionen, CSIRT-nätverket och medlemsstaternas behöriga myndigheter. Om inte annat föreskrivs i unionsrätten ska Enisa inte ha tillgång till de anmälningar som lämnas in via den gemensamma kontaktpunkten. Den gemensamma kontaktpunkten ska uppfylla delarna i förslaget till artikel 23a.3.

Inom 18 månader efter det att förordningen har trätt i kraft ska Enisa göra en provundersökning och provning av den gemensamma kontaktpunkten. Utifrån detta ska kommissionen i samarbete med Enisa bedöma den gemensamma kontaktpunktens funktion, tillförlitlighet, integritet och konfidentialitet. Kommissionen ska även samråda med CSIRT-nätverket och nationella behöriga myndigheter. Om kommissionen konstaterar att den gemensamma kontaktpunkten uppfyller nödvändiga krav ska den offentliggöra ett tillkännagivande i Europeiska unionens officiella tidning så att Enisa med detta som grund kan börja ta emot anmälningar via kontaktpunkten. Om kommissionen då kontaktpunkten är i drift konstaterar att den inte uppfyller nödvändiga krav ska Enisa i samarbete med kommissionen vidta alla nödvändiga korrigerande åtgärder för att säkerställa korrekt funktion, tillförlitlighet, integritet eller konfidentialitet. Kommissionen ska vid behov ompröva den gemensamma kontaktpunktens funktion och uppdatera eller offentliggöra ett tillkännagivande som ligger till grund för Enisas drift av kontaktpunkten.

Förslaget innebär att det i artikel 23.1 i NIS 2-direktivet införs att incidenter ska anmälas via den gemensamma kontaktpunkt som inrättats i enlighet med artikel 23a. Ett ytterligare tillägg i artikel 23 i NIS 2-direktivet är punkt 12, som innebär att anmälningar om allvarliga incidenter som påverkar säkerheten för en produkt med digitala element enligt artikel 14.3 i förordning (EU) 2024/2847 (cyberresiliensförordningen) också ska anses som anmälan av en incident enligt NIS 2-direktivet. Därtill ändras artikel 30 i NIS 2-direktivet så att medlemsstaterna ska

säkerställa att de anmälningar på frivillig basis som avses i artikeln kan göras till dem via den EU-gemensamma kontaktpunkten.

Förslaget innebär att artikel 19a, 4 och 45a i eIDAS-förordningen ändras genom att införa punkter om att de anmälningar som avses i artiklarna ska göras via den EU-gemensamma kontaktpunkten.

Genom förslaget ändras artikel 19 i DORA-förordningen så att där avsedda anmälningar ska göras via den EU-gemensamma kontaktpunkten. Därtill ska det finnas möjlighet att göra frivilliga anmälningar via den EU-gemensamma kontaktpunkten.

Genom förslaget ändras artikel 15 i CER-direktivet så att där avsedda anmälningar ska göras via den EU-gemensamma kontaktpunkten. Därtill ska det finnas möjlighet att göra frivilliga anmälningar via den EU-gemensamma kontaktpunkten.

I artikel 33 i den allmänna dataskyddsförordningen införs en hänvisning till att anmälningar om personuppgiftsincidenter ska göras via den EU-gemensamma kontaktpunkten.

Innan den EU-gemensamma kontaktpunkten tas i bruk ska anmälningar enligt rättsakterna göras till de nationella behöriga myndigheterna enligt nuvarande modell för genomförande av rättsakterna.

Upphävande av vissa rättsakter

Kommission föreslår upphävande av förordningen om främjande av rättvisa villkor och transparens för företagsanvändare av onlinebaserade förmedlingstjänster (P2B-förordningen). Enligt kommissionens är de centrala kraven (transparens, rättvis behandling, tvistlösning) införda i förordningarna om digitala tjänster (DSA) och digitala marknader (DMA), som trädde i kraft 2022 och tillhandahåller mer omfattande och bindande regler för plattformsekonomin. Vissa artiklar i P2B-förordningen ska förbli i kraft under hela övergångsperioden till 2032 för att garantera rättssäkerheten i rättsakter som hänvisar till P2B-förordningen. Detta berör en del av definitionerna i artikel 2 ('företagsanvändare', 'onlinebaserad förmedlingstjänst', 'onlinebaserad sökmotor'), artikel 4 om begränsning, tillfälligt avbrytande eller avslutande av tjänster, artikel 11 om internt system för hantering av klagomål och artikel 15 om efterlevnad.

3.2 AI-omnibus

Ändringar i AI-förordningen föreslås med syftet att lätta på den administrativa bördan för leverantörer av AI-system och organ som bedömer överensstämmelse. Kommissionen får befogenheter för tillsyn över AI-system som bygger på AI-modeller för allmänna ändamål från samma leverantör och AI-system som är inbyggda i mycket stora onlineplattformar och mycket stora sökmotorer.

Kommissionen föreslår att den särskilda hänsynen mot små och medelstora företag utökas till att även omfatta små midcapföretag: vissa undantag från kraven på AI-system med hög risk, avdelade stödåtgärder som tar hänsyn till behoven hos företagen och lägre tak för administrativa sanktionsavgifter.

Den nuvarande skyldigheten för leverantörer och tillhandahållare av AI-system att främja AI-kunnighet omvandlas till en skyldighet för kommissionen och medlemsstaterna.

Jämfört med dagens reglering föreslår kommissionen att utöver leverantörer även tillhandahållare av AI-system med hög risk samt leverantörer och tillhandahållare av andra AI-system under vissa förutsättningar ska få behandla särskilda kategorier av personuppgifter, om det behövs för upptäckt och begränsning av bias. Behandlingen får grundas på behov i stället för absolut nödvändighet som i dag. Enligt kommissionen ligger det i allmänhetens intresse att bias upptäcks och korrigeras eftersom detta skyddar fysiska personer från negativa konsekvenser av AI, däribland diskriminering. Denna behandling ska omfattas av särskilda skyddsåtgärder.

AI-system för högriskanvändning som ändå inte utgör AI-system med hög risk behöver inte längre registreras i kommissionens databas.

Förslaget syftar också till att underlätta bedömningen av överensstämmelse samt förfarandet för anmälan från organ för bedömning. Regleringen av organ för bedömning av överensstämmelse ändras så att samma ansökan kan omfatta anmälan som organ för bedömning av överensstämmelse med AI-förordningen och överensstämmelse med annan sektorslagstiftning. Dessutom förtydligas bedömningen av överensstämmelse.

Kommissionens fråntas befogenheten att anta genomförandeakter om förfarandekoder för AI-modeller för allmänna ändamål och om transparens för vissa AI-system. Syftet är att harmoniserade regler för genomförandet endast ska antas ifall det är absolut nödvändigt.

Regleringen av regulatoriska sandlådor utvidgas för att möjliggöra tätare testning under verkliga förhållanden i anslutning till sandlådorna och även utanför dem. Testning tillåts i större omfattning än tidigare även med system i bilaga I, inte bara med system i bilaga III. Det blir möjligt att kommissionen och medlemsstaterna ingår frivilliga avtal om att genomföra praktisk testning av system i del B i bilaga I. Kommissionen får befogenhet att inrätta sandlådor för AI-system för allmänna ändamål som bygger på AI-modeller för allmänna ändamål från samma leverantör. I dessa fall ska kommissionen ha motsvarande befogenheter som nationella marknadskontrollmyndigheter. Kommissionen får befogenhet att utöva tillsyn över AI-system som omfattas av förordningen om digitala tjänster och utgör eller är en del av en mycket stor onlineplattform eller onlinesökmotor.

Mikroföretagsundantaget från kraven på ett kvalitetsstyrningssystem för AI-system utökas till att även gälla små och medelstora företag.

Regleringen av den vetenskapliga panelen specificeras genom att ersättningarna till panelens experter för stöd till medlemsstaterna i genomförandet av förordningen fastställs tydligare. Medlemsstaterna får även möjlighet att konsultera experterna i den vetenskapliga panelen direkt, utan inblandning från kommissionen.

Mer flexibilitet ges i övervakningen efter utsläppandet på marknaden genom att kommissionen fråntas befogenheten att anta en genomförandeakt med detaljerade bestämmelser som fastställer en mall för planen för övervakning efter utsläppande på marknaden och en förteckning över de element som ska ingå i planen.

Avseende myndigheter som utövar tillsyn över skyddet av grundläggande rättigheter förtydligas rätten att få information från behöriga marknadskontrollmyndigheter, vars skyldighet att svara på sådana begäranden betonas i förslaget.

Harmoniserade standarder som stöd för efterlevnaden av AI-förordningen kommer med all sannolikhet inte att färdigställas före den 2 augusti 2026, då förordningen ska börja tillämpas

fullt ut. Detta gäller även högrisksystem i bilaga III, såsom krav avseende utbildning, sysselsättning och kritisk infrastruktur. Förslaget inbegriper därför flera ändringar i övergångsperioder och tidpunkter för ikraftträdande för att ge mer tid åt utarbetandet av standarder och ekonomiska aktörers anpassning:

- Regleringen av system som genererar artificiellt innehåll såsom ljud eller bild samt deras transparens tillämpas på system som har släppts ut på marknaden före den 2 augusti 2026 efter en övergångsperiod på 6 månader, dvs. från den 2 februari 2027. Det här är sex månader efter det nuvarande datumet för tillämpning, den 2 augusti 2026.

- Tillämpning av kraven på AI-system med hög risk knyts till att stödverktyg såsom harmoniserade standarder, gemensamma specifikationer eller kommissionens riktlinjer finns på plats enligt beslut av kommissionen. Efter att beslutet offentliggjorts ska de ekonomiska aktörerna göra nödvändiga förändringar inom sex månader (bilaga III) eller 12 månader (bilaga I). Ett förbehåll i förordningen är att kraven ska tillämpas senast den 2 december 2027 på system i bilaga III och senast den 2 augusti 2028 på system i bilaga I även om standarderna inte är färdiga.

- Tillämpning av kraven på AI-system som redan släppts ut på marknaden eller tillhandahållits motsvarar tillämpningstiderna för AI-system med hög risk. Denna ändring gäller inte system avsedda att användas av myndigheter. Dessa ska alltjämt uppfylla förordningens krav senast den 2 augusti 2030.

Därtill ändras förordningen om säkerheten på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet EASA så att AI-förordningens krav på AI-system med hög risk kan införlivas i den.

4 Förslagets rättsliga grund och förhållande till proportionalitets- och subsidiaritetsprincipen

4.1 Rättslig grund

Båda förslagen till förordning, digital omnibus och AI-omnibus, har som rättslig grund artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), som gäller de åtgärder som hänför sig till genomförande av och verksamhet på den inre marknaden. Syftet med artikeln är tillnärmning av medlemsstaternas lagstiftning och säkerställande av att sammanhållen och icke-diskriminerande lagstiftning är tillämplig i Europeiska unionen. På grundval av den tillämpas det ordinarie lagstiftningsförfarandet, och rådet ska fatta beslut med kvalificerad majoritet.

Unionens domstol har i sin rättspraxis slagit fast att en rättsakt endast kan antas utifrån artikel 114 i EUF-fördraget, om det av rättsakten framgår och objektivt kan påvisas att den syftar till att förbättra villkoren för upprättandet av den inre marknaden och dess funktion. Om detta villkor är uppfyllt, ger artikel 114 EUF-fördraget unionslagstiftaren omfattande prövningsrätt vid valet av nödvändiga tillnärmnings- och harmoniseringsåtgärder.

Digital omnibus-förslaget har som ytterligare rättslig grund artikel 16 i EUF-fördraget för ändringar i den allmänna dataskyddsförordningen och dataskyddsförordningen för institutioner. Artikel 16 i EUF-fördraget gäller skydd för personuppgifter och utgör rättslig grund för EU:s dataskyddslagstiftning. Artikeln fastställer att skyddet för personuppgifter är en grundläggande rättighet i EU. EU har behörighet att stifta lagar om behandling av personuppgifter. Även på

grundval av artikel 16 i EUF-fördraget tillämpas det ordinarie lagstiftningsförfarandet, och rådet ska fatta beslut med kvalificerad majoritet.

Den rättsliga grunden för en rättsakt ska fastställas utifrån dess syfte och huvudsakliga innehåll. EU-domstolen har i sin praxis ansett att unionslagstiftaren om möjligt alltid bör sträva efter att använda endast en rättslig grund. Att använda en eller flera parallella rättsliga grunder är en exceptionell lösning. Enligt EU-domstolen är det möjligt när det rör sig om en rättsakt som samtidigt har flera syften eller beståndsdelar, vilka är oskiljaktigt förbundna med varandra, utan att den ena är underordnad eller indirekt i förhållande till den andra.

Enligt statsrådets bedömning förefaller det motiverat att använda flera rättsliga grunder i samband med digital omnibus-förslaget. Det är problemfritt att kombinera de föreslagna rättsliga grunderna även med tanke på behandlings- och beslutsförfaranden eftersom det ordinarie lagstiftningsförfarandet tillämpas på båda och rådet följer samma röstningsförfarande i sitt avgörande.

Statsrådet anser sammanfattningsvis att förslagens rättsliga grunder är lämpliga. Vad gäller de föreslagna ändringarna i AI-förordningen bör dock artikel 16 i EUF-fördraget prövas som ytterligare rättslig grund eftersom ändringarna delvis även berör skyddet för personuppgifter.

4.2 Subsidiaritets- och proportionalitetsprinciperna

Digital omnibus

Förslagen avseende dataförordningen inklusive dataförvaltningsakten, direktivet om öppna data och förordningen om det fria flödet av andra data än personuppgifter är förenliga med subsidiaritets- och proportionalitetsprinciperna enligt statsrådets initiala uppfattning.

Förslagen avseende den allmänna dataskyddsförordningen och dataskyddsförordningen för institutioner är förenliga med subsidiaritets- och proportionalitetsprinciperna enligt statsrådets initiala uppfattning, men under förhandlingarna måste det bedömas om alla delar i den föreslagna regleringen är proportionella utan att äventyra en hög nivå av dataskydd. Kommissionens förslag till ny reglering (bland annat om anonymisering och pseudonymisering, utveckling och drift av AI-system samt kakor) innehåller till exempel inte förslag om nivån på administrativa sanktionsavgifter (artikel 83 i allmänna dataskyddsförordningen). Nivån på administrativa sanktionsavgifter har inte heller bedömts för ny reglering som gäller dataskyddsförordningen för institutioner (artikel 66 i den förordningen). Sanktioner är en viktig del av regleringens effektivitet, och för att säkerställa regleringens proportionalitet är det viktigt att säkerställa att den föreslagna regleringen inte blir otydlig i fråga om huruvida administrativa sanktionsavgifter kan påföras enligt den nya regleringen och vilken nivå de påförda avgifterna skulle ligga på. Vidare finns skäl att säkerställa att befogenheter till kommissionen för att anta akter och för genomförandet delegeras ändamålsenligt samt tillräckligt noga avgränsat och exakt i alla delar (förslag till ny artikel 41 a och till ändringar i artikel 35).

För direktivet om integritet och elektronisk kommunikation finns det ingen bedömning av subsidiaritets- och proportionalitetsprinciperna från kommissionen. Här måste det under förhandlingarna bedömas om den föreslagna regleringen följer principerna i alla delar.

Förslaget om inrättande av en EU-gemensam anmälningsordning är förenligt med subsidiaritets- och proportionalitetsprinciperna enligt statsrådets uppfattning. Kommissionen har dock inte bedömt ifall det är förenligt med subsidiaritets- och proportionalitetsprinciperna att de berörda ska vara skyldiga att anmäla och rapportera via EU-systemet i alla situationer.

Här måste det under förhandlingarna klargöras och bedömas om förslaget avseende skyldigheten är förenligt med subsidiaritets- och proportionalitetsprinciperna, till exempel då uppgifter som ska rapporteras innehåller sådant som rör den nationella säkerheten eller då rapporteringen sker i en enskild medlemsstat med bara en rättsakt som grund.

Förslaget om upphävande av P2B-förordningen är förenligt med subsidiaritets- och proportionalitetsprinciperna enligt statsrådets uppfattning. Att förenkla regleringen och minska den administrativa bördan talar för en granskning av överlappningarna mellan P2B-förordningen och förordningarna om digitala tjänster och digitala marknader. När ett upphävande av rättsakterna övervägs ska deras olika objekt och tillämpningsområden beaktas. P2B-förordningen tryggar transparensen i avtal mellan onlinebaserade förmedlingstjänster av alla storlekar och deras företagsanvändare medan förordningen om digitala marknader bara gäller stora grindvaktsföretag och förordningen om digitala tjänster förmedlingstjänsternas ansvar för publicerat innehåll på deras plattformar. Det är centralt att säkerställa hur företagens rättssäkerhet kommer att tryggas i plattformsavtalen efter ett upphävande av P2B-förordningen.

AI-omnibus

Förslaget om AI-förordningen är förenligt med subsidiaritets- och proportionalitetsprinciperna enligt statsrådets uppfattning. Med tanke på skyddet av personuppgifter måste det under förhandlingarna emellertid bedömas om den föreslagna regleringen i alla delar är proportionerlig utan att äventyra en hög nivå av dataskydd. Här bör man framförallt beakta behandling av särskilda kategorier av personuppgifter i AI-system med hög risk och de stora risker behandlingen medför.

5 Förslagets konsekvenser

Dataförordningen

Enligt kommissionens bedömning främjas enhetligheten och tydligheten av att dataregleringen samlas i dataförordningen. Förslagen förutsätter dock åtminstone tekniska ändringar av myndigheters uppgifter och befogenheter i den nationella genomförandelag som träder i kraft den 1 januari 2026, vilket innebär en viss administrativ börda för myndigheterna. Ansvarsfördelningen mellan nationella myndigheter i vidareutnyttjandet av skyddade data kan påverkas eftersom oklar reglering kan medföra betydande kostnader för den offentliga förvaltningen, om sådana data ska tillgängliggöras i större omfattning än i dag eller om dagens system måste ändras.

Genom att datahållare tillåts neka utlämning av affärshemligheter till tredjelandsaktörer med svagt skydd räknar kommissionen med att lätta företagens börda i samband med framställning, delning och skydd av data och affärshemligheter. De största besparingarna kan komma från datahanteringsavtal, införande av applikationsprogrammeringsgränssnitt, minskade juridiska risker särskilt i gränsöverskridande sammanhang och visad överensstämmelse när ramarna för skydd av affärshemligheter utanför EU bedöms. Ändringarna kommer sannolikt ändå inte eliminera behovet av ytterligare vägledning i det praktiska arbetet med tillämpningen.

En ny datadelningsram för den offentliga sektorn kommer att minska företagens administrativa och juridiska börda, enligt kommissionens bedömning. Trots att kostnaderna för behandling av begäranden vid allmänna nödlägen alltjämt är betydande (t.ex. nödvändiga programlösningar, data- och personalkostnader) kommer ett fokus på enbart allmänna nödlägen att minska komplexiteten när företagen inte längre behöver skräddarsy datainfrastrukturen och förhandla om avtal för andra situationer. Kostnaderna minskar också för behöriga myndigheter när

hanteringen av datadelningsbefogenheter mellan medlemsstaterna förenklas och samordningen underlättas, särskilt i gränsöverskridande sammanhang.

Finland har sedan tidigare nationella bestämmelser om rätten att få information från datahållare i undantagssituationer. I detta har dataförordningen endast varit kompletterande. Den förra regleringen har även möjliggjort att myndigheter i andra medlemsstater begär ut information från datahållare i Finland om ett exceptionellt behov uppstår. Den administrativa bördan för finska företag kan minska något om denna möjlighet försvinner.

Kommissionen bedömer att minst 100 000 avtal om skräddarsydda PaaS- och SaaS-tjänster omfattas av den förenklade regleringen. Möjligheten att inte omförhandla avtalen skulle kunna ge cirka en miljard euro i besparingar. Omförhandlingslättnaden gäller avtal som har ingåtts före förordningens ikraftträdande, så besparingarna avser aktörer som inte hunnit ändra sina avtal. Att lättnaderna gäller avtal ingångna före förordningens ikraftträdande innebär utmaningar för både tjänsteleverantörer och myndigheter i genomförandet av förordningen. Förslaget kan också tolkas så, att kommissionen inte förväntar sig efterlevnad av förordningen på denna punkt. Lättnaderna antas inte ha betydande marknadskonsekvenser eftersom nya avtal ska upprättas i enlighet med förordningen.

Kommissionen har inte beräknat kostnader eller besparingar som regleringen av smarta kontrakt innebär men bedömer att avregleringen minskar den administrativa bördan. Utvecklarna skulle inte behöva omarbeta de smarta kontrakten för att uppfylla dataförordningens krav eller utföra bedömningar av överensstämmelse. Även myndigheternas börda bedöms minska när tillsyn av överensstämmelsen inte längre behövs för den framväxande marknaden och tekniken. En mer flexibel miljö kan främja utvecklingen av smarta kontraktslösningar, vilket i sin tur kan främja ekonomisk aktivitet och teknisk utveckling.

Kommissionen bedömer att en frivillig och enklare ordning för dataförmedlingstjänster ökar förtroendet, minskar kostnaderna och uppmuntrar utvecklingen av affärsmodeller. Den administrativa bördan minskar när centrala definitioner förtydligas och reglerna specificeras. Att kravet på tillhandahållande av tjänster genom en separat juridisk person tas bort ger besparingar i etablerings- och administrativa kostnader. Medlemsstaterna sparar in rapporteringskostnader när kravet gällande nationella dataaltruismorganisationer tas bort.

På EU-nivå kan ändringarna spara in upp till 318 750 euro i engångskostnader och cirka 6 miljoner euro i administrativa kostnader per år. Detta minskar hindren för marknadstillträde och kan locka nya leverantörer av dataförmedlingstjänster så att konkurrensen ökar och marknaden växer.

Den frivilliga delningen av data väntas öka när fler företag hittar tjänster för sina behov, och kommissionen förväntar sig att detta leder till framsteg inom forskning av allmänt intresse eller om samhälleliga mål (sällsynta sjukdomar, miljöskydd. biologisk mångfald).

Att registreringskravet för leverantörer av dataförmedlingstjänster tas bort kan leda till sämre transparens och ansvarstagande på marknaden eftersom de behöriga myndigheterna endast övervakar registrerade aktörer. Framförallt konsumenter kan ha svårt att uppfatta skillnaden mellan registrerade och rent avtalsbaserade dataförmedlingstjänster och därför bör man fästa vikt vid registrering och en gemensam logotyp till exempel då tjänster används av EU:s dataområden och den offentliga sektorn.

De bestämmelser som specificerar dataförordningen och dataförvaltningsakten har Finland i stort sett redan fört in i samma lag. Enligt transport- och kommunikationsverket har den tidigare

definitionen av dataförmedlingstjänster uteslutit aktörer från förordningen. Definitionsändringsförslagen klargör tolkningarna och utökar gruppen potentiella leverantörer av dataförmedlingstjänster.

Förslaget behåller möjligheten att placera icke-personuppgifter på den effektivaste EU-platsen, vilket minskar juridiskt dubbelarbete och sänker kostnaderna. Kommissionen bedömer att myndigheterna slipper tunga övervakningsuppgifter ifall kravet på en gemensam informationspunkt om datalokaliseringskraven tas bort. Detta uppskattas ge besparingar på cirka 31 000 euro per medlemsstat och år (cirka 847 000 euro på EU-nivå). Regelförenklingen underlättar även utövandet av företagsverksamhet och främjar den fria rörligheten för tjänster som är baserade på icke-personuppgifter.

Att reglerna för vidareutnyttjande av data från den offentliga sektorn samlas i dataförordningen kommer enligt kommissionens bedömning att harmonisera definitionerna och förfarandena samt eliminera dubbelarbete utan att göra avkall på regleringens nivå. Förslaget gör det lättare att hitta och använda data, minskar efterlevnadskostnaderna och ger snabbare åtkomst till data från den offentliga sektorn genom tydligare, direkt tillämpliga och harmoniserade regler på EU-nivå.

I Finland ska behovet av nationell lagstiftning som implementerar direktivet bedömas. Förslaget ser inte ut att ha nämnvärda konsekvenser för offentliga organ eller för dem som vill vidareutnyttja öppna data som innehas av den offentliga sektorn. Konsekvenser kan finnas för dataskydd, vetenskaplig frihet, offentlighetsprincipen och den offentliga förvaltningens datahantering, och dessa kräver ytterligare granskning. Konsekvenserna för myndigheternas laglighetskontroll, forskningsverksamhet och ändringssökande i beslut enligt offentlighetslagen måste också bedömas ifall de allmänna bestämmelserna i kapitel IX i dataförordningen blir tillämpliga i det nya kapitlet VIIc.

Förslaget om en möjlighet för offentliga organ att av vissa företag ta ut högre avgifter för vidareutnyttjande av handlingar och data samt fastställa villkor för användningen har en oklar utformning eftersom myndigheterna därmed får befogenhet att själv fastställa högre avgifter medan utgångspunkten i Finland är att grunden för myndighetsavgifter föreskrivs i lagar och i förordningar utfärdade med stöd av lag. Det är också oklart hur stor den administrativa bördan skulle bli ifall offentliga organ vid begäran om vidareutnyttjande av data eller handlingar måste utreda om undantagsvillkor eller högre avgifter kan tillämpas på det företag som gör begäran. Förslaget behöver även granskas ytterligare i relation till principerna om icke-diskriminering och konkurrensneutralitet.

Kommissionen beräknar att 38 000 företag i unionen omfattas av SMC-definitionen. Om SMC-företagens nedsatta pris för åtkomst till den offentliga sektorns skyddade databaser utökas till att omfatta alla små och medelstora företag skulle det kunna ge årliga besparingar på totalt 5–19 miljoner euro i hela EU. Förslaget att regelverket ska omfatta SMC-företagen väntas främja vidareutnyttjandet av data och påskynda innovation genom att data från den offentliga sektorn blir lättillgängligare för en större grupp ekonomiska aktörer, vilket borde ha en positiv ekonomisk effekt.

Den allmänna dataskyddsförordningen, dataskyddsförordningen för institutioner och direktivet om integritet och elektronisk kommunikation

Den allmänna dataskyddsförordningen

Enligt kommissionen skulle de riktade ändringar som föreslås i den allmänna dataskyddsförordningen förenkla kraven på lågriskbehandling samt harmonisera och klargöra vissa centrala begrepp i förordningen. Enligt kommissionen bistår förslaget de personuppgiftsansvariga utan att äventyra en hög skyddsnivå för personuppgifter. Ändringarna stöttar framförallt små och medelstora företag utan dataintensiv eller riskfylld verksamhet. Enligt kommissionen kan personuppgiftsanvariga i fortsättningen rikta sina resurser till mer dataintensiva och riskfyllda verksamheter där det är mest kritiskt att ha åtgärder för skydd av personuppgifter. De föreslagna ändringarna väntas ge aktörerna direkta regleringsfördelar genom effektivare verksamhet och minskade risker samt bättre innovations- och utvecklingsmiljö. Tydligare reglering främjar också indirekt att data utnyttjas för exempelvis forskningsändamål. Dessa fördelar innebär kostnadsbesparingar bland annat genom att mindre tid och resurser går åt till att säkerställa databehandling i enlighet med dataskyddsförordningen. Kommissionen har inte gett mer specifika kvantitativa bedömningar av besparingarna.

Dataskyddsförordningen för institutioner

Kommissionen har inte gett några separata bedömningar om dataskyddsförordningen för institutioner. Ändringsförslagen motsvarar dock i stor utsträckning det som kommissionen föreslår om dataskyddsförordningen.

Direktivet om integritet och elektronisk kommunikation

Enligt kommissionen syftar förslaget till att minska förfrågningarna om kakor genom att användarens samtycke ska begäras i färre situationer. Kommissionen bedömer att företagens kostnader minskar genom minskad användning av förfrågningar när reglerna för kakor har uppdaterats. Dagens kostnader för efterlevnad av reglerna för kakor uppskattas till cirka 400 euro per år och företag, och enligt förslaget kan dessa sänkas. Utöver minskade kostnader för företagen genom färre antal förfrågningar skulle förslaget leda till förenkling och förbättra medborgarnas upplevelse av webbsidor med bibehållande av en hög personuppgiftsstandard. Enligt kommissionen kommer förslaget att stärka användarnas rätt att utöva sina dataskyddsrättigheter och göra sina val på nätet.

I Finland innebär kommissionens förslag att dataombudsmannen blir behörig myndighet för lagring och användning av personuppgifter i terminalutrustning och ska utgöra en sådan nationell tillsynsmyndighet som avses i den allmänna dataskyddsförordningen. Tillsynsansvaret för kakor och andra uppgifter i terminalutrustning samt för fysiska och juridiska personer har antingen dataombudsmannen eller Transport- och kommunikationsverket beroende på om terminalutrustningen hanterar en personuppgift eller någon annan uppgift eller tillhör en fysisk eller en juridisk person. Enligt kommissionens förslag ska gällande artikel 5.3 i direktivet om integritet och elektronisk kommunikation fortsatt tillämpas på uppgifter i juridiska personers terminalutrustning. Den föreslagna ändringen skulle således ändra dagens befogenhetsfördelning mellan dataombudsmannen och Transport- och kommunikationsverket. Förslagets ekonomiska konsekvenser och inverkan på nationell lagstiftning såsom dataskyddslagen (1050/2018) och lagen om tjänster inom elektronisk kommunikation (917/2014) ska granskas närmare.

Enligt artikel 15 i direktivet om integritet och elektronisk kommunikation får medlemsstaterna genom lagstiftning vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som anges i bl.a. artikel 5 i nämnda direktiv. I enlighet med artikel 15 får det exempelvis föreskrivas om rättsvårdande myndigheters åtkomst till data som lagras av leverantörer av elektroniska kommunikationstjänster. Enligt kommissionens förslag ska lagring och användning av personuppgifter i terminalutrustning i fortsättningen regleras i den allmänna

dataskyddsförordningen. Kommissionens förslag inbegriper en liknande undantagsmöjlighet som i artikel 15 i direktivet om integritet och elektronisk kommunikation. I den fortsatta beredningen behöver det göras en närmare bedömning av om ändringen till exempel påverkar vad som kan föreskrivas om rättsvårdande myndigheters rätt till information.

EU-gemensam anmälningsordning för incidenter

Genomförande av en EU-gemensam kontaktpunkt i den form som föreslås av kommissionen skulle medföra datasystemkostnader för myndigheter som tar emot och behandlar anmälningar via den. Sådana myndigheter är i varje fall Transport- och kommunikationsverket, Energimyndigheten, Säkerhets- och kemikalieverket, Tillstånds- och tillsynsverket. Livskraftscentralen i Sydöstra Finland, Livsmedelsverket. Säkerhets- och utvecklingscentret för läkemedelsområdet, Finansinspektionen och Dataombudsmannen. Nämnda myndigheter har på senare tid fått datasystemkostnader när bland annat NIS 2-direktivet, CER-direktivet och den allmänna dataskyddsförordningen genomförts.

I Finland upprätthåller Transport- och kommunikationsverket Traficoms Cybersäkerhetscenter ett system för anmälningar enligt NIS 2-direktivet och cybersäkerhetslagen (124/2025). Om en EU-gemensam anmälningsordning genomförs enligt kommissions förslag skulle det medföra ändringar i systemets funktion. I detta skede kan ändringarnas omfattning eller kostnader inte fastställas i detalj eftersom det saknas tekniska detaljer om genomförandet av anmälningsordningen. Myndighetskonsekvenserna av genomförandet av NIS 2- och CER-direktiven har bedömts i regeringens propositioner om genomförandet av direktiven (RP 57/2024 rd och RP 205/2024 rd).

Enligt kommissionens konsekvensbedömning skulle inrättandet av en EU-gemensam anmälningsordning kosta 6 miljoner euro på EU-nivå. För att upprätthålla EU-systemet skulle det krävas cirka 8 årsverken vid Enisa, och framtida rapportering via systemet i enlighet med de nya rättsakterna beräknas kosta 500 000 euro per rättsakt. Enligt kommissionens konsekvensbedömning varierar uppbyggnadskostnaden för ett motsvarande gemensamt system mellan 150 000 och 1 500 000 euro beroende på medlemsstat och uppgår i snitt till 550 000 euro.

Enligt kommissionens konsekvensbedömning skulle den ekonomiska nyttan av rapportering via det EU-gemensamma systemet uppgå till 0,29–41,5 miljoner euro för de berörda på EU-nivå. Bakom det stora variationsintervallet ligger en osäkerhet om antalet anmälningar. Beräkningen utgår från kommissionens uppskattning att rapporteringen kostar i snitt 440 euro per regleringsobjekt, vilket skulle halveras med ett EU-gemensamt system.

Kommissionen har inte bedömt vilka konsekvenser förslaget har för medlemsstaterna eller befintliga nationella system. Enligt statsrådets initiala bedömning kommer de nationellt anvisade kostnaderna för utveckling av kontaktpunkter i enlighet med NIS 2- och CER-direktiven och den allmänna dataskyddsförordningen att öka eftersom ett genomförande av förslaget kräver ändringar i både kontaktpunkterna och de behandlingsrelaterade datasystemen. Ett genomförande av förslaget skulle innebära nya datasystemkostnader för myndigheterna såsom beskrivits ovan.

Enligt statsrådets initiala bedömning kommer en EU-gemensam kontaktpunkt att minska rapporteringskostnaderna för regleringsobjekten jämfört med nuläget i Finland när samma händelse ska rapporteras på basis av fler än en rättsakt eller till myndigheter i fler än en EU-medlemsstat. Den EU-gemensamma kontaktpunkten skulle dock enligt statsrådets bedömning

även kunna öka rapporteringskostnaderna jämfört med nuläget i Finland när en händelse ska rapporteras på basis av bara en rättsakt eller till en enda myndighet i en EU-medlemsstat.

Europeiska kommissionen uppskattar antalet anmälningar via den EU-gemensamma kontaktpunkten till 1 340–188 000 per år. Trots det stora variationsintervallet kan uppskattningen enligt statsrådets initiala bedömning anses måttfull. År 2024 fick till exempel Dataombudsmannen i Finland totalt 7 152 anmälningar om personuppgiftsincidenter.

Upphävande av vissa rättsakter

Kommissionen konstaterar att det regelverket som tillämpas på onlineplattformar och företagsanvändare förenklas när P2B-förordningen upphävs och överlappande regler i förhållande till förordningarna om digitala tjänster (DSA) och digitala marknader (DMA) tas bort. Kommissionen anser att upphävande av P2B-förordningen minskar risken för rättslig osäkerhet och onödiga kostnader för onlinebaserade tjänster förknippade med efterlevnaden av bestämmelserna, vilket ökar företagens tillit till den rättsliga ramen och uppmuntrar nya aktörer att träda in på EU-marknaden. Enligt kommissionen skulle upphävandet av P2B-förordningen främja ett mer effektivt och riktat genomförande av regelverket eftersom medlemsstaternas ansvar för tillsyn över genomförandet är noga avgränsat i de gällande reglerna. Medlemsstaterna kan fastställa egna liknande regler efter att P2B-förordningen har upphävts, men enligt kommissionen finns det liten risk för att regleringen splittras eftersom DSA och DMA innebär full harmonisering och lämnar därmed bara lite utrymme åt nationella åtgärder.

Enligt kommissionen har vissa medlemsstater under samrådet hänvisat till nuvarande överlappningar mellan P2B-förordningen och annan lagstiftning såsom DSA eller DMA. Likaså uppgav flera företag att de upplevt rättslig osäkerhet och överlappning beroende på överlappningar mellan P2B-förordningen och andra EU-regler. Vissa europeiska forum har till exempel pekat på specifika överlappningar i kravet på att inrätta ett internt system för hantering av klagomål. Överlappande transparenskrav upptäcktes också i bestämmelserna om rangordning, villkor och medling.

Statsrådet anser att kommissionen i sitt arbetsdokument granskar upphävandet av P2B-förordningen främst genom de onlineplattformsföretag som den tillämpas på. P2B-förordningens mål är att trygga transparensen i avtalsförhållanden mellan onlinebaserade förmedlingstjänster av alla storlekar och deras företagsanvändare. Flera av DSA- och DMA-kraven gäller bara onlineplattformstjänster i grindvaktsställning. Risken är att företag som använder onlineplattformstjänster får en svagare ställning i avtal med leverantörer av dessa tjänster om P2B-förordningen upphävs. Enligt P2B-förordningen har företagsanvändare till exempel rätt att få besked 30 dagar innan en tjänst begränsas eller tillfälligt avbryts och rätt att överklaga beslutet (artikel 4). DSA och DMA ger företagsanvändare bara möjligheten att överklaga i efterhand om deras applikationer tas bort.

AI-omnibus

Enligt kommissionen syftar förslaget till en betydande minskning av den administrativa bördan. Enligt de inledande beräkningarna uppskattas de möjliga besparingarna kunna uppgå till ungefär 300–430 miljoner euro per år, och ändringarna skulle även ha icke-kvantifierbara positiva effekter.

Enligt statsrådets initiala bedömning kommer den administrativa bördan för ekonomiska aktörer att minska något genom ändringarna i AI-förordningen, men skillnaden kan inte anses betydande.

Särskilt relevanta är dock förändringarna för midcapföretag eftersom kommissionen uppskattar deras antal i EU till cirka 38 000. Utöver effekterna kan det ses som en lättbegriplig och juridiskt enklare åtgärd att utöka de i vissa delar lättare kraven på små och medelstora företag till små midcapföretag. Lättnader för små midcapföretag ingår i kommissionens allmänna förenklingslinje även inom andra sektorer.

Om kommissionen får befogenhet för tillsyn över AI-system som bygger på samma leverantörs AI-modell för allmänna ändamål eller som är inbyggda i mycket stora plattformar och sökmotorer skulle det stärka kommissionens potential för tillsyn över dessa system, som har en stor och alltjämt växande roll särskilt hos konsumentanvändare och som inte beaktas tillräckligt i den ursprungliga förordningen. Kommissionens tillsyn över dessa kan förväntas vara effektivare än om varje medlemsstat svarar för tillsynen på sitt håll. Kommissionen uppskattas dock behöva 38 nya årsverken för tillsynen. I Finland har det inte avsatts nya resurser för tillsyn över AI-system utan den ska ske inom nuvarande anslag. Därför skulle förslaget inte ge direkta kostnadsbesparingar för nationella myndigheter i Finland till skillnad från bedömningarna i förslaget.

Enligt en samlad bedömning kommer den offentliga förvaltningens administrativa börda eller kostnader inte att minska i någon betydande grad med de föreslagna ändringarna i AI-förordningen. Å andra sidan kommer de inte heller att öka nämnvärt. Om registreringsskyldigheten tas bort för system som används i den offentliga förvaltningen men som inte anses utgöra högrisksystem skulle den administrativa bördan minska något. Längre tidsfrister för tillämpning av förordningens krav skulle ge nationella tillsynsmyndigheter mer tid att förbereda sig på tillsynsuppdraget såsom att ordna det administrativa och utveckla kompetensen. Kravet på nationella myndigheter att främja AI-kunnighet har en öppen utformning och kan potentiellt uppfyllas genom åtgärder som redan planerats och inom nuvarande anslag. Ändringen skulle i varje fall klargöra nuläget, där även små offentliga aktörer och företag måste överväga behovet av åtgärder som främjar AI-kunnighet.

Kravet på att främja AI-kunnighet (artikel 4) har överlag beaktats i rätt stor omfattning av olika aktörer såsom utbildningsanstalter, tredje sektorn, myndigheter och näringslivets intresseorganisationer. Åtgärder för att främja AI-kunnigheten har vidtagits med anledning av artikeln. Sådan verksamhet behövs och välkomnas, men kravet är av allmän karaktär och utan sanktion och skiljer sig därför från det övriga innehållet i förordningen.

I den offentliga debatten före omnibusförslaget och flera medlemsstaters förslag utkristalliserades särskilt förslagen om att senarelägga tillämpningen av förordningens krav. Det handlade särskilt om förseningen av harmoniserade standarder och om AI-system med hög risk. Företagens verksamhet skulle underlättas av en senareläggning, som troligen även minskar de framtida kostnaderna och höjer kvaliteten på genomförandet av kraven när harmoniserade standarder kan användas för efterlevnad av kraven. En senareläggning skulle samtidigt minska lagstiftningens förutsägbarhet på sikt. Företagen har i viss mån förberett sig på att kraven införs och en senareläggning skulle påverka den tidsplanen.

Konsekvenserna av att ändra artikel 4 a om behandling av särskilda kategorier av personuppgifter och att ta bort registreringsskyldigheten för andra än AI-system med hög risk behöver granskas närmare.

6 Förslagets förhållande till grundlagen och till de grundläggande fri- och rättigheterna och de mänskliga rättigheterna

Enligt statsrådets bedömning kommer förslagen att ha inverkan på skyddet för personuppgifter, kommunikationens förtrolighet, offentlighetsprincipen, vetenskapens frihet och näringsfriheten, vilka granskas närmare nedan.

6.1 Skyddet för personuppgifter och kommunikationens förtrolighet

Digital omnibus

Ändringarna i den allmänna dataskyddsförordningen, dataskyddsförordningen för institutioner och direktivet om integritet och elektronisk kommunikation bedöms ha konsekvenser för skyddet av personuppgifter enligt 10 § 1 mom. i grundlagen. Ändringarna i direktivet om öppna data och i dataförvaltningsakten liksom att den materiella regleringen flyttas till dataförordningen kan också ha konsekvenser för skyddet av personuppgifter. Ändringarna i direktivet om integritet och elektronisk kommunikation kan påverka den förtroliga kommunikation som tryggas i 10 § 2 mom. i grundlagen. Personuppgifter skyddas av unions- och internationella instrument såsom Europeiska unionens stadga om de grundläggande rättigheterna och den europeiska konventionen om de mänskliga rättigheterna. Artikel 8 i Europeiska unionens stadga garanterar alla en rätt till skydd för personuppgifter och artikel 7 har bestämmelser om respekt för privat- och familjelivet. Artikel 8 i den europeiska konventionen om de mänskliga rättigheterna innehåller likaså bestämmelser om var och ens rätt till respekt för sitt privatliv.

Genom digital omnibus-förslaget föreslås ändringar som ska skapa klarhet i de osäkra tolkningar av personuppgiftsdefinitionen som bland annat berör anonymisering och pseudonymisering. Enligt kommissionens bedömning syftar ändringen av personuppgiftsdefnitionen enbart till att kodifiera EU-domstolens rättspraxis för pseudonymisering. I målet C-413/23 P ansåg EU-domstolen att pseudonymiserade uppgifter inte ska anses utgöra personuppgifter under alla omständigheter och för alla personer eftersom pseudonymisering, beroende på omständigheterna i det enskilda fallet, faktiskt kan hindra andra personer än den personuppgiftsansvarige från att identifiera den registrerade, så att de inte längre kan identifiera den registrerade. Om definitionen av personuppgifter ändras kan det ha vittgående konsekvenser för nivån på skyddet av personuppgifter i EU. Ändringen kan också ha konsekvenser för fullgörandet av Finlands och andra EU-länders bindande internationella åtaganden såsom Europarådets konvention om skydd för enskilda vid automatisk behandling av personuppgifter (FördrS 35—36/1992, nedan dataskyddskonvention 108).

Kommissionen föreslår att utveckling och drift av AI-system i fortsättningen får grundas främst på berättigat intresse, om annan unionsrätt eller nationell rätt inte uttryckligen kräver registrerades samtycke. Utveckling och drift av AI-system kan inbegripa hög risk för registrerade med tanke på skyddet av personuppgifter, särskilt i fråga om AI-system med hög risk och särskilda kategorier av personuppgifter. Skyddsnivån för personuppgifter.kan försämras särskilt i högrisksituationer ifall behandlingen grundas på berättigat intresse i stället för registrerades samtycke.

Grundlagsutskottet (GrUU 14/2018 rd) har fäst avseende vid de hot och risker som behandlingen av personuppgifter medför. Denna omständighet är av särskild betydelse när det gäller behandling av särskilda kategorier av personuppgifter. Enligt utskottet kan behandlingen i fråga innebära allvarliga risker med avseende på informationssäkerhet och missbruk av uppgifter, som i sista hand kan utgöra ett hot mot personens identitet (GrUU 13/2016 rd, s. 4,

GrUU 14/2009 rd, s. 3/I) och särskilt påpekat att det bör finnas exakta och noga avgränsade bestämmelser om att det är tillåtet att behandla känsliga uppgifter bara om det är absolut nödvändigt (se t.ex. GrUU 3/2017 rd, s. 5). Att begränsa behandlingen till det nödvändiga stöds också av artikel 52.1 i EU:s stadga om de grundläggande rättigheterna. Unionens domstol har härvid ansett att begränsningarna inte får gå utöver vad som är strikt nödvändigt, och den lagstiftning som innebär ett ingrepp måste innehålla tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden (se mål 740/22, 52 punkten, mål C-439/19, 105 punkten, mål 172–176 punkten, mål C-13/16, 30 punkten, de förenade målen C-92/09 och C-93/09, 86 punkten, mål C-473/12, 39 punkten och mål C-212/13, 28 punkten). När unionens domstol bedömt nödvändigheten av begränsningarna har den ansett att nödvändighetskravet inte uppfylls ifall målet rimligen kan uppnås lika effektivt på sätt som inte begränsar registrerades grundläggande rättigheter lika mycket (se t.ex. mål C-548/21, 87 och 88 punkten med hänvisningar till rättspraxis).

Avseende utveckling och drift av AI-system föreslås också en ny grund för undantag som gäller biometriska uppgifter vid behandling av särskilda kategorier av personuppgifter. Enligt kommissionens bedömning medför behandling av biometriska uppgifter för att bekräfta en persons identitet (kontroll) sannolikt inte några betydande risker för hans eller hennes grundläggande rättigheter och friheter. Den personuppgiftsansvarige kommer inte, eller endast under en mycket begränsad tid, att få kännedom om de biometriska uppgifterna under behandlingen för kontroll och den registrerade har ensam kontroll över autentiseringsprocessen. Med hänsyn till unionsrätten och grundlagsutskottets utlåtandepraxis bör behandling av särskilda kategorier av personuppgifter begränsas till det nödvändiga och regleringen innehålla ändamålsenliga och adekvata skyddsåtgärder för att skydda registrerades rättigheter.

Digital omnibus innebär lättnader i personuppgiftsansvarigas skyldighet att informera registrerade om rapporteringsskyldigheten. Föreslagna ändringar som minskar den administrativa bördan och förenklar regleringen skulle enligt kommissionens bedömning inte ha negativa konsekvenser för skyddsnivån för personuppgifter utan en tydligare reglering kan till viss del rent av anses förbättra skyddsnivån. I fråga om den föreslagna regleringen finns dock skäl att säkerställa att den föreslagna regleringen inte är för översiktlig så att den ger möjlighet till mer omfattande avsteg från skyddsnivån för personuppgifter (se GrUU 14/2018 rd och EU-domstolens mål 740/22 (52 punkten) och C-439/19 (105 punkten och 172–176 punkten). Allmänna och omfattande undantag från bestämmelserna om information till registrerade kan de facto begränsa deras rätt att få information om behandlingen av sina personuppgifter, en rätt som garanteras i dataskyddsförordningen. Om anmälningströskeln för uppgiftsincidenter höjs till hög risk och anmälningsfristen samtidigt förlängs kan det också försämra dagens skyddsnivå för personuppgifter eftersom syftet med anmälan kan äventyras ju längre tiden går mellan uppgiftsincidenten och anmälan till dataskyddsmyndigheten. Förslaget kan indirekt även påverka hur den registrerade får information om en uppgiftsincident.

Kommissionen bedömer att förslaget med inriktning på att minska antalet förfrågningar om kakor förbättrar skyddsnivån för användarna. Genom förslaget skulle användarna få äkta valmöjligheter och fördelar av regleringens skydd. Att säkerställa tillräcklig information är väsentligt både för samtycket och den registrerades rätt att invända så att registrerade har möjlighet att påverka behandlingen av sina personuppgifter. Överensstämmelsen med reglerna för samtycke och rätten att invända i dataskyddsförordningen och dataskyddsförordningen för institutioner samt med direktivet om integritet och elektronisk kommunikation ska också säkerställas.

AI-omnibus

Med hänsyn till artikel 52.1 i stadgan om de grundläggande rättigheterna och relevant EU-domstolspraxis samt grundlagsutskottets praxis i utlåtanden om behandling av känsliga personuppgifter ska begränsningar av skyddet för personuppgifter genomföras inom gränserna för det som är absolut nödvändigt, och regelverk som innebär ingrepp i skyddet av personuppgifter ska ha tydliga och exakta bestämmelser om åtgärdens omfattning och tillämpning. Vad gäller förslagen om artikel 4 a i AI-förordningen och AI-system med hög risk bör det övervägas ifall nödvändighetskravet ska behållas för att säkerställa att särskilda kategorier av personuppgifter behandlas inom nödvändighetens gränser och att dagens höga skyddsnivå för personuppgifter bibehålls.

6.2 Offentlighetsprincipen, vetenskapens frihet och näringsfrihet

Med ändringarna i dataförordningen och kapitel III och IV i dataförvaltningsakten (som föreslås bli flyttade till förordningen), eftersträvas främst lättnader i den administrativa bördan för aktörerna och förslaget innehåller inte väsentliga nya krav för företagen. Förslaget utökar vissa lättnader för små och medelstora företag till att omfatta små midcapföretag. Åtskillnaden kan anses ske på objektiva och godtagbara grunder och vara proportionerlig. Förslaget är således inte problematiskt med tanke på näringsfriheten eller likabehandlingen av företag.

Ändringarna i direktivet om öppna data och kapitel II i dataförvaltningsakten och att reglering flyttas till dataförordningen kan ha inverkan på offentlighetsprincipen enligt 12 § 2 mom. i grundlagen i delar som berör utlämning av handlingar som innehas av myndigheter samt inverkan på vetenskapens frihet enligt 16 § 2 mom. i grundlagen i delar som berör framläggande av forskningsdata genererade med offentliga medel.

Ändringarna och att reglering flyttas kan också ha inverkan på näringsfriheten enligt 18 § 1 mom. i grundlagen i delar som tillämpas på forskningsdata genererade med offentliga medel och handlingar som innehas av vissa företag under offentlig kontroll samt i delar där avvikande villkor och avgifter kan tillämpas på vidareutnyttjande av handlingar och data om företagen uppfyller vissa kriterier.

Förslagen om incidentrapportering och en EU-gemensam kontaktpunkt innebär inte ändringar i nu gällande bestämmelser om datainnehåll som omfattas av anmälnings- och rapporteringsskyldighet eller om anmälnings- eller rapporteringsfrågor. I denna del påverkar förslaget således inte näringsfriheten enligt 18 § i grundlagen.

7 Ålands behörighet

18, 27 och 29 § i självstyrelselagen för Åland (1144/1991, nedan även självstyrelselagen) reglerar fördelningen av lagstiftningsbehörighet mellan landskapet Åland och riket. Ansvaret för att genomföra unionslagstiftning fördelas enligt den föreskrivna behörighetsfördelningen i självstyrelselagen. Landskapet ansvarar för genomförandet av unionsakter till den del som ärendet omfattas av dess behörighet enligt självstyrelselagen.

Vad gäller dataåtkomst och -delning samt relaterad myndighetstillsyn har riket ansetts ha lagstiftningsbehörighet till största del. Riket har lagstiftningsbehörighet i fråga om statsmyndigheternas organisation och verksamhet (27 § 3 punkten i självstyrelselagen) Flera av bestämmelserna i dataförordningen kan anses beröra den privata sektorns verksamhet, som hör

till rikets behörighet (27 § 8, 10 och 41 punkten i självstyrelselagen). Enligt 18 § 1 punkten i självstyrelselagen för Åland har landskapet lagstiftningsbehörighet i fråga om landskapsregeringen och under denna lydande myndigheter och inrättningar. Dessutom har landskapet enligt 4 punkten lagstiftningsbehörighet i fråga om kommunernas förvaltning. I lagstiftningskontrollen har det ansetts att offentligheten för handlingar som myndigheterna förfogar över hör till landskapet Ålands lagstiftningsbehörighet. Vad gäller direktivet om öppna data och kapitel II i dataförvaltningsakten är det således Åland som har lagstiftningsbehörighet enligt 18 § 2 och 4 punkten i självstyrelselagen.

I fråga om den allmänna dataskyddsförordningen har det i lagstiftningskontrollen av de landskapslagar som avses i 19 § i självstyrelselagen ansetts att skyddet för personuppgifter som innehas av Ålands landskap och kommuner ingår i landskapets lagstiftningsbehörighet enligt 18 § 1 och 4 punkten i självstyrelselagen. Förslaget till förordning påverkar angelägenheter inom landskapet Ålands lagstiftningsbehörighet när sådan behandling av personuppgifter som avses i förslaget berör angelägenheter eller verksamheter som tas upp i 18 § 1 och 4 punkten i självstyrelselagen.

Dataskyddsförordningen för institutioner tillämpas på behandlingen av personuppgifter i unionens institutioner, organ och byråer och i denna del förefaller kommissionens förslag inte beröra de frågor om skydd för personuppgifter som ingår i landskapet Ålands lagstiftningsbehörighet.

AI-förordningen ingår delvis i Ålands och delvis i rikets lagstiftningsbehörighet. Enligt 18 § 22 punkten i självstyrelselagen för Åland har landskapet lagstiftningsbehörighet i fråga om näringsverksamhet med beaktande av vad som stadgas i 27 § 1 mom. 2, 10, 12, 40 och 41 punkten. Riket har lagstiftningsbehörighet i fråga om utövande av yttrande-, förenings- och församlingsfriheten och brev-, telegraf- och telefonhemligheten enligt 27 § 1 mom. 2 punkten i självstyrelselagen samt i fråga om konsumentskydd enligt 10 punkten, utrikeshandel enligt 12 punkten och televäsendet enligt 40 punkten. Vid tolkning av 27 § 1 mom. 40 punkten i självstyrelselagen ska det noteras att informationsnät som internet inte kunde beaktas när självstyrelselagen stiftades (se GrUU 22/2001 rd). Vad gäller dataskydd anses landskapet ha lagstiftningsbehörighet enligt 18 § 1 och 4 punkten i självstyrelselagen. I fråga om marknadstillsyn över AI-system med hög risk har landskapet lagstiftningsbehörighet i vissa delar (sjö- och vägtrafik, undervisning och utbildning, främjande av sysselsättningen, hälso- och sjukvård, socialvård, allmän ordning och säkerhet, brand- och räddningsväsendet, nödcentralsverksamhet, kritisk infrastruktur) och riket i vissa delar (bank- och kreditväsendet, försäkringsavtal, arbetspensionsskydd, arbetsrätt, televäsendet, medicinsk utrustning, tryckbärande anordningar, linbaneanläggningar och radioutrustning).

8 Behandling av förslaget i Europeiska unionens institutioner och de övriga medlemsstaternas ståndpunkter

Behandlingen av förslaget inleddes den 21 november 2025 i rådets förenklingsunderarbetsgrupp Antici. Europaparlamentet har ännu inte valt det utskott som ska ansvara för huvudbehandlingen av förslagen. Föredragande har ännu inte valts för betänkandet.

Majoriteten av medlemsstaterna har initialt förhållit sig skeptiska till förslaget om en EU-gemensam kontaktpunkt. Medlemsstaternas frågor gäller särskilt hänsynen till nationella system, nationell säkerhet, kontaktpunktens säkerhet och praktiskt genomförande. Därtill har det ställts preciserande frågor, särskilt om ändringsförslagen avseende dataskyddsregleringen och AI-förordningen.

9 Nationell behandling av förslaget

U-skrivelsen har beretts som ett tjänsteuppdrag vid kommunikationsministeriet. Beredningssamarbete har skett med arbets- och näringsministeriet, finansministeriet, justitieministeriet och inrikesministeriet.

Kommunikationsministeriet ordnade ett samråd för intressenter och myndigheter den 26 november 2025.

Ett utkast till U-skrivelse behandlades på ett gemensamt möte för sektionerna konkurrenskraft (EU-8) och kommunikation (EU-19) den 19 december 2025 samt i skriftligt förfarande 19.12.2025–7.1.2026. I samband med detta behandlades även E-skrivelsen om datauniONstrategin.

Utkastet till U-skrivelse har behandlats i EU-ministerutskottet den 23 januari 2026.

10 Statsrådets ståndpunkt

10.1 Allmän ståndpunkt

Statsrådet stöder kommissionens mål att förenkla regleringen. Åtgärderna ska vara modiga, målinriktade och på riktigt minska företagens administrativa börda. Statsrådet anser det viktigt att EU:s digital- och cyberlagstiftning utgör en tydlig och integrerad helhet så att kraven är tydliga och proportionerliga. Statsrådets mål är bättre och mindre EU-reglering. Statsrådet understryker att åtgärderna ska konkret främja en smidigare vardag samt konkurrenskraft och rättssäkerhet.

Enligt statsrådets uppfattning är kommissionens förslag i huvudsak sådana att de kan harmonisera regleringen, främja digitaliseringen och lätta den administrativa börda som följer av EU-regleringen, särskilt för företagen. Statsrådet anser det nödvändigt att man i följande skeden ambitiöst genomför viktiga åtgärder för att minska den administrativa bördan av regleringen inom ramen för en bredare granskning av regelverket på det digitala området (Digital Fitness Check).

Statsrådet anser att man i de fortsatta förhandlingarna bör se till att delegeringen av befogenheter till kommissionen för genomförandet och för att anta akter är ändamålsenlig samt tillräckligt noga avgränsad och exakt. Statsrådet anser det också viktigt att tiden för genomförandet och övergångsperioden är tillräcklig och förutsebar.

Statsrådet instämmer i hur kommissionen ser på betydelsen av AI som drivkraft för digitalisering och innovation. Statsrådet framhåller också betydelsen av andra nya teknologier under utveckling.

10.2 Kommissionens förslag: digital omnibus

Dataförordningen

Statsrådet ställer sig bakom en unionsomfattande horisontal datareglering som harmoniserar kraven i olika medlemsländer och sektorer.

Statsrådet stöder förslaget att åtkomst till data som innehåller företagshemligheter även kan förhindras på grund av otillräcklig skyddsnivå i jurisdiktioner utanför EU. Samtidigt ser statsrådet det som viktigt att främja digital handel och ett internationellt regelbaserat system som säkerställer internationella dataflöden samt en hög nivå av dataskydd och -säkerhet internationellt.

Statsrådet stöder precisering av dataförmedlingstjänstdefinitionen, frivilligt anmälningsförfarande och lättnader i kraven.

Statsrådet anser det viktigt att dataregleringen lämnar ett tillräckligt nationellt handlingsutrymme, särskilt i reglering som hittills varit av minimikaraktär och avser utlämning av myndighetshandlingar. Då blir det möjligt att beakta till exempel den nationella offentlighetslagstiftningen samt nationella åtgärder som främjar interoperabilitet och hantering av data.

Statsrådet betonar att den nationella lagstiftningen och offentliga sektorn har en varierande roll i olika medlemsstater och regelverket bör möjliggöra olika sätt att organisera tjänsterna och modellerna för dataförmedling. Regelverket bör också möjliggöra omorganisering av verksamheter så att kraven på myndigheterna och tillsynen kan ordnas vid behov. När det gäller administrativa strukturer och förfaranden ska sektorsspecifika behov och samarbetet mellan behöriga organ uppmärksammas.

Statsrådet anser att ändringarna i vidareutnyttjandet av data från den offentliga sektorn gör helheten otydlig, och därför bör konsekvenserna av dessa bedömas närmare i den fortsatta beredningen. Statsrådet förhåller sig skeptiskt till förslaget att de allmänna bestämmelserna i kapitel IX i dataförordningen ska tillämpas på det nya kapitlet VIIc. De allmänna bestämmelserna skulle innebära materiellt ny reglering av den offentliga förvaltningen och utgivarna av forskningsdata, och sådan finns inte i de upphävda rättsakterna.

I den fortsatta beredningen bör det göras en närmare bedömning av de föreslagna ändringarna i förhållande till den nationella offentlighetslagstiftningen, särskilt om ändringen kan ha inverkan på grundlagens offentlighetsprincip och vetenskapens frihet genom att begränsa myndigheters utlämning av handlingar samt tillgången till forskningsdata som har genererats med offentliga medel.

Statsrådet anser att ändringsförslagen om Europeiska datainnovationsstyrelsen kräver närmare bedömning i den fortsatta beredningen. Det bör ägnas uppmärksamhet åt ändamålsenlig organisering av samarbetet mellan behöriga myndigheter och kommissionen.

Den allmänna dataskyddsförordningen, dataskyddsförordningen för institutioner och direktivet om integritet och elektronisk kommunikation

Statsrådet förhåller sig i princip positivt till kommissionens mål att förtydliga och förenkla den allmänna dataskyddsförordningen och dataskyddsförordningen för institutioner i syfte att minska den administrativa bördan, stärka EU:s konkurrenskraft och stödja införandet av ny teknik. Statsrådet ser det som viktigt att förslagen stöttar framförallt små och medelstora företag och andra mindre aktörer och även tar hänsyn till den offentliga sektorn.

Statsrådet förhåller sig i princip positivt till förslagets mål att reda ut oklarheterna kring anonymisering och pseudonymisering, vetenskaplig forskning samt utveckling och drift av AI-system för att förbättra rättssäkerheten, främja innovation och säkerställa en enhetlig tolkning i EU. Statsrådet anser det dock viktigt att man under förhandlingarna säkerställer att förslagen de

facto inte försämrar dagens dataskyddsnivå och registrerades rättigheter, även med hänsyn till den dataskyddsnivå som föreskrivs i Europarådets ändrade dataskyddskonvention 108. Här ska man framförallt uppmärksamma kommissionens förslag att komplettera personuppgiftsdefinitionen och under förhandlingarna säkerställa att föreslagna ändringar som rör anonymisering och pseudonymisering är tillräckligt tydliga och noga avgränsade. I förhandlingarna ska det även säkerställas att definitionen av vetenskaplig forskning är tillräckligt tydlig och exakt så att den inte försämrar dagens dataskyddsnivå utan främjar vetenskaplig forskning och innovation. För att garantera rättssäkerheten och lätta den administrativa bördan ska man överlag under förhandlingarna ägna uppmärksamhet åt den föreslagna regleringens tydlighet och exakthet.

Statsrådet anser det viktigt att man under förhandlingarna säkerställer att den föreslagna regleringen i alla delar är proportionerlig och att delegeringen av befogenheter till kommissionen för genomförandet och för att anta akter är ändamålsenlig samt tillräckligt noga avgränsad och exakt. Statsrådet anser att man i den fortsatta beredningen även ska klargöra nivån för eventuella administrativa sanktionsavgifter i den föreslagna regleringen som rör behandling av personuppgifter i bland annat kakor och AI-system.

När det gäller behandling av särskilda kategorier av personuppgifter anser statsrådet det viktigt att man under förhandlingarna säkerställer ändamålsenliga och adekvata skyddsåtgärder samt begränsar avsaknaden av skydd till det som är nödvändigt. Statsrådet förhåller sig positivt till att höja tröskeln för anmälan av personuppgiftsincidenter till dataskyddsmyndigheterna. Men eftersom det rör sig om behandling som inbegriper hög risk för skyddet av registrerade är statsrådet skeptiskt till att tidsfristerna för anmälan förlängs jämfört med i dag.

Statsrådet välkomnar i princip att regleringen av kakor förnyas. Regleringen ska främja såväl elektroniska tjänsters tillförlitlighet som utvecklingen av ansvarsfull digital affärsverksamhet och tjänster. På vissa områden såsom medierna och den offentliga sektorn kan ett adekvat handlingsutrymme behöva tryggas inom ramen för ett balanserat regelverk. Statsrådet ställer sig bakom åtgärder som ökar tjänsternas tillgänglighet. Regleringen ska dock säkerställa registrerades möjligheter att påverka vilka egna personuppgifter som samlas in och behandlas och få tillräcklig information om behandlingen.

Statsrådet betonar att man i den fortsatta beredningen bör säkerställa att förslagen till reglering i den allmänna dataskyddsförordningen och dataskyddsförordningen för institutioner i alla delar överensstämmer med och är tydliga i förhållande till direktivet om integritet och elektronisk kommunikation. Enligt statsrådets initiala uppfattning är det inte nödvändigtvis en ändamålsenligt lösning att en del av uppgifterna i terminaler (såsom kakor) fortsatt skulle omfattas av direktivet om integritet och elektronisk kommunikation medan behandlingen av personuppgifter förs till den allmänna dataskyddsförordningen ifall detta leder till att andra uppgifter får ett starkare skydd än personuppgifter. Statsrådet fäster uppmärksamhet vid att uppgifter som lagras i terminalutrustning inte är begränsade till kakor utan omfattar även andra data såsom foton, kontaktuppgifter och dokument. Därför ska andra än samtyckesbaserade grunder för behandlingen vara noga avgränsade och proportionella.

EU-gemensam kontaktpunkt för incidentrapportering

Statsrådet stöder åtgärder som minskar den administrativa bördan av och kostnaderna för incidentrapportering enligt olika rättsakter. Statsrådet anser det viktigt att incidentrapporteringen ordnas på ett ändamålsenligt sätt. Statsrådet stöder harmonisering av medlemsstaternas rapportering, med beaktande av befintliga nationella lösningar avseende handlingsutrymme och organisering av myndigheternas ansvarsuppgifter. Statsrådet förhåller

sig positivt till att medlemsstaterna åläggs ta emot anmälningar enligt olika rättsakter antingen via den EU-gemensamma kontaktpunkten eller någon annan gemensam kanal för olika anmälningar.

Statsrådet noterar att en centralisering av incidentrapporteringen till ett enda system på EU-nivå inbegriper risker avseende anhopning av data och systemets funktion. Statsrådets ambition är att under förhandlingarna få närmare uppgifter av kommissionen om systemets datasäkerhet och dess inverkan på befintliga system. Statsrådet ser det som viktigt att man säkerställer den EU-gemensamma kontaktpunktens datasäkerhet, tillförlitlighet och tillräckliga funktionaliteter. Innan Europeiska unionens cybersäkerhetsbyrå Enisa anvisas nya uppgifter ska dess förmåga att sköta dessa bedömas.

Vad gäller kommissionens förslag att föremålen för regleringen i alla situationer ska anmäla och rapportera incidenter via en EU-gemensam kontaktpunkt är det enligt statsrådets uppfattning osäkert om detta bidrar till regelförenkling, målet att minska den administrativa bördan eller till kostnadsbesparingar. När anmälningspliktiga uppgifter har att göra med den nationella säkerheten eller försvaret bör anmälningskravet kunna uppfyllas genom nationella arrangemang. Statsrådet förhåller sig positivt till att föremålen för regleringen ges handlingsutrymme för genomförandet av rapporteringen till den del det främjar regleringens mål. Statsrådet förhåller sig kritiskt till att föremålen för regleringen ska vara skyldiga att rapportera via den EU-gemensamma kontaktpunkten i alla situationer.

Statsrådet stöder åtgärder som främjar informationsutbytet mellan medlemsstaterna avseende cybersäkerhetsincidenter utan att det överlappar nuvarande funktioner. Statsrådet understryker att övergången till en EU-gemensam kontaktpunkt inte får försämra tillsynsmyndigheternas rättigheter och faktiska möjligheter att tillräckligt snabbt erhålla uppgifter som de behöver för att sköta sitt uppdrag. EU-regleringen får inte heller bli ett hinder för att information vid behov överförs till en annan myndighet, exempelvis för uppdrag inom krishantering. Vidare anser statsrådet att man ska undvika överlappningar i Enisa uppdrag samt på EU-nivå fokusera på åtgärder med särskilt mervärde.

Statsrådet anser det viktigt att man under vidarebehandlingen av förslaget på ovan beskrivet sätt bedömer det i förhållande till subsidiaritetsprincipen samt den nationella säkerheten och försvaret.

Upphävande av vissa rättsakter

Statsrådet anser att man under förhandlingarnas gång bör få mer information om hur kommissions förslag att upphäva P2B-förordningen påverkar de europeiska företagens konkurrenskraft. I förhandlingarna bör det specificeras hur man framöver garanterar rättssäkerheten för företag som använder onlineplattformar och ingått avtal med plattformsföretag.

10.3 Kommissionens förslag: AI-omnibus

Statsrådet välkomnar överlag förslagen om att förenkla AI-förordningen och minska den administrativa bördan av denna. Statsrådet anser det dock viktigt att säkerställa att den föreslagna regleringen i alla delar är proportionerlig och förordar att artikel 16 i EUF-fördraget prövas som ytterligare rättslig grund under förhandlingarna eftersom ändringarna i AI-förordningen delvis även berör skyddet för personuppgifter.

Statsrådet förhåller sig i princip positivt till förslaget att möjliggöra mer omfattande behandling av särskilda kategorier av personuppgifter för att säkerställa att bias kan upptäckas och korrigeras i alla AI-system. Under förhandlingarna bör dock ändamålsenliga och adekvata skyddsåtgärder säkerställas för AI-system med hög risk, och avsaknaden av skydd för personuppgifter ska begränsas till det som är nödvändigt, särskilt med hänsyn till högriskfaktorn i AI-system med hög risk.

Statsrådet välkomnar att tillämpningen av kraven på högrisksystem senareläggs för att ge mer tid åt beredning av harmoniserade standarder och förberedelse inför förordningens krav. Företagen och övriga aktörer, däribland den offentliga sektorn, ska få besked om kravens ikraftträdande i tillräckligt god tid före augusti 2026, då AI-förordningens krav på AI-system med hög risk i bilaga III senast ska börja iakttas. Statsrådet understryker därför vikten av att ändringarna i AI-förordningen behandlas skyndsamt. Statsrådet kan även tänka sig att ändringar gällande senareläggning av tillämpningen bryts ut till en egen helhet som prioriteras tidsmässigt mot övriga AI-omnibus i den fortsatta behandlingen.

Det är viktigt att en tydlig bortre gräns för kravens ikraftträdande fastställs på ett sätt som klargör det rättsliga läget och minskar kostnaderna och den administrativa börda som oförutsägbarheten orsakar företagen. Statsrådet ställer sig även bakom förslaget att senarelägga transparenskravet för artificiellt innehåll.

Statsrådet anser att förslagen om AI-förordningen endast innebär en liten minskning av den administrativa bördan och kostnaderna för företag och offentliga aktörer som använder AI och att man i förhandlingarna bör sträva efter att hitta ytterligare sätt att minska dessa när det är möjligt. Enligt statsrådet är det dock viktigt att föreslagna ändringar i AI-förordningen såsom lättnader i registreringsskyldigheten inte försämrar dagens nivå av skydd för personuppgifter.