Regeringens proposition till riksdagen med förslag till lagar om ändring av lagar som har samband med genomförandet Europeiska unionens av direktiv om nät- och informationssäkerhet

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det för vissa leverantörer av samhällsviktiga tjänster och vissa leverantörer av digitala tjänster ett antal skyldigheter som gäller hantering av informationssäkerhetsrisker samt rapportering av störningar. Dessutom införs bestämmelser om tillsyn över dessa skyldigheter, om informationsutbyte mellan myndigheter samt om myndigheternas allmänna verksamhet i anknytning till informationssäkerhet. Genom den föreslagna lagstiftningen införlivas Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen i den nationella lagstiftningen.

Propositionen bidrar till att genomföra målen i regeringsprogrammet att främja digitaliseringen och säkerställa den digitala säkerheten genom att förbättra informationssäkerhetsnivån för de tjänster som är viktiga för samhället och medborgarna. Genom propositionen ökas medborgarnas och företagens förtroende för digitaliseringen och främjas därmed också den digitala affärsverksamhetens tillväxt och konkurrenskraft.

För att förbättra informationssäkerheten för samhällsviktiga tjänster införs i informationssamhällsbalken, luftfartslagen, järnvägslagen, lagen om fartygstrafikservice, lagen om sjöfartskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet, lagen om transportservice, elmarknadslagen, naturgasmarknadslagen och lagen om vattentjänster bestämmelser om skyldigheten för viktiga tillhandahållare av tjänster att hantera riskerna i fråga om kommunikationsnät och informationssystem samt att till den myndighet som utövar tillsyn och till allmänheten rapportera störningar som är betydande med tanke på informationssäkerheten. Skyldigheterna enligt informationssamhällsbalken gäller tillhandahållare av internetbaserade marknadsplatser, sökmotortjänster och molntjänster. Skyldigheterna enligt luftfartslagen gäller leverantörer av flygtrafiktjänster samt operatörer av samhällsviktiga flygplatser. Skyldigheterna enligt järnvägslagen gäller förvaltaren av statens bannät samt bolag som tillhandahåller trafikledningstjänster. Skyldigheterna enligt lagen om fartygstrafikservice gäller leverantörer av fartygstrafikservice. Skyldigheten enligt lagen om sjöfartskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet gäller innehavare av samhällsviktiga hamnar. Skyldigheterna enligt lagen om transportservice gäller förvaltare av intelligenta trafiksystem. Skyldigheten enligt elmarknadslagen gäller nätinnehavare. Skyldigheterna enligt naturgasmarknadslagen gäller överföringsnätsinnehavare och skyldigheterna enligt lagen om vattentjänster vattentjänstverk som levererar eller tar emot avloppsvatten minst 5 000 kubikmeter vatten per dygn.

De sektorsvisa tillsynsmyndigheterna har behörighet att utöva tillsyn över fullgörandet av skyldigheterna i fråga om riskhantering och rapportering av störningar. Dessa är Kommunikationsverket, Trafiksäkerhetsverket, Energimyndigheten, Finansinspektionen samt närings-, trafik- och miljöcentralen. För att trygga samarbetet mellan myndigheterna föreslås att det i anslutning till bestämmelserna om myndigheternas behörighet införs bestämmelser om samarbete mellan tillsynsmyndigheterna samt om utbyte av sekretessbelagd information som behövs för skötseln av uppgifter som gäller informationssäkerheten.

Dessutom införs bestämmelser om Kommunikationsverkets skyldighet att samarbeta med de enheter för hantering av it-säkerhetsincidenter, de tillsynsmyndigheter och den samarbetsgrupp för medlemsstaterna som avses i direktivet om nät- och informationssäkerhet.

De föreslagna lagarna avses träda i kraft den 1 maj 2018.

———————

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL 1
ALLMÄN MOTIVERING 5
1 INLEDNING 5
2 NULÄGE 7
2.1 Lagstiftning och praxis 7
2.1.1 Allmänt 8
2.1.2 Strategierna för informationssäkerhet och cybersäkerhet i Finland 8
2.1.3 Samhällsviktiga funktioner 9
2.1.4 Kvalitetskrav och riskhanteringsrelaterade krav på leverantörer av tjänster samt rapportering av säkerhetsstörningar till myndigheterna 10
2.1.5 Försörjningsberedskap och förberedelse för undantagsförhållanden 21
2.1.6.Övrig lagstiftning av betydelse för informationssäkerheten i samhällsviktiga tjänster 22
2.1.7 Myndighetstillsyn och lägesbilden 24
2.1.8 Samarbete och utbyte av information mellan myndigheter 28
2.1.9 Påföljder 28
2.2 Den internationella utvecklingen samt lagstiftningen i utlandet och i EU 29
2.2.1 EU-lagstiftningen 29
2.2.2 Den internationella utvecklingen 37
2.3 Bedömning av nuläget 40
2.3.1 Informationssäkerhetsstrategin 40
2.3.2 Åtgärder till följd av it-säkerhetsincidenter och undersökning av dem 40
2.3.3 Samhällsviktiga tjänster och leverantörer av samhällsviktiga tjänster 41
2.3.4 Krav som gäller tjänsteleverantörernas verksamhet med avseende på informationssäkerhetsrisker och rapportering 47
2.3.5 Tillsyn över riskhanterings- och rapporteringsskyldigheter 52
3 MÅLSÄTTNING OCH DE VIKTIGASTE FÖRSLAGEN 53
3.1 Målsättning 53
3.2 Alternativ 53
3.3 De viktigaste förslagen 55
4 PROPOSITIONENS KONSEKVENSER 56
4.1 Ekonomiska konsekvenser 56
4.2 Konsekvenser för myndigheterna 57
4.3 Samhälleliga konsekvenser 57
5 BEREDNINGEN AV PROPOSITIONEN 58
5.1 Beredningsskeden och beredningsmaterial 58
5.2 Remissyttranden och hur de har beaktats 59
6 SAMBAND MED ANDRA PROPOSITIONER 59
6.1 Propositionens samband med Ålands självstyrelse 60
DETALJMOTIVERING 61
1 LAGFÖRSLAG 61
1.1 Lagen om ändring av informationssamhällsbalken 61
1.2 Lagen om ändring av luftfartslagen 64
1.3 Lagen om ändring av järnvägslagen 66

1.4 Lagen om ändring av lagen om fartygstrafikservice....68
1.5 Lagen om ändring av lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet....70
1.6 Lagen om ändring av lagen om transportservice....72
1.7 Lagen om ändring av elmarknadslagen....74
1.8 Lagen om ändring av naturgasmarknadslagen....75
1.9 Lagen om ändring av 27 och 28 § i lagen om tillsyn över el- och naturgasmarknaden....76
1.10 Lagen om ändring av lagen om vattentjänster....77
1.11 Lagen om ändring av lagen om Finansinspektionen....79
2 IKRAFTTRÄDANDE....79
3 FÖRHÅLLANDE TILL GRUNDLAGEN SAMT LAGSTIFTNINGSORDNING....79
LAGFÖRSLAG....82
om ändring av informationssamhällsbalken....82
om ändring av luftfartslagen....85
om ändring av järnvägslagen....87
om ändring av lagen om fartygstrafikservice....88
om ändring av lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet....90
om ändring av lagen om transportservice....92
om ändring av elmarknadslagen....93
om ändring av naturgasmarknadslagen....94
om ändring av 27 och 28 § i lagen om tillsyn över el- och naturgasmarknaden....95
om ändring av lagen om vattentjänster....96
om ändring av lagen om Finansinspektionen....97
PARALLELLTEXT....98
om ändring av informationssamhällsbalken....98
om ändring av luftfartslagen....102
om ändring av järnvägslagen....104
om ändring av lagen om fartygstrafikservice....106
om ändring av lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet....108
om ändring av lagen om transportservice....110
om ändring av elmarknadslagen....112
om ändring av naturgasmarknadslagen....114
om ändring av 27 och 28 § i lagen om tillsyn över el- och naturgasmarknaden....115
om ändring av lagen om vattentjänster....117
om ändring av lagen om Finansinspektionen....119

ALLMÄN MOTIVERING

1 Inledning

Informations- och kommunikationstekniken och de tjänster som hör samman med dem förändrar samhällets mekanismer och maktstrukturer på ett omvälvande sätt. Sakernas internet, utvecklingen av intelligent automatisering av trafiken och utnyttjandet av massdata samt spridningen av robotteknik och olika smarta tekniker är exempel på tekniska innovationer som digitaliseringen möjliggör.

Digitaliseringen kan utgöra en katalysator för ekonomisk aktivitet. Den tekniska utvecklingen gör det möjligt att erbjuda nya slags tjänster som är skräddarsydda efter kundernas behov och att tillägna sig mer ekonomiska och effektiva verksamhetssätt. Juha Sipiläs regering har därför som mål att ta ett produktivitetssprång inom den offentliga servicen och den privata sektorn genom att främja digitaliseringen och utnyttja dess möjligheter. För att detta ska bli verklighet är ett av spetsprojekten i regeringsprogrammet att skapa en tillväxtmiljö för digital affärsverksamhet.

Samtidigt som digitaliseringen möjliggör nya innovationer och verksamhetssätt blir allt fler tjänster mer beroende av tillförlitligt fungerande kommunikationsnät och informationssystem. Detta gäller även föremål, anordningar och fordon, av vilka en allt större del är uppkopplade till internet och vars funktioner styrs genom behandling av digital information. Den här utvecklingen påverkar också utbudet av samhällsviktiga tjänster.

Det är sannolikt att de samhällsviktiga tjänsterna blir föremål för färre traditionella säkerhetsrisker tack vare ny teknik. Exempelvis kan cirka 90 procent av alla trafikolyckor anses bero på mänskliga misstag. Genom intelligent automatisering av trafiken kommer dock den mänskliga faktorns betydelse för säkerheten att minska. Däremot finns det betydande nya utmaningar när det gäller säkerheten, tillförlitligheten och dataskyddet i digitala system. Sambandet mellan fysisk och digital säkerhet blir allt starkare.

Finländarna har ett starkt förtroende för såväl säkerheten i samhället och de tjänster som är viktiga för samhället som för myndigheternas verksamhet. När samhället digitaliseras är det av avgörande betydelse att medborgarnas och företagens förtroende för digitala verksamhetssätt ökas ytterligare. Man måste förtjäna kundernas förtroende för t.ex. självkörande bilar, nätbanker eller digitala hälsovårdstjänster för att de ska acceptera nya typer av service. En tjänsts tillförlitlighet kan utnyttjas som konkurrensfördel och för vissa tjänster kan tillförlitlighet vara en absolut förutsättning för verksamheten.

Att säkerställa informationssäkerheten är således ett centralt mål för regeringsprogrammets spetsprojekt om att skapa en tillväxtmiljö för digital affärsverksamhet.

Att höja informationssäkerhetsnivån är viktigt med tanke på den övergripande säkerheten i samhället. Störningar i informationssäkerheten för samhällsviktiga tjänster kan äventyra säkerheten och kontinuiteten i dessa tjänster. Exempelvis kan betydande störningar i eldistributionen som har samband med informationssäkerheten i informationssystemen avsevärt påverka utbudet av de flesta tjänsterna i samhället. I och med de omfattande attackerna med utpressningsvirus i början av 2017 har informationssäkerheten i samhällsviktiga tjänster fått allt

större fokus. Sabotageprogram har försvårat verksamheten för t.ex. järnvägssystem, hamnar, sjukhus och energibolag runtom i världen.

Informationssäkerhetsrelaterade störningar kan dessutom ha betydande ekonomiska konsekvenser såväl för samhället som för enskilda medborgare och företag. Av särskild betydelse för enskilda medborgare och företag är störningar som gör att utomstående aktörer såsom cyberbrottslingar kan komma åt deras konfidentiella uppgifter, t.ex. lösenord till olika webbtjänster. Även störningar som gör att tjänster eller de data som lagras i dem inte är tillgängliga för användarna kan vara skadliga. Ekonomiska skador som förorsakas av en störning kan bero på t.ex. egendomsskador, avbrott i ett företags affärsverksamhet eller kostnader som skydd mot skadan medför.

IT-brottslighet, omfattande kränkningar av integritetsskyddet och andra informationssäkerhetsrelaterade störningar bidrar till ett bristande förtroende bland tjänsternas användare. En ökad brist på förtroende skulle ha avsevärda ekonomiska konsekvenser för samhället, eftersom marknadens utveckling kan bromsas upp eller användningen av digitala tjänster kan påverkas negativt på något annat sätt. Exempelvis uppgav hela 88 procent av de 28 000 européer som intervjuades i Europeiska kommissionens Eurobarometer att de har ändrat sitt sätt att använda internet på grund av oro över bristande informationssäkerhet. Ändringar i konsumentbeteendet kan också bromsa upp den generella digitaliseringsutvecklingen och därmed ha en negativ inverkan på möjligheten att uppfylla regeringsprogrammets mål för digitaliseringen.

När det gäller informationssäkerhet finns det många slags risker som kan bero på mycket varierande orsakssamband. En realiserad informationssäkerhetsrisk kan bero på ett oavsiktligt misstag (t.ex. misstag i programmeringen) eller av en uppsåtlig olaglig gärning (t.ex. spridning av utpressningsvirus).

Eftersom informationssäkerhet är förknippad med olika slags risker kan dessa också hanteras med flera olika metoder. Man kan påverka riskhanteringen t.ex. genom att välja rätt miljö, upprätta riskhanteringsplaner, beakta informationssäkerheten i avtalsförhållanden eller ta i bruk särskilda tjänster som ökar förtroendet, t.ex. identifieringstjänster, elektroniska signaturer eller andra datakrypterings- och skyddsmetoder. Man kan dessutom öka förtroendet genom att följa kända standarder och utvärdera och verifiera de åtgärder som standarderna förutsätter (kvalitetsrevision). Det finns också försäkringar mot informationssäkerhetsrisker.

Det viktigaste i hanteringen av informationssäkerhetsrisker är att man delar information. Information om sårbarheter och it-säkerhetsincidenter kan gälla flera aktörer, även inom olika sektorer. Alla gynnas av att aktörerna delar information om informationssäkerhetsrelaterade störningar med varandra. I Finland har Kommunikationsverkets nätverk för informationsdelning och samarbete som bygger på frivilligt informationsutbyte och förtroende mellan aktörerna visat sig vara en framgång som också uppskattas internationellt. Lagstadgade skyldigheter om rapportering av störningar bör inte äventyra denna typ av informationsdelning som bygger på frivillighet och ömsesidig nytta.

Generellt sett förutsätter tillhandahållandet av högkvalitativa och tillförlitliga tjänster som utnyttjar digitala uppgifter att man tar hänsyn till informationssäkerheten som helhet när affärsverksamheten organiseras. Informationssäkerheten måste beaktas under hela den tid som affärsverksamheten pågår. Mot bakgrund av detta betonar slutrapporten av den arbetsgrupp som stöder genomförandet av direktivet om nät- och informationssäkerhet att de skyldigheter som följer av direktivet med avseende på hanteringen av informationssäkerhetsrisker bör kunna införlivas i företagens normala riskhantering.

Ett centralt mål med den här propositionen är att förbättra informationssäkerheten i de samhällsviktiga tjänsterna. Det är nödvändigt för att man på det sätt som beskrivs ovan ska kunna skapa en tillväxtmiljö för digital affärsverksamhet. Dessutom är informationssäkerhet en betydande faktor när det gäller att öka samhällets inre säkerhet.

Även Europeiska unionen har som ett centralt mål att öka förtroendet för unionens digitala inre marknad och därmed effektivisera den inre marknadens funktion och möjliggöra en betydande ekonomisk tillväxt. Som ett led i förbättrandet av den inre marknadens funktion antog Europeiska unionen, *nedan EU*, den 6 juli 2015 Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (nedan kallat *direktivet om nät- och informationssäkerhet*). Direktivet om nät- och informationssäkerhet ska genomföras nationellt före den 9 maj 2018.

Genom direktivet om nät- och informationssäkerhet åläggs medlemsstaterna att upprätta en nationell strategi för säkerhet i nätverks- och informationssystem samt att fastställa myndighetsuppgifter enligt direktivet för att garantera informationssäkerheten och hantera risker inom olika sektorer. Medlemsstaterna åläggs också att samarbeta sinsemellan i nya samarbetsgrupper på EU-nivå för att dela information om säkerhetsöverträdelser samt bästa nationella praxis.

Vidare åläggs medlemsstaterna att inom de sektorer som anges i direktivet om nät- och informationssäkerhet (energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten, digital infrastruktur) identifiera de leverantörer av samhällsviktiga tjänster som är etablerade på deras territorium. Enligt direktivet ska medlemsstaterna ålägga dessa leverantörer av samhällsviktiga tjänster och de leverantörer av digitala tjänster som definieras särskilt i direktivet (internetbaserade marknadsplatser, internetbaserade sökmotorer samt molntjänster) att hantera risker för säkerheten i deras nätverks- och informationssystem och att rapportera incidenter i nätverks- och informationssystemen till den övervakande myndigheten.

Även om lagstiftningen i Finland redan för närvarande tryggar ett relativt högt dataskydd och hög informationssäkerhet behöver lagstiftningen fortfarande utvecklas för att den på bästa möjliga sätt ska bidra till att öka förtroendet för digitala verksamhetssätt och höja säkerheten i de samhällsviktiga tjänsterna med hänsyn till kraven i direktivet om nät- och informationssäkerhet.

Vår gällande lagstiftning utgör en konkurrensfördel för företag jämfört med de stater där man inte har lyckats bygga upp ett förtroende på samma sätt. Detta förslag har utarbetats med tanke på såväl bevarandet av denna konkurrensfördel som målen för spetsprojektet om smidigare författningar i enlighet med regeringsprogrammet.

Dessutom kan den föreslagna lagstiftningen skapa förutsättningar för framväxten av en ny marknad för tillförlitliga digitaliserade tillgångar. Samtidigt bidrar den föreslagna lagstiftningen till att förbättra den offentliga förvaltningens möjligheter att tillhandahålla medborgarna säkrare tjänster i vardagen som tagits fram genom att effektivt utnyttja möjligheterna med digitaliseringen.

2 Nuläge

2.1 Lagstiftning och praxis

2.1.1 Allmänt

I Finland finns lagstiftningen om informationssäkerhet inte samlad i en enda lag, utan bestämmelserna är spridda på ett flertal författningar som gäller såväl den offentliga förvaltningen som tillhandahållandet av olika tjänster. Lagstiftningen om informationssäkerhet innehåller bestämmelser om hur uppgifter av en viss typ ska hanteras på ett informationssäkert sätt. Som exempel kan nämnas bestämmelserna om hantering av personuppgifter och säkerhetsskyddsklassificerade handlingar. Dessutom ingår bestämmelser om informationssäkerhet i lagstiftningen om såväl den offentliga förvaltningens som privata tjänsteleverantörers verksamhet med avseende på t.ex. riskhantering och kontinuitet. Vissa av skyldigheterna i fråga om informationssäkerhet gäller i regel endast den offentliga förvaltningen, medan vissa gäller t.ex. specifika privata tjänsteleverantörer.

Skyldigheter som gäller hanteringen av informationssäkerhetsrisker ingår i de allmänna förvaltningslagarna (lagen om offentlighet i myndigheternas verksamhet (621/1999), personuppgiftslagen (523/1999), i den allmänna lagstiftningen om kvalitetskrav eller säkerhetsrelaterade skyldigheter för tjänsteleverantörer (t.ex. informationssamhällsbalkens (917/2014) bestämmelser om informationssäkerhet i kommunikationstjänster och kommunikationsnät och om trafiksäkerhetsrelaterade skyldigheter), i lagstiftningen om riskhantering i samband med affärsverksamhet (t.ex. om operativ riskhantering i kreditinstitut) och i lagstiftningen om beredskap för störningar (t.ex. vattentjänstverks beredskapsskyldighet). Skyldigheternas innehåll varierar från sektor till sektor. Förutom av lagstiftningen styrs främjandet av säkerheten i samhället, cybersäkerheten och informationssäkerheten av ett flertal strategier som kompletterar varandra. Åtgärder som syftar till att öka informationssäkerheten har samlats i informationssäkerhetsstrategin för Finland, som godkänts i enlighet med regeringens handlingsplan, och i strategin för cybersäkerhet, som godkänts som ett principbeslut av statsrådet. I säkerhetsstrategin för samhället definieras dessutom samhällets vitala funktioner.

2.1.2 Strategierna för informationssäkerhet och cybersäkerhet i Finland

Informationssäkerhetsstrategin för Finland godkändes genom ett beslut av kommunikationsministeriet den 10 mars 2016. Prioriteringar i strategin är säkerställande av konkurrenskraften och exportvillkoren, utvecklingen av EU:s digitala inre marknad samt tryggande av integritetsskyddet och andra grundläggande fri- och rättigheter.

Ramarna för strategiarbetet anges i handlingsplanen för statsminister Juha Sipiläs regeringsprogram och presenteras i strategins inledning. Visionen för strategin har tagits fram för att svara mot de mål och prioriteringar som bygger på dessa utgångspunkter.

Förutom av regeringsprogrammet ha strategins innehåll påverkats av de krav på strategin som anges i direktivet om nät- och informationssäkerhet. Strategin behandlar i enlighet med direktivet om nät- och informationssäkerhet främjandet av den allmänna medvetenheten om informationssäkerhet och kompetensen på området samt betydelsen av forskning och utveckling. Vad gäller riskhantering och identifiering av risker är det centrala budskapet i strategin att aktörerna bör ha möjlighet att utvärdera sina informationssäkerhetsåtgärder på ett riskbaserat sätt, dvs. så att de ställs i relation till hanteringen av övriga risker i affärsverksamheten. Flera av åtgärderna i strategin gäller samarbetet mellan den offentliga och den privata sektorn när det gäller förebyggande, reaktiva och korrigerande åtgärder i samband med nät- och informationssäkerhet.

Strategin är en förlängning av informationssäkerhetsstrategin från 2003 respektive 2008 och cybersäkerhetsstrategin från 2013. I enlighet med dess syfte ligger fokus i strategin särskilt på digital affärsverksamhet och på de strategiska krav som följer av direktivet om nät- och informationssäkerhet.

I informationssäkerhetsstrategin anges också de viktigaste målen för genomförandet av direktivet om nät- och informationssäkerhet. Enligt strategin tryggas i samband med genomförandet av direktivet företagens möjligheter att samordna de nya skyldigheter som gäller hanteringen av informationssäkerhetsrisker till en del av hanteringen av övriga risker för affärsverksamheten.

Strategin för cybersäkerheten i Finland utfärdades 2013 i form av ett principbeslut av statsrådet. Dess syfte är att skapa en gemensam förståelse för cybersäkerhet och stärka den övergripande säkerheten i samhället. I strategin skildras en vision, en handlingsmodell och strategiska riktlinjer för cybersäkerheten. I verkställighetsprogrammet 2017–2020 för strategin för cybersäkerhet som publicerades av Säkerhetskommittén den 20 april 2017 beskrivs åtgärderna för att genomföra strategin närmare. Som en del av programmet genomförs informationssäkerhetsstrategin, som godkänts av kommunikationsministeriet. Därmed kompletterar cybersäkerhetsstrategin och informationssäkerhetsstrategin varandra.

2.1.3 Samhällsviktiga funktioner

I Finland har begreppen kritisk infrastruktur eller samhällsviktiga funktioner egentligen inte definierats på lagstiftningsnivå. Däremot definieras samhällets vitala funktioner i säkerhetsstrategin för samhället.

Statsrådet godkände i oktober 2017 ett principbeslut om en säkerhetsstrategi för samhället. I strategin definieras samhällets vitala funktioner. Enligt strategin är vitala funktioner i det finländska samhället ledningen av staten, internationell och EU-verksamhet, Finlands försvarsförmåga, inre säkerhet, ekonomi, infrastruktur och försörjningsberedskap, befolkningens handlingsförmåga och service samt mental kristålighet.

Enligt strategin ska informations- och kommunikationssystem, digitala tjänster och kunskaper som är nödvändiga för de vitala funktionerna säkras i de lokaler som används av den offentliga förvaltningen och offentliga samfund. En fungerande modell för hantering av informations- och cyberstörningssituationer beaktar de skyldigheter som följer av Europeiska unionens nät- och informationssäkerhetsbestämmelser.

Den 5 december 2013 utfärdade statsrådet dessutom i enlighet med 2 § i lagen om tryggande av försörjningsberedskapen (1390/1992) ett beslut om målen med försörjningsberedskapen (SRb 857/2013). Enligt beslutet är centrala hot som äventyrar samhällets funktionsförmåga störningar i de elektroniska data- och kommunikationssystemen och näten, avbrott i energitillförseln, allvarliga störningar i befolkningens hälsa och funktionsförmåga samt natur- och miljökatastrofer. I beslutet är skyddet av kritisk infrastruktur indelat i följande områden:

1) Systemen för produktion, överföring och distribution av energi

2) System, nät och tjänster för information och kommunikation

3) Tjänster inom finanssektorn

4) Transporter och logistik

5) Vattenförsörjning

6) Byggande och underhåll av infrastrukturen, samt

7) Avfallshanteringen i exceptionella situationer

I beslutet konstateras dessutom att de mest kritiska och centrala samhällsfunktionerna som är beroende av informationsteknik ska identifieras och att de informationssystemlösningar och tjänster som har samband med dem ska tryggas genom arrangemang som tål olika slags allvarliga störningar och undantagsförhållanden.

2.1.4 Kvalitetskrav och riskhanteringsrelaterade krav på leverantörer av tjänster samt rapportering av säkerhetsstörningar till myndigheterna

Såsom konstateras ovan är de samhällsviktiga tjänsterna alltmer beroende av tillförlitligt fungerande datanät och informationssystem. Digital information utnyttjas dessutom i ökande grad för att tillhandahålla tjänster. Inom många samhällsviktiga sektorer finns lagstadgade skyldigheter för leverantörer och användare av tjänster som syftar till att säkerställa verksamhetens kvalitet och säkerhet. Bakom de lagstadgade kvalitetskraven ligger ett värderingsbaserat behov av att hantera en verksamhets betydande samhällskonsekvenser.

Nedan följer en närmare redogörelse för skyldigheterna avseende hantering av säkerhetsrisker enligt den gällande lagstiftningen inom de sektorer som omfattas av direktivet om nät- och informationssäkerhet. Till tillämpningsområdet för direktivet om nät- och informationssäkerhet hör enligt direktivets bilaga II följande sektorer: digital infrastruktur, transporter, energi, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård samt leverans och distribution av dricksvatten. I bilaga II har en del av sektorerna ytterligare delats in i delsektorer. I bilaga II räknas dessutom upp olika typer av enheter inom alla sektorer.

Digital infrastruktur

För sektorn digital infrastruktur anges i bilaga II till direktivet om nät- och informationssäkerhet inga delsektorer, men som typer av enhet nämns internetknutpunkter (Internet exchange point, IXP), leverantörer av DNS-tjänster samt registreringsenheter för toppdomäner. I Finland ingår regleringen om digital infrastruktur huvudsakligen i informationssamhällsbalken. I den föreskrivs om tillhandahållande av elektroniska kommunikationstjänster och informationssamhällets tjänster. I 29 kap. i informationssamhällsbalken föreskrivs om kvalitetskrav på kommunikationsnät och kommunikationstjänster. Enligt lagens 243 § ska allmänna kommunikationsnät och kommunikationstjänster samt kommunikationsnät och kommunikationstjänster som ansluts till dem planeras, byggas och underhållas så att den elektroniska kommunikationens tekniska standard är god och informationssäker. Med informationssäkerhet avses i informationssamhällsbalken administrativa och tekniska åtgärder genom vilka det säkerställs att information är tillgänglig endast för dem som har rätt att använda den, att informationen inte kan ändras av andra än dem som har rätt till detta samt att informationen och informationssystemen kan utnyttjas av dem som har rätt att använda informationen och systemen. Det föreskrivs också att kommunikationsnät och kommunikationstjänster ska tåla sådana normala hot mot informationssäkerheten som kan förväntas, att deras kvalitet och funktionssäkerhet ska gå att följa upp, att mot dem riktade betydande kränkningar av och hot mot informationssäkerheten

ska gå att upptäcka liksom också sådana fel och störningar som avsevärt stör deras funktion samt att ingens dataskydd, informationssäkerhet eller andra rättigheter får äventyras.

Enligt 246 § i informationssamhällsbalken får abonnenter och användare inte till ett allmänt kommunikationsnät ansluta annan radio- och teleterminalutrustning än sådan som är funktionsduglig och som stämmer överens med kraven enligt den lagen. Dessutom ska abonnenterna administrera utrustning och system som ansluts till ett allmänt kommunikationsnät i enlighet med teleföretagets anvisningar så att de inte äventyrar informationssäkerheten i det allmänna kommunikationsnätet och i de allmänna kommunikationstjänsterna.

I X avd. i informationssamhällsbalken föreskrivs om tryggande av kommunikationens och tjänsternas kontinuitet och i dess 33 kap. om hantering av informationssäkerhet och störningar samt anmälan om störningar. I kapitlet föreskrivs om de åtgärder som teleföretag, sammanslutningsabonnenter och leverantörer av mervärdestjänster samt aktörer som handlar för dessas räkning har rätt att vidta i syfte att sörja för informationssäkerheten, om skyldigheten för teleföretag eller andra innehavare av kommunikationsnät eller utrustning att avhjälpa störningar och om skyldigheten för teleföretag och leverantörer av mervärdestjänster att meddela användarna och myndigheterna om störningar.

Enligt 275 § i informationssamhällsbalken ska ett teleföretag utan dröjsmål göra en anmälan till Kommunikationsverket om dess tjänster utsätts för eller hotas av betydande kränkningar av informationssäkerheten eller av någonting annat som gör att en kommunikationstjänst inte fungerar eller väsentligen stör den. Teleföretaget ska också utan obefogat dröjsmål anmäla hur länge störningen eller hotet beräknas pågå, om vilka verkningar störningen eller hotet har, om avhjälpande åtgärder samt om åtgärder för att förhindra att störningen upprepas.

I informationssamhällsbalken avses med teleföretag en aktör som tillhandahåller nättjänster eller kommunikationstjänster för en grupp av användare som inte har avgränsats på förhand, dvs. bedriver allmän televerksamhet. Regleringen av televerksamhet är teknikneutral och verksamheten kan utövas mot vederlag eller utan vederlag. Med allmän televerksamhet avses tillhandahållande av kommunikationstjänster till en grupp av användare som inte har avgränsats på förhand.

Internetknutpunkter erbjuder som minst en teknisk punkt (point of presence) för utbyte av trafik mellan kommunikationsnät som identifierats med ett AS-nummer. Tillhandahållare av internetknutpunkter kan också erbjuda tjänster för avtal om sammankoppling.

Enligt Kommunikationsverkets tolkning är internetknutpunkter sådan allmän televerksamhet som avses i informationssamhällsbalken, åtminstone i den mån de används för att koppla samman allmänna kommunikationsnät. Internetknutpunkter kan användas även av andra teleföretag än de som tillhandahåller allmänna kommunikationsnät, oftast t.ex. innehavare av nätverk för innehållsdistribution (content delivery network, CDN).

Tillhandahållande av DNS-tjänster (Domain Name System, DNS) är enligt den gällande regleringen allmän televerksamhet eller annan verksamhet beroende på om den hänför sig till internetaccesstjänster eller inte. När verksamheten är en del av tillhandahållandet av internetaccesstjänster omfattas den av bestämmelserna och föreskrifterna om allmän televerksamhet. DNS-tjänster tillhandahålls också på andra sätt än som en del av en internetaccesstjänst, t.ex. av registrarer och andra nättjänsteleverantörer. En DNS-tjänst skaffas vanligen inte separat utan som en del av en övrig tjänst.

Bestämmelser om domännamnsregistren för toppdomänerna fi och ax, vilka hör till Finlands lagstiftningsbehörighet, finns i informationssamhällsbalken. Kommunikationsverket förvaltar ett register över domännamn under toppdomänen fi och en databas med teknisk information om domännamn för styrning av internettrafiken (fi-roten). Ålands landskapsregering ansvarar för ax-roten.

I 21 kap. i informationssamhällsbalken finns bestämmelser om domännamn. I lagens 171 § föreskrivs om organisering av domännamnsförvaltningen. Enligt paragrafen har Kommunikationsverket till uppgift att sörja för informationssäkerheten i den domännamnsverksamhet som avser fi-domäner. Enligt lagens 172 § har Kommunikationsverket dessutom rätt att vidta nödvändiga åtgärder för att upptäcka, förhindra och utreda sådana betydande kränkningar av informationssäkerheten som innebär att fi-domännamn utnyttjas och som är riktade mot allmänna kommunikationsnät eller kommunikationstjänster eller mot användare av dem, samt för att inleda förundersökning med anledning av kränkningarna. Myndigheternas verksamhet när det gäller förvaltningen av domännamnsregistret och roten omfattas av informationssäkerhetskraven i såväl informationssamhällsbalken som i lagen om offentlighet i myndigheternas verksamhet (621/1999) och i statsrådets förordning om informationssäkerheten inom statsförvaltningen (681/2010, nedan *informationssäkerhetsförordningen*) som utfärdats med stöd av den lagen.

Energi

Sektorn energi är i bilaga II till direktivet om nät- och informationssäkerhet uppdelad i delsektorerna elektricitet, olja och gas. För dessa delsektorer ingår riskhanteringsrelaterade skyldigheter åtminstone i elmarknadslagen (588/2013) och naturgasmarknadslagen (587/2017), och för delsektorn olja även i lagen om säkerhet vid hantering av farliga kemikalier och explosiva varor (2005/390). Även i kärnenergilagen (990/1987) finns bestämmelser om riskhantering, men kärnenergi hör inte till tillämpningsområdet för direktivet om nät- och informationssäkerhet.

Elektricitet

Stamnätet för eldistribution ska planeras, byggas och upprätthållas så att nätet uppfyller de krav som ställs i Europeiska unionens lagstiftning på nätens driftsäkerhet och tillförlitlighet och de krav i fråga om nätets driftsäkerhet och tillförlitlighet som i elnätstillståndet ställs på den systemansvariga stamnätsinnehavaren.

Enligt elmarknadslagen omfattas elföretag, distributionsnätsinnehavare och överföringsnätsinnehavare av skyldigheten att utveckla nätet (19 §) och att upprätta en beredskapsplan (28 §), och nätinnehavare av skyldigheten att samarbeta vid störningar (29 §). Elföretag och distributionsnätsinnehavare omfattas dessutom av kvalitetskraven i fråga om distributionsnätets funktion (50–52 §).

Enligt 28 § i elmarknadslagen ska nätinnehavaren genom ändamålsenlig planering förbereda sig för störningar i elnätet under normala förhållanden och sådana undantagsförhållanden som avses i beredskapslagen (1552/2011). Nätinnehavaren ska göra upp en beredskapsplan och i behövlig omfattning delta i beredskapsplanering som ska trygga försörjningsberedskapen.

Enligt 59 § i elmarknadslagen ska distributionsnätsinnehavaren informera distributionsnätsanvändarna om eldistributionen i distributionsnätet avbryts i betydande omfattning. Samtidigt ska användarna ges en uppskattning av felets eller avbrottets varaktighet och omfattning.

Naturgas

I naturgasmarknadslagen ingår endast några skyldigheter som gäller hantering av säkerhetsrisker. Den reviderade naturgasmarknadslagen träder i kraft i början av 2018. I lagens 4 kap. finns bestämmelser om nätinnehavarens allmänna skyldigheter. Lagens 27 § innehåller bestämmelser om nätinnehavarens beredskapsplanering. Enligt lagen ska nätinnehavaren genom ändamålsenlig planering förbereda sig för störningar i naturgasnätet under normala förhållanden, för genomförande av ransoneringsåtgärder som föranleds av störningar i tillgången på naturgas i naturgassystemet och för sådana undantagsförhållanden som avses i beredskapslagen. Nätinnehavaren ska göra upp en beredskapsplan och i behövlig omfattning delta i beredskapsplanering som ska trygga försörjningsberedskapen..

Olja

I lagen om säkerhet vid hantering av farliga kemikalier och explosiva varor och i statsrådets förordning om övervakning av hanteringen och upplagringen av farliga kemikalier (685/2015) som utfärdats med stöd av lagen föreskrivs bl.a. om säkerhetskraven vid hantering av farliga kemikalier och explosiva varor, förebyggande av olyckor och om anmälan av olyckor och tillbud till myndigheterna.

Transporter

För sektorn transporter anges i bilaga II till direktivet om nät- och informationssäkerhet fyra delsektorer: lufttransport, järnvägstransport, sjöfart och vägtransport. Den nationella lagstiftningen om hantering av säkerhetsrisker i fråga om transporter bygger ofta på antingen internationella konventioner eller harmoniserad lagstiftning på EU-nivå. Lagstiftningen om transporter är ofta spridd på olika lagar för varje transportslag och regleringen kan bestå av kombinationer av olika internationella konventioner, EU-reglering och nationell reglering.

Lufttransport

Luftfart är internationell verksamhet och regleringen om civil luftfart grundar sig således på gemensamma regler som överenskommits inom ramen för Internationella civila luftfartsorganisationen (ICAO), Europeiska unionens lagstiftning, Europeiska byrån för luftfartssäkerhet (EASA), Europeiska organisationen för luftfartssäkerhet (Eurocontrol) och Europeiska civila luftfartskonferensen (ECAC). Det finns inte mycket nationellt handlingsutrymme när det gäller regleringen av civil luftfart och lufttransporter.

De grundläggande utgångspunkterna i internationella luftfartsavtal har varit säkerhet, effektivitet och lönsamhet. I artikel 37 i konventionen angående internationell luftfart (Chicagokonventionen, FördrS 11/1949) anges som ICAO:s uppgift att godkänna och vid behov ändra internationella standarder, rekommenderade metoder och förfaranden för luftfartens säkerhet, regelbundenhet och effektivitet.

Under de senaste åren har en allt större del av luftfartslagstiftningen i Europeiska unionen utfärdats på förordningsnivå i stället för som direktiv. Därmed har man kunnat säkerställa att lagstiftningen tillämpas så enhetligt som möjligt i Europeiska unionens medlemsstater.

Bestämmelser om de allmänna förutsättningarna för flygverksamhet finns i Europaparlamentets och rådets förordning (EG) nr 216/2008 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av en europeisk byrå för luftfartssäkerhet, nedan

EASA-förordningen, närmare bestämt i artikel 8, bilagorna IV (grundläggande krav på drift av luftfartyg som avses i artikel 8), V a (grundläggande krav för flygplatser) och V b (flygledningstjänster och flygtrafiktjänster samt grundläggande krav för flygledare), och i de genomförandeförordningar som utfärdats med stöd av förordningen. Kommissionen har lagt fram ett förslag till ändring av EASA-förordningen (COM(2015) 613 FINAL). Förslaget behandlas för närvarande inom unionen.

Kraven i EU-lagstiftningen och deras tillämpningsföreskrifter garanterar att medlemsstaterna fullgör de förpliktelser som följer av Chicagokonventionen. I EASA-förordningen, dess bilagor och de tillämpningsföreskrifter som utfärdats med stöd av förordningen föreskrivs om relativt omfattande skyldigheter i fråga om hanteringen av säkerhetsrisker för operatörer, flygplatser, flygledningstjänster, flygtrafiktjänster och flygledningen.

I Europaparlamentets och rådets förordning (EU) nr 376/2014 om rapportering, analys och uppföljning av händelser inom civil luftfart, nedan *händelseförordningen*, föreskrivs om rapportering av händelser som påverkar säkerheten inom luftfarten till den behöriga myndigheten.

I förordningens artikel 4 föreskrivs om rapporteringsskyldigheten om händelser som kan utgöra en betydande risk för flygsäkerheten. Det är obligatoriskt att rapportera händelser som t.ex. rör driften av ett luftfartyg, tekniska förhållanden, underhåll och reparation av ett luftfartyg, flygtrafiktjänster och tillhörande anordningar samt flygplatser och marktjänster.

På nationell nivå kompletteras regleringen av luftfarten av luftfartslagen (864/2014). I luftfartslagen ingår emellertid endast ett fåtal säkerhetsrelaterade krav t.ex. i fråga om upprätthållande av luftvärdighet (33 och 34 §), intyg över godkännande av trafikflygplats (83 §), tillhandahållande av marktjänster (93 §) och beredskap för undantagsförhållanden och störningar (160 §).

Enligt 118 § i luftfartslagen ska Trafiksäkerhetsverket underrättas om olyckor och allvarliga tillbud inom civil luftfart. Enligt 125 § 1 mom. tillämpas EU:s händelseförordning på alla luftfartyg i Finland. Enligt 2 mom. i samma paragraf ska händelser som inbegriper ett luftfartyg som är registrerat i Finland eller som används av en organisation som är etablerad i Finland i enlighet med händelseförordningen rapporteras även om de har inträffat utomlands. Trafiksäkerhetsverket ansvarar för och driver ett rapporteringssystem enligt händelseförordningen till vilket obligatorisk och frivillig information om händelser rapporteras (126 §).

Trafiksäkerhetsverket har utfärdat en luftfartsanvisning (GEN TI-4) med närmare förfaranden och anvisningar för rapportering, analys och uppföljning av luftfartsolyckor, allvarliga tillbud och händelser inom luftfart.

Järnvägstransport

Allmänna bestämmelser om järnvägssäkerhet för myndigheter och aktörer har utfärdats på EU-nivå. I författningarna anges krav som gäller bl.a. säkerhetsstyrningssystemet, anmälningsskyldigheten och tillsynen. De viktigaste författningarna på EU-nivå är Europaparlamentets och rådets direktiv (EU) 2016/798 om järnvägssäkerhet, kommissionens förordning (EU) nr 1078/2012 om en gemensam säkerhetsmetod för övervakning som ska tillämpas av järnvägsföretag och infrastrukturförvaltare efter erhållande av säkerhetsintyg eller säkerhetstillstånd, samt av enheter som ansvarar för underhåll samt kommissionens förordning (EU) nr 1077/2012 om en gemensam säkerhetsmetod för nationella säkerhetsmyndigheters tillsyn efter utfärdande av ett säkerhetsintyg eller säkerhetstillstånd. Nationella bestämmelser om järnvägs-

säkerhet finns i järnvägslagen (304/2011), en förordning av statsrådet och Trafiksäkerhetsverkets föreskrifter.

I 6 kap. i järnvägslagen föreskrivs om järnvägssystemets säkerhet. Enligt lagens 39 § ska järnvägssystemets säkerhetsnivå upprätthållas och utvecklas enligt de möjligheter som Europeiska unionens lagstiftning samt den tekniska och vetenskapliga utvecklingen inom branschen ger. Enligt paragrafen ansvarar bannätsförvaltarna och järnvägsoperatörerna för en trygg användning av järnvägssystemet och för hantering av de risker som användningen medför. Enligt lagens 40 § ska järnvägsoperatörerna och bannätsförvaltarna ha säkerhetsstyrningssystem som överensstämmer med bestämmelserna och föreskrifterna om järnvägssäkerhet. Enligt 75 § kan Trafiksäkerhetsverket i syfte att säkerställa järnvägssystemets säkerhet och tekniska funktion utfärda närmare föreskrifter om bl.a. säkerhetsstyrningssystem och beredskap för olyckor och olyckstillbud. Trafiksäkerhetsverket har utfärdat en föreskrift om järnvägsoperatörernas och bannätsförvaltarnas säkerhetsstyrningssystem.

Enligt 79 § i järnvägslagen ska järnvägsoperatörer och bannätsförvaltare ha tillräcklig beredskap för faror och olyckor som hotar järnvägarna. Vidare ska innehavare av säkerhetsintyg eller säkerhetstillstånd enligt 81 § förbereda sig för undantagsförhållanden och se till att verksamheten fortgår så störningsfritt som möjligt också under sådana undantagsförhållanden som avses i beredskapslagen och vid därmed jämförbara störningar under normala förhållanden.

I 81 a § föreskrivs om åtgärder som bannätsförvaltare ska vidta vid störningar inom järnvägssystemet på grund av tekniska missöden eller olyckor för att återställa situationen till det normala.

Enligt 82 § i järnvägslagen ska järnvägsoperatörer och bannätsförvaltare underrätta Trafiksäkerhetsverket om olyckor och olyckstillbud som de fått kännedom om. Enligt lagen är dessa uppgifter sekretessbelagda.

Närmare bestämmelser om anmälningsskyldigheten finns i statsrådets förordning om järnvägssystemets säkerhet och driftskompatibilitet (372/2011).

Sjöfart

Den internationella regleringen av sjöfarten bygger på Internationella sjöfartsorganisationens (IMO) konventioner. De viktigaste internationella konventionerna är 1974 års internationella konvention om säkerheten för människoliv till sjöss (SOLAS-konventionen, International Convention for the Safety of Life at Sea [FördrS 11/1981]), som gäller sjösäkerhet, och protokollet av år 1978 till 1973 års internationella konvention till förhindrande av förorening från fartyg (MARPOL-konventionen, International Convention for the Prevention of Pollution from Ships), som gäller miljöskydd.

Skyldigheter som gäller bolagens (rederiernas) riskhantering finns i den internationella säkerhetsorganisationskoden (International Safety Management Code, ISM-koden) som grundar sig på SOLAS-konventionen. Inom EU har koden genomförts genom Europaparlamentets och rådets förordning (EG) nr 336/2006 om genomförande av Internationella säkerhetsorganisationskoden i gemenskapen. Även systemet för rapportering av händelser ingår i kraven i ISM-koden. Rapportering av avvikande händelser är motiverad eftersom man kan minska risken för allvarliga olyckor genom att analysera olyckstillbud och mindre olyckor samt genom att vidta föregripande korrigeringsåtgärder.

Bestämmelser om skyldigheten att rapportera olyckor inom kommersiell sjöfart till Trafiksäkerhetsverket finns i sjölagen (674/1994). Enligt lagen ska en anmälan om sjöolycka göras i de fall som avses i 18 kap. 6 och 8 § i sjölagen. I 15 § i samma kapitel föreskrivs om rapportering om olyckor och tillbud. Enligt 20 § i lagen om tillsyn över fartygssäkerheten (370/1995) ska anmälan om brott mot en bestämmelse eller föreskrift som gäller fartygssäkerheten om möjligt göras skriftligen till tillsynsmyndigheten.

Sjötrafikinformationstjänster

I lagen om fartygstrafikservice (623/2005) föreskrivs om vissa sjöfartsrelaterade trafikledningsuppgifter, för vilka Trafikverket enligt lagen är ansvarig myndighet (VTS-myndighet) (2 § 1 och 4 punkten). Enligt lagens 19 § ska VTS-myndigheten föra en drifthandbok i vilken anges de uppgifter och åtgärder som anknyter till upprätthållandet av VTS-centralens verksamhet och tekniska system samt beredskapen för upprätthållandet av fartygstrafikservicen i undantagssituationer. I drifthandboken ska det, i fråga om skyldigheterna enligt lotsningslagen, anges förfaringssätt, meddelandepraxis och former för samarbetet med Trafiksäkerhetsverket.

I 20 a § föreskrivs om systemet för hantering av information inom sjöfarten och de krav som ställs på det. När det gäller systemet för hantering av information meddelar Trafikverket enligt paragrafen närmare föreskrifter om anmälningsförfarande, struktur, datainnehåll och åtkomsträttigheter, om utlämnande av uppgifter till myndigheter och om utbytet av information med andra medlemsstater och med Europeiska unionens system för hantering av information inom sjöfarten (centralsystemet SafeSeaNet).

VTS-myndigheten är skyldig att till vederbörande sjöfarts-, sjöräddnings-, miljö-, territorialövervaknings-, polis- eller tullmyndighet samt vederbörande hamninnehavare rapportera om alla sådana väsentliga omständigheter som har samband med ett visst fartygs eller de på fartyget ombordvarandes säkerhet, sjöräddningen, miljöskyddet eller territorialövervakningen eller tullkontrollen och som myndigheten har observerat eller som har anmälts till myndigheten (18 §). Vidare ska befälhavaren på finskt vattenområde underrätta VTS-myndigheten om varje kritiskt läge eller olycka som påverkar fartygets säkerhet eller äventyrar sjösäkerheten samt om varje situation som kan leda till förorening av farvatten eller stränder och om alla till sjöss kringdrivande föroreningsbälten, containrar och förpackningar (23 §).

Hamnar

Säkerhetsskyldigheter som gäller hamnar finns i ISPS-koden (International Ship and Port Facility Security Code) som syftar till att öka säkerheten ombord på fartyg och i hamnar. Koden har utarbetats av Internationella sjöfartsorganisationen IMO. ISPS-koden återfinns också som bilaga till den internationella SOLAS-konventionen (kapitel XI-2 ”Special measures to enhance maritime security”) och den har genomförts i EU genom Europaparlamentets och rådets förordning (EG) nr 715/2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar, nedan *förordningen om sjöfartsskydd*. Nationella bestämmelser om skyddsåtgärder som ska iakttas i hamnar finns i lagen om sjöfartskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet. Behörig myndighet enligt lagen är Trafiksäkerhetsverket, vars uppgift är att övervaka efterlevnaden av förordningen om sjöfartsskydd och bestämmelserna i den lagen. Gränsbevakningsväsendet, polisen och tullverket har till uppgift att informera Trafiksäkerhetsverket om brister som de observerat i efterlevnaden av förordningen om sjöfartsskydd och bestämmelserna i den lagen. Trafiksäkerhetsverket ska utan dröjsmål vidta åtgärder

för att rätta till bristerna. I lagen föreskrivs också om särskilda uppgifter för Trafiksäkerhetsverket, gränsbevakningsväsendet, polisen och tullverket (4–7 §).

Vägtransport

Reglerna för vägtrafikanter, dvs. trafikreglerna, ingår i vägtrafiklagen (267/1981).

Olika aktörer ansvarar för funktioner med anknytning till styrningen av vägtrafiken. Enligt landsvägslagen är Trafikverket och närings-, trafik- och miljöcentralerna väghållningsmyndigheter. De kan bl.a. tillfälligt förbjuda eller begränsa trafiken (35 §) och bevilja tillstånd för placering av olika slags anläggningar, anordningar och kablar på vägområdet (42 och 42 a §). Enligt vägtrafiklagen har Trafikverket också befogenheter att bl.a. sätta upp trafikanordningar och reglera trafiken i plankorsningar mellan väg och järnväg samt att tillfälligt stänga av en väg i enlighet med 49 § i vägtrafikförordningen. Kommunerna har också uppgifter i anslutning till trafikledning. Exempelvis ska kommunen enligt 51 § i vägtrafiklagen uppsätta trafikanordningar på gator, byggnadsplanevägar, torg och andra trafikområden av motsvarande slag.

Intelligenta trafiksystem i vägtrafiken

Automatstyrda fordon utgör en del av det intelligenta trafiksystemet. I intelligenta trafiksystem använder de automatstyrda fordonen sådan information som de själva producerar när de färdas i trafiken. Informationen om miljön insamlas med hjälp av sensorer, radaranordningar och kameror. Därutöver använder fordonen sig av den omfattande information som via nätet förmedlas till dem om den övriga trafikmiljön, övriga fordon i trafiken, vägmiljön och trafikanordningarna samt om kommersiella tjänster.

Målet för Europaparlamentets och rådets direktiv 2010/40/EU om ett ramverk för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportslag (nedan *ITS-direktivet*) är att påskynda ett samordnat införande och användning av intelligenta transportsystem i vägtrafiken överallt i Europa. ITS-direktivet ska tillämpas på alla intelligenta transportsystem inom vägtransportområdet samt på vägtransporternas gränssnitt mot andra transportslag. I ITS-direktivet betonas den europeiska arkitekturen för intelligenta transporter, genom vilken man kan främja även multimodalt biljettutställande, det vill säga biljettutställande som kopplar ihop olika transportslag. ITS-direktivet innehåller en bestämmelse med stöd av vilken Europeiska kommissionen har getts befogenhet att anta delegerade akter i fråga om sådana tekniska specifikationer som behövs för att kompatibiliteten ska kunna garanteras liksom interoperabiliteten och kontinuiteten vad gäller införande och operativ användning av ITS inom hela unionen. ITS-direktivet är till sin karaktär en ramlag, vars innehåll grundar sig på de delegerade akter som utfärdats med stöd av artiklarna 6 och 7. Dessa är kommissionens förordningar, varför de är direkt tillämplig rätt och endast i begränsad utsträckning kräver nationell reglering.

I Finland har ITS-direktivet införlivats i lagen om transportservice (320/2017). Bestämmelser om införande av intelligenta transportsystem finns i III avd. 2 kap. 6 § i lagen. I 2 mom. anges Trafiksäkerhetsverket som den behöriga myndighet som har i uppgift att bedöma överensstämmelse med kraven. Av kommissionens förordningar som utfärdats med stöd av ITS-direktivet förutsätts för närvarande att en aktör som bedömer överensstämmelsen med kraven utses i artikel 4 i förordning nr 305/2013 avseende harmoniserat tillhandahållande av interoperabelt EU-omfattande eCall respektive artikel 9 i förordning nr 886/2013 vad gäller data och förfaranden för kostnadsfritt tillhandahållande, när så är möjligt, av ett minimum av vägsäkerhetsrelaterad universell trafikinformation för användare.

Kommissionens delegerade förordning (EU) nr 886/2013 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller data och förfaranden för kostnadsfritt tillhandahållande, när så är möjligt, av ett minimum av vägsäkerhetsrelaterad universell trafikinformation för användare ska tillämpas på tillhandahållande av ett minimum av vägsäkerhetsrelaterade universella trafikinformationstjänster på det transeuropeiska vägnätet. Med ett minimum av vägsäkerhetsrelaterad universell trafikinformationstjänst avses en trafikinformationstjänst med ett överenskommet minsta vägsäkerhetsrelaterat innehåll som kan nås med minimal ansträngning av ett maximalt antal slutanvändare.

Bankverksamhet och finansmarknadsinfrastruktur

I bilaga II till direktivet om nät- och informationssäkerhet delas bankverksamhet och finansmarknadsinfrastruktur inte in i delsektorer. Som typer av enheter inom bankverksamhet anges kreditinstitut och inom finansmarknadsinfrastruktur operatörer av handelsplatser och centrala motparter enligt definitionen i unionens direktiv 2014/65/EU.

Regleringen och tillsynen av banksektorn och sektorn för finansmarknadsinfrastrukturer har i hög grad harmoniserats på unionsnivå. Detta kommer till uttryck vid tillämpningen av unionens primärrätt och sekundärrätt och standarder som utvecklats tillsammans med de europeiska tillsynsmyndigheterna. Inom bankunionen säkerställs tillämpningen och tillsynen av dessa krav genom den gemensamma tillsynsmekanismen. Inom tillsynspraxis på andra områden inom regleringen av finanssektorn säkerställer Europeiska systemet för finansiell tillsyn också en hög grad av enhetlighet och konvergens. Inom banksektorn är det viktigaste målet med riskhanteringen att trygga en tillräcklig kapitalbas i förhållande till risktagandet och riskhanteringssystemen. Riskerna för verksamheten kan delas in i exempelvis kreditrisker, operativa risker, marknadsrisker och likviditetsförvaltning.

Operativ risk utgör en viktig del av reglering och tillsyn inom banksektorn och sektorn för finansmarknadsinfrastrukturer. Med operativa risker avses t.ex. risker som beror på otillräckliga eller misslyckade interna processer eller på personal, system eller externa faktorer. Hantering av operativa risker omfattar all verksamhet, inbegripet nätverks- och informationssystems säkerhet, integritet och motståndskraft.

Kreditinstitut

I 5 kap. 10 och 11 § i kreditinstitutslagen (610/2014) föreskrivs om utläggning på entreprenad av verksamhet som är viktig för kreditinstitut och om förutsättningarna för utläggning. Bestämmelser om skyldigheten att vidta förberedelser finns i 16 §. De allmänna kraven avseende riskhanteringssystem anges i 9 kap. 2 § i kreditinstitutslagen. Kraven avseende hanteringen av operativa risker anges i kapitlets 16 §, enligt vilken kreditinstitutet ska ha adekvata, trygga och funktionssäkra betalningsdatasystem, värdepappersdatasystem och andra datasystem. I paragrafen föreskrivs dessutom om beredskapsplanering.

Enligt lagens 24 § får Finansinspektionen meddela närmare föreskrifter om operativa risker som avses i 16 §. Finansinspektionen har utfärdat föreskrifter om hantering av operativa risker i företag under tillsyn inom finanssektorn (Föreskrifter och anvisningar 8/2014) och om utläggning (Föreskrifter och anvisningar 1/2012). I kapitel 6 i föreskriften om hantering av operativa risker i företag under tillsyn inom finanssektorn finns bestämmelser om informationssäkerheten i informationssystem.

Enligt 18 § 2 mom. i lagen om Finansinspektionen får Finansinspektionen meddela föreskrifter om vilka uppgifter om tillsynsobjekts ekonomiska ställning, ägare, interna kontroll och riskhantering, förvaltnings- och kontrollorgan, tjänstemän och verksamhetsställen som regelbundet ska lämnas till Finansinspektionen.I Finansinspektionens föreskrift om hanteringen av operativa risker bestäms närmare om rapportering av störningar i informationssystemen till Finansinspektionen.

Reglerade marknader, multilaterala handelsplattformar, organiserade handelsplattformar samt börser

När det gäller bedrivande av börsverksamhet finns bestämmelser om riskhanteringskrav och rapportering av störningar i 3 kap. i den föreslagna lagen om handel med finansiella instrument som ingår i regeringens proposition (RP 151/2017 rd) av den 26 oktober 2017.. I lagens 1 § finns bestämmelser om krav som gäller organisering av verksamheten på en reglerad marknad. Enligt lagen ska börsen säkerställa att dess system och förfaranden också i störningssituationer tryggar tillförlitligheten och kontinuiteten i handelssystemet. Börsen ska kunna säkerställa att dess handelssystem är motståndskraftiga, har tillräcklig kapacitet för att hantera toppbelastning i fråga om order- och meddelandevolymer och kan säkerställa ordnad handel under svåra förhållanden på marknaden. Börsen ska regelbundet testa handelssystemets funktion med belastningstest för att uppfylla de krav som beskrivs ovan. Enligt 2 § ska börsen utan obefogat dröjsmål underrätta Finansinspektionen om systemavbrott som rör ett finansiellt instrument.

Hälso- och sjukvårdssektorn

För hälso- och sjukvårdssektorn anges i bilaga II till direktivet om nät- och informationssäkerhet delsektorn hälso- och sjukvårdsmiljöer (inklusive sjukhus och privata kliniker). I Finland tillämpas hälso- och sjukvårdslagen (1326/2010) på tillhandahållandet av den hälso- och sjukvård som kommunerna enligt folkhälsolagen (66/1972) och lagen om specialiserad sjukvård (1062/1989) är skyldiga att ordna och på innehållet i denna hälso- och sjukvård. I lagens 8 § föreskrivs om kvalitetskrav på verksamheten inom hälso- och sjukvården och om patientsäkerhet. Enligt lagen ska verksamheten inom hälso- och sjukvården vara högkvalitativ och säker och bedrivas på behörigt sätt. Därtill ska verksamhetsenheterna inom hälso- och sjukvården göra upp en plan för kvalitetsledningen och för hur patientsäkerheten tillgodoses. Genom förordning av social- och hälsovårdsministeriet föreskrivs det närmare om de frågor som det ska överenskommas om i planen.

Syftet med lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) är att främja datasäker elektronisk behandling av klientuppgifter inom social- och hälsovården. Genom lagen genomförs ett enhetligt elektroniskt behandlings- och arkiveringssystem för patientuppgifter för effektiv produktion av hälso- och sjukvårdstjänster så att patientsäkerheten beaktas samt för främjande av patientens möjligheter att få information. Lagen tillämpas när tillhandahållare av offentliga och privata social- och hälsovårdstjänster ordnar eller genomför social- eller hälsovård.

I lagens 5 a kap. föreskrivs om väsentliga krav på informationssystem som används för behandling av klient- och patientuppgifter inom social- eller hälsovården. I 5 b kap. föreskrivs dessutom om skyldigheten för den som tillhandahåller tjänster att upprätta en plan för egenkontroll som innehåller riskhanteringsåtgärder.

Enligt 19 § i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården ska den som tillhandahåller tjänster underrätta Tillstånds- och tillsynsverket för social- och hälsovården om betydande avvikelser när det gäller tillgodoseendet av de väsentliga kraven på ett informationssystem, om avvikelsen kan innebära en betydande risk för patientsäkerheten, informationssäkerheten eller dataskyddet.

Syftet med lagen om produkter och utrustning för hälso- och sjukvård (629/2010) är att upprätthålla och främja säkerheten hos produkter och utrustning för hälso- och sjukvård och i användningen av dem. Lagen tillämpas på konstruktion och tillverkning av produkter och utrustning för hälso- och sjukvård och tillbehör till dem samt på hopsättning av vårdset och modulsammansatta produkter. Dessutom tillämpas lagen på utsläppande på marknaden av ovan nämnda produkter och sterilisering av dem i sådant syfte samt på ibruktagande, installation, underhåll, yrkesmässig användning, marknadsföring och distribution av produkterna.

Enligt definitionen i lagens 5 § avses med produkter för hälso- och sjukvård instrument, apparater, anordningar, programvara, material och andra produkter eller annan utrustning som används separat eller i kombinationer och som tillverkaren avsett för användning på människor vid

a) påvisande, förebyggande, övervakning, behandling eller lindring av sjukdom,

b) påvisande, övervakning, behandling, lindring eller kompensation av en skada eller en funktionsnedsättning,

c) undersökning, ersättning eller ändring av anatomin eller av en fysiologisk process, eller

d) befruktningskontroll.

I lagens 2 kap. finns bestämmelser om krav som gäller produkter för hälso- och sjukvård. Enligt 6 § 3 mom. ska en produkt vara lämpad för avsett ändamål och uppnå den funktion och de prestanda som den uppgetts ha, om den används för avsett ändamål. Användningen av en produkt på avsett sätt får inte i onödan äventyra patientens, användarens eller andra personers hälsa eller säkerhet.

I lagens 17 § föreskrivs om verksamhetsutövarens skyldigheter. Enligt paragrafen ska verksamhetsutövaren iaktta de upplysningar och anvisningar om transport, förvaring, installation, underhåll och annan behandling av produkter för hälso- och sjukvård som tillverkaren har lämnat.

Enligt lagens 25 § ska en yrkesmässig användare lämna rapport till Tillstånds- och tillsynsverket för social- och hälsovården och tillverkaren eller den auktoriserade representanten om varje sådan riskhändelse som inträffat vid användningen av en produkt för hälso- och sjukvård och som har lett till eller kunde ha lett till att patientens, användarens eller någon annans hälsa äventyrades och som beror på bl.a. produktens egenskaper, en avvikelse i produktens prestanda, brister i märkningen av produkten eller en felaktig bruksanvisning för produkten.

Tillstånds- och tillsynsverket för social- och hälsovården kan meddela föreskrifter om hur riskhändelser ska rapporteras och vilka uppgifter som ska lämnas om dessa. Tillstånds- och tillsynsverket för social- och hälsovården har meddelat en föreskrift om anmälan från yrkesmässiga användare om riskhändelser i samband med produkter och utrustning för hälso- och sjukvård.

Leverans och distribution av dricksvatten

För sektorn leverans och distribution av dricksvatten anges inga delsektorer i bilaga II till direktivet om nät- och informationssäkerhet. Syftet med den finländska lagen om vattentjänster (119/2001) är att trygga vattentjänster som, till skäliga kostnader, ger tillgång till tillräckligt med hygieniskt och även i övrigt oklanderligt hushållsvatten samt sådan avloppshantering som är ändamålsenlig med avseende på hälso- och miljöskyddet. Enligt 14 § i lagen om vattentjänster ska vattentjänstverket se till att det hushållsvatten som verket levererar uppfyller kvalitetskraven i hälsoskyddslagen (763/1994). Enligt 15 § ska ett vattentjänstverk hålla sig informerat om dels de risker som hänför sig till kvantiteten av eller kvaliteten på det råvatten som det använder, dels i vilket skick verkets anordningar är. I detta syfte ska verket kontrollera kvantiteten av och kvaliteten på det råvatten som det använder, anordningarnas skick och mängden läckvatten i verkets vattenlednings- och avloppsnät. Enligt 15 a § svarar ett vattentjänstverk för att vattentjänsterna för de till verkets ledningsnät anslutna fastigheterna är tillgängliga i störningssituationer. Med störningssituationer avses enligt regeringens proposition om ändring av lagen om vattentjänster (RP 218/2013 rd) alla störningssituationer som försvårar eller riskerar produktionen av vattentjänster, utom sedvanliga driftstörningar. Exempel på störningssituationer är sådana skador på anordningar som har omfattande följder, andra allvarliga störningar i anordningar, system eller tjänster som hänför sig till vatten och avlopp, störningar som drabbar tekniska system samt störningssituationer som drabbar vattenförsörjning samt energi- och informationssystem. Störningar kan orsakas av bl.a. naturkatastrofer, extremt väder, lokala eller landsomfattande olyckor, ofog och brott. Med störningssituationer avses störningssituationer i såväl normala förhållanden som undantagsförhållanden.

För att trygga tjänsterna ska verket enligt 15 a § i lagen om vattentjänster samarbeta med andra vattentjänstverk som är anslutna till samma ledningsnät samt med kommunen, de kommunala tillsynsmyndigheterna, räddningsmyndigheterna, avtalsparterna och kunderna. Vattentjänstverket ska utarbeta och uppdatera en plan för beredskap för störningssituationer och vidta de åtgärder som behövs enligt planen. Verket ska ge in planen till tillsyns myndigheten, räddningsmyndigheten och kommunen.

De kvalitetskrav som gäller hushållsvattnets säkerhet grundar sig på Europaparlamentets och rådets direktiv 98/83/EG om kvaliteten på dricksvatten. Nationella bestämmelser om kvalitetskraven för hushållsvatten och om övervakning av kvaliteten finns i 17 § respektive 20 § i hälsoskyddslagen.

Social- och hälsovårdsministeriet har i enlighet med 17 § och 20 § i hälsoskyddslagen utfärdat en förordning om kvalitetskrav på och kontrollundersökning av hushållsvatten (1352/2015).I förordningen finns bestämmelser om kvalitetskrav, kvalitetsmål och desinfektion i fråga om hushållsvatten, det förfarande som ska iakttas om hushållsvattnet inte uppfyller kvalitetskraven eller kvalitetsmålen, regelbunden övervakning av hushållsvatten, innehållet i ansökan som gäller verksamheten för en anläggning som levererar hushållsvatten, bedömning och kontroll av risker som påverkar hushållsvattnets hälsokvalitet, begränsning av strålningsexponering som föranleds av radioaktiva ämnen i hushållsvatten och om innehållet i och utarbetandet av planer för beredskap med tanke på störningssituationer.

2.1.5 Försörjningsberedskap och förberedelse för undantagsförhållanden

Med försörjningsberedskap avses enligt lagen om tryggande av försörjningsberedskapen de ekonomiska funktioner och därtill hörande tekniska system som tryggar befolkningens utkomst, landets näringsliv och landets försvar med tanke på undantagsförhållanden och allvar-

liga störningar som kan jämföras med undantagsförhållanden. Sektorer som är kritiska med tanke på Finlands försörjningsberedskap är enligt beslutet om försörjningsberedskapen, utöver informationssamhällssektorn, energiförsörjningen, finansförsörjningen, transportlogistiken, hälso- och sjukvården, livsmedelsförsörjningen och den kritiska industriproduktionen. Alla dessa områden är i olika avseende beroende av att informations- och kommunikationssystemen fungerar störningsfritt.

Beredskapslagen som trädde i kraft 2012 ska tillämpas i samband med allvarliga samhälleliga kriser. I beredskapslagen föreskrivs om de finländska myndigheternas interna befogenheter under undantagsförhållanden för att garantera befolkningens säkerhet och livsbetingelser samt ett fungerande samhälle. Som undantagsförhållanden enligt 3 § i beredskapslagen betraktas 1) ett mot Finland riktat väpnat angrepp eller annat så allvarligt angrepp att det kan jämställas med ett väpnat angrepp och förhållandena omedelbart efter angreppet, 2) ett mot Finland riktat avsevärt hot om väpnat angrepp eller om annat så allvarligt angrepp att det kan jämställas med ett väpnat angrepp, om befogenheter enligt beredskapslagen måste tas i bruk omedelbart för att avvärja verkningarna av hotet, 3) sådana synnerligen allvarliga händelser eller hot mot befolkningens försörjning eller mot grunderna för landets näringsliv som innebär en väsentlig risk för samhällets vitala funktioner, 4) en synnerligen allvarlig storolycka och förhållandena omedelbart efter den, samt 5) en pandemi som till sina verkningar kan jämföras med en synnerligen allvarlig storolycka. Enligt lagens 13 § leds och övervakas förberedelserna av statsrådet samt av varje ministerium inom sitt ansvarsområde. Varje ministerium samordnar förberedelserna inom sitt eget ansvarsområde.

Bestämmelser om förberedelser för undantagsförhållanden och störningar under normala förhållanden finns också i flera sektorspecifika speciallagar.

2.1.6.Övrig lagstiftning av betydelse för informationssäkerheten i samhällsviktiga tjänster

Förutom i den sektorspecifika speciallagstiftningen finns det också i den övriga lagstiftningen sådana bestämmelser om hantering av informationssäkerhetsrisker och rapportering av störningar i informationssäkerheten som påverkar tillhandahållandet av tjänster. Exempelvis gäller säkerhetsskyldigheterna i samband med behandlingen av personuppgifter i princip leverantörer av tjänster inom alla sektorer. När tjänster tillhandahålls av myndigheter omfattas de dessutom av kraven på informationssäkerhet enligt informationssäkerhetsförordningen, som utfärdats med stöd av offentlighetslagen.

Säkerhetsrelaterade skyldigheter vid behandling av personuppgifter

Syftet med personuppgiftslagen (523/1999) är att genomföra de grundläggande fri- och rättigheter som tryggar skydd för privatlivet samt övriga grundläggande fri- och rättigheter som tryggar skyddet för den personliga integriteten vid behandling av personuppgifter samt att främja utvecklandet och iakttagandet av god informationshantering. Personuppgiftslagen är en allmän lag vars bestämmelser ska iakttas vid behandling av personuppgifter, om inte annat anges någon annanstans i lag. Bestämmelserna i personuppgiftslagen ska därmed i regel iakttas också när personuppgifter behandlas i samband med tillhandahållandet av samhällsviktiga tjänster.

I lagens 7 kap. finns bestämmelser om informationssäkerhet vid hanteringen av personuppgifter och förvaringen av dem. Enligt lagens 32 § ska den registeransvarige genomföra de tekniska och organisatoriska åtgärder som behövs för att skydda personuppgifterna mot obehörig åtkomst och mot förstöring, ändring, utlämnande och översändande som sker av misstag eller i

strid med lag eller mot annan olaglig behandling. Vid genomförandet av åtgärderna ska hänsyn tas till de tillgängliga tekniska möjligheterna, kostnaderna som orsakas av åtgärderna, uppgifternas art, mängd och ålder samt vilken betydelse behandlingen av uppgifterna har med avseende på integritetsskyddet.

Genom personuppgiftslagen har Finland genomfört Europaparlamentets och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter nedan *personuppgiftsdirektivet*. Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG, nedan *den allmänna dataskyddsförordningen*,, ersätter personuppgiftsdirektivet fr.o.m. den 25 maj 2018. Förordningen är direkt tillämplig i Finland. I artikel 32 i den allmänna dataskyddsförordningen föreskrivs om säkerhet i samband med behandlingen av personuppgifter. I artikel 33 i förordningen föreskrivs om skyldigheten att anmäla personuppgiftsincidenter till tillsynsmyndigheten. Enligt artikeln ska den registeransvarige utan onödigt dröjsmål anmäla personuppgiftsincidenten till tillsynsmyndigheten. I artikeln finns också bestämmelser om minimikrav för innehållet i anmälan och om skyldigheten att dokumentera personuppgiftsincidenter.

Säkerhetsrelaterade skyldigheter som gäller myndigheternas informationshantering

Bestämmelser om myndighetshandlingars offentlighet och om behandlingen av en begäran om att få ta del av en handling samt om allmänna skyldigheter i anknytning till god informationshantering finns i offentlighetslagen.

I informationssäkerhetsförordningen, som utfärdats med stöd av bemyndigandet att utfärda förordningar i offentlighetslagens 36 §, föreskrivs om de allmänna kraven på informationssäkerhet i fråga om hanteringen av handlingar hos en statsförvaltningsmyndighet samt om grunderna för klassificeringen av handlingar och de krav på informationssäkerhet som motsvarar klassificeringen och som ska iakttas vid hanteringen av handlingar. Om samhällsviktiga tjänster tillhandahålls av en myndighet ska den iaktta skyldigheterna enligt informationssäkerhetsförordningen.

Säkerhetsrelaterade skyldigheter som gäller elektronisk identifiering

I lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) (autentiseringslagen) finns bestämmelser om stark autentisering och tillhandahållande av identifieringstjänster till tjänsteleverantörer, till allmänheten och till andra leverantörer av identifieringstjänster. I lagens 8 § föreskrivs om krav på system för elektronisk identifiering, inklusive informationssäkerhetskrav. Enligt 13 § ska leverantören av identifieringstjänster ansvara för skyddet av uppgifterna enligt 32 § i personuppgiftslagen och för en tillräcklig informationssäkerhet i fråga om sina tjänster. Enligt 16 § ska en leverantör av identifieringstjänster trots sekretessbestämmelserna utan ogrundat dröjsmål anmäla betydande hot och störningar som riktas mot tjänsternas funktion, informationssäkerheten eller användningen av en elektronisk identitet till de tjänsternas förlitande parter, till innehavarna av identifieringsverktyg, till övriga avtalsparter i förtroendenätet och till Kommunikationsverket. Kommunikationsverket får för anmälarens räkning på teknisk väg förmedla uppgifterna mellan parterna i förtroendenätet trots vad som föreskrivs i offentlighetslagen. Enligt 29 § ska en leverantör av identifieringstjänster regelbundet låta ett sådant bedömningsorgan som nämns i lagen bedöma om identifieringstjänsten uppfyller kraven på interoperabilitet, informationssäkerhet, dataskydd och annan tillförlitlighet enligt autentiseringslagen.

2.1.7 Myndighetstillsyn och lägesbilden

I Finland utövas tillsyn över de kvalitets- och säkerhetsrelaterade skyldigheter som beskrivs ovan av olika myndigheter beroende på verksamhetens art. Efterlevnaden av skyldigheterna i samband med verksamhetens säkerhet eller informationssäkerhet övervakas av flera myndigheter. Exempelvis övervakar Kommunikationsverket efterlevnaden av säkerhets- och informationssäkerhetsrelaterade skyldigheter som gäller televerksamhet medan Finansinspektionen övervakar dessa skyldigheter i fråga om kreditinstituts verksamhet och Tillstånds- och tillsynsverket för social- och hälsovården övervakar skyldigheterna i fråga om behandlingen av klientuppgifter inom sjukvården. Kommunikationsverket har inga egentliga allmänna tillsynsuppgifter som gäller informationssäkerheten i samhällsviktiga tjänster, även om verket generellt stöder och hjälper medborgarna och företagen att sörja för informationssäkerheten, t.ex. genom att tillhandahålla en nationell kontaktpunkt för hantering av it-säkerhetsincidenter, CERT (Computer Emergency Response Team), vars uppgift är att utreda kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster och mervärdestjänster, samla information om sådana incidenter och informera om informationssäkerhet på ett allmänt plan. Kommunikationsverket upprätthåller också en allmän lägesbild av informationssäkerheten. Kommunikationsverket får en betydande del av sin information om incidenter och sårbarheter genom frivilliga anmälningar från näringsidkare.

Den allmänna lägesbilden av säkerheten på statsnivå sammanställs av Statsrådets lägescentral, som också utnyttjar information från tillsynsmyndigheterna inom olika sektorer och från andra myndigheter.

Statsrådets lägescentral

Enligt 12 § 7 punkten i reglementet för statsrådet (262/2003), som utfärdats med stöd av lagen om statsrådet (175/2003), hör statsrådets gemensamma lägesbild, beredskap och säkerhet samt den allmänna samordningen av hanteringen av störningssituationer till statsrådets kanslis ansvarsområde.

Statsrådets lägescentral, som är verksam dygnet runt, inrättades i september 2007 för att statsledningen och myndigheterna kontinuerligt ska få information. Lagen om statsrådets lägescentral trädde i kraft i juli 2017. I lagen föreskrivs om statsrådets lägescentrals uppgifter och om informationsutbyte mellan myndigheterna. Enligt lagens 1 § ska statsrådets lägescentral för att stödja republikens presidents och statsrådets beslutsfattande och verksamhet samla in och analysera information om säkerhetssituationen och sådana störningar och hot om störningar som äventyrar samhällets vitala funktioner, sköta och koordinera förvaltningsövergripande uppgifter som hänför sig till upprätthållande, sammanställande, samordnande och förmedlande av en beskrivning av lägesbilden samt sprida den samordnade informationen till republikens president, statsrådet och andra myndigheter. I lagen föreskrivs dessutom om skyldigheten för ministerierna samt ämbetsverken och inrättningarna inom deras förvaltningsområde att informera statsrådets lägescentral om olyckor, farosituationer, exceptionella händelser och andra motsvarande störningar samt om rätten för lägescentralen att få information och om utlämnande av sekretessbelagd information.

Statsrådets lägescentral tar fram information om säkerhetsincidenter i realtid och sammanställer en lägesbild utifrån uppgifter från de behöriga myndigheterna. Lägescentralen sammanför uppgifterna från de olika myndigheterna och från öppna källor och lämnar utifrån dessa en rapport till statsledningen och de olika myndigheterna.

Kommunikationsverket

Kommunikationsverkets uppgifter och särskilda uppgifter definieras i informationssamhällsbalken och i vissa andra lagar. Enligt informationssamhällsbalken hör till Kommunikationsverkets särskilda uppgifter att bl.a. främja den elektroniska kommunikationens funktion, störningsfrihet och trygghet, samla in information om kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster och mervärdestjänster samt om fel och störningar i kommunikationsnät och kommunikationstjänster, informera om frågor som gäller informationssäkerhet samt om kommunikationsnäts och kommunikationstjänsters funktion samt utreda kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster och mervärdestjänster.

Trafiksäkerhetsverket

Enligt lagen om Trafiksäkerhetsverket svarar Trafiksäkerhetsverket för reglerings- och övervakningsuppgifter inom trafiksystemet och främjar trafiksäkerheten. Trafiksäkerhetsverket upprätthåller också en lägesbild av trafiksystemet, som beskriver säkerhetsläget inom Finlands trafiksystem.

I luftfartslagen föreskrivs om Trafiksäkerhetsverkets uppgifter som gäller efterlevnaden av säkerhetskraven inom luftfarten och luftfartsverksamhetens överensstämmelse med kraven. Utöver vad som i luftfartslagen föreskrivs om Trafiksäkerhetsverkets uppgifter, är Trafiksäkerhetsverket behörig nationell myndighet enligt bl.a. EASA-förordningen och händelseförordningen. Trafiksäkerhetsverket är också den luftfartsmyndighet som avses i Finlands internationella luftfartsavtal och om vilken det föreskrivs i luftfartslagens 173 §. Händelser som kan äventyra flygsäkerheten ska rapporteras till Trafiksäkerhetsverket i enlighet med gällande lagstiftning.

Trafiksäkerhetsverket ska övervaka den allmänna sjösäkerheten och att gott sjömanskap iakttas. Enligt lagen om fartygstrafikservice övervakar Trafiksäkerhetsverket och VTS-myndigheten iakttagandet av de bestämmelser och föreskrifter som utfärdats med stöd av den. I 18 § i lagen om fartygstrafikservice föreskrivs om VTS-myndighetens skyldighet att till Trafiksäkerhetsverket rapportera om vissa väsentliga omständigheter som har samband med sjösäkerheten och att meddela verket sina iakttagelser av hur lotsningslagen (940/2003) följs. Trafiksäkerhetsverket är även behörig myndighet enligt lagen om sjöfartskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet.

Trafiksäkerhetsverket övervakar att järnvägssystemets säkerhetskrav iakttas samt överensstämmelsen hos järnvägsoperatörernas och bannätsförvaltarnas säkerhetsstyrningssystem. Övervakningen regleras av Europeiska kommissionens förordning (EU) nr 1077/2012 om nationella säkerhetsmyndigheters tillsyn efter utfärdande av ett säkerhetsintyg eller säkerhetstillstånd.

Tillstånds- och tillsynsverket för social- och hälsovården

Enligt 38 § i lagen om produkter och utrustning för hälso- och sjukvård har Tillstånds- och tillsynsverket för social- och hälsovården till uppgift att övervaka och främja säkerheten hos produkter för hälso- och sjukvård och i användningen av dem samt produkternas överensstämmelse med kraven.

För skötseln av denna uppgift för Tillstånds- och tillsynsverket för social- och hälsovården ett register över riskhändelser. Tillstånds- och tillsynsverket för social- och hälsovården ska utvärdera de rapporter om riskhändelser som lämnats in av de anmälningsskyldiga och vidta åtgärder som behövs för tryggandet av hälsa och säkerhet.

Tillstånds- och tillsynsverket för social- och hälsovården ska dessutom övervaka att de väsentliga kraven på informationssystem avsedda för behandling av klient- och patientuppgifter inom social- och hälsovården uppfylls. Enligt lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården har Tillstånds- och tillsynsverket för social- och hälsovården till uppgift att övervaka och främja informationssystemens överensstämmelse med kraven. Enligt lagen ska tillhandahållare av social- eller hälsovårdstjänster underrätta Tillstånds- och tillsynsverket för social- och hälsovården om betydande avvikelser när det gäller tillgodoseendet av de väsentliga kraven på ett informationssystem om avvikelsen kan innebära en betydande risk för patientsäkerheten, informationssäkerheten eller dataskyddet.

Institutet för hälsa och välfärd

Institutet för hälsa och välfärd lyder under social- och hälsovårdsministeriet, och dess syfte enligt lagen om Institutet för hälsa och välfärd är att främja befolkningens välfärd och hälsa, förebygga sjukdomar och sociala problem och utveckla social- och hälsovården och dess service. Enligt 2 § 4 b-punkten i ovan nämnda lag ska institutet svara för planeringen, styrningen och uppföljningen av den elektroniska behandlingen av klientuppgifter inom social- och hälsovården och informationsadministrationen i anslutning därtill samt av användningen och realiseringen av riksomfattande informationssystemtjänster. Enligt 19 a § i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården får Institutet för hälsa och välfärd vid behov meddela närmare föreskrifter om innehållet i de väsentliga kraven på informationssystem som används för behandling av klient- och patientuppgifter inom socialvården.

Finansinspektionen

Enligt lagen om Finansinspektionen är syftet med Finansinspektionens verksamhet är att kreditinstituten, försäkringsanstalterna, pensionsanstalterna och andra tillsynsobjekt bedriver en stabil verksamhet som är en förutsättning för finansmarknadens stabilitet, att de försäkrade förmånerna tryggas och att det allmänna förtroendet för finansmarknadens funktionssätt upprätthålls. Finansinspektionen ska övervaka att finansmarknadsaktörerna iakttar de på dem tillämpliga bestämmelserna om finansmarknaden och med stöd av dem utfärdade föreskrifter, villkoren i sina verksamhetstillstånd och stadgarna som gäller deras verksamhet. Enligt lagen om Finansinspektionen får Finansinspektionen meddela föreskrifter om vilka uppgifter om tillsynsobjekts ekonomiska ställning, ägare, interna kontroll och riskhantering, förvaltnings- och kontrollorgan, tjänstemän och verksamhetsställen som regelbundet ska lämnas till Finansinspektionen.

Energimyndigheten

Bestämmelser om Energimyndighetens uppgifter finns i lagen om tillsyn över el- och naturgasmarknaden (590/2013). Enligt 2 § tillämpas lagen på skötseln av de tillsyns- och kontrolluppgifter som Energimyndigheten ska sköta enligt bl.a. elmarknadslagen och naturgasmarknadslagen samt i de bestämmelser och myndighetsföreskrifter som utfärdats med stöd av lagarna.

Bestämmelser om Energimyndighetens behörighet i tillsynsärenden finns i lagens 9 §. Om någon bryter mot eller försummar de förpliktelser som föreskrivs i den nationella lagstiftning eller EU-lagstiftning som avses i 2 § i den lagen, ska Energimyndigheten förplikta vederbörande att rätta till sin överträdelse eller försummelse. I beslutet kan det bestämmas hur överträdelsen eller försummelsen ska rättas.

I lagens 30 § föreskrivs om Energimyndighetens rätt att få uppgifter och utföra granskningar. Enligt lagen ska näringsidkare som bedriver verksamhet som är underkastad tillsyn lämna Energimyndigheten den information och de handlingar som behövs för skötseln av de tillsynsuppgifter som avses i den lagen. Utöver detta ska Energimyndigheten ges de statistikuppgifter och andra uppgifter som behövs för skötseln av andra uppgifter som avses i denna lag eller för uppfyllande av internationella avtalsförpliktelser.

Leverans och distribution av dricksvatten

Den allmänna styrningen och uppföljningen av verkställigheten av lagen om vattentjänster hör till jord- och skogsbruksministeriets uppgifter. Tillsynsmyndigheter enligt lagen om vattentjänster är närings-, trafik- och miljöcentralen, den kommunala hälsoskyddsmyndigheten och miljövårdsmyndigheten, var och en av dem inom sitt ansvarsområde.

Närings-, trafik- och miljöcentralen och den kommunala miljövårdsmyndigheten övervakar att vattentjänstverket fullgör sin lagstadgade samarbets- och planeringsskyldighet för att förbereda sig för störningssituationer. Vattentjänstverken är dock enligt lagen om vattentjänster inte skyldiga att underrätta myndigheten om avbrott i distributionen eller om andra störningar.

Enligt 4 § i hälsoskyddslagen utövas den högsta ledningen och styrningen av den allmänna planeringen av och tillsynen över hälsoskyddet av social- och hälsovårdsministeriet. Social- och hälsovårdsministeriet ansvarar för kvalitetskraven på och kontrollen av hushållsvattnet i Finland. Den förordning av social- och hälsovårdsministeriet som utfärdats med stöd av hälsoskyddslagen föreskriver om kvalitetskrav på och kontrollundersökning av hushållsvatten.

Husållsvattnets kvalitet kontrolleras regelbundet. Syftet med kontrollen är att övervaka vattnets kvalitet så att man kan säkerställa att det vatten som distribueras inte ger sanitära olägenheter. Om hushållsvattnet inte uppfyller kvalitetskraven och vattnet kan ge sanitära olägenheter, ska den kommunala hälsoskyddsmyndigheten tillsammans med anläggningen som levererar vattnet utreda orsaken till störningen i vattnets kvalitet. Hälsoskyddsmyndigheten ska förelägga vattenleverantören att så snart som möjligt rätta förhållandet och ge vattenförbrukarna anvisningar om hur sanitära olägenheter kan förebyggas.

I lagstiftningen delas anläggningarna in i stora och små anläggningar. Stora anläggningar är sådana som levererar minst 10 kubikmeter vatten om dagen eller motsvarande minst 50 personers behov. Uppgifterna om vattenkvaliteten hos de allra största leverantörerna av hushållsvatten – de som levererar minst 1 000 kubikmeter vatten om dagen eller för behoven hos minst 5 000 förbrukare – sänds till Europeiska kommissionen.

Den kommunala hälsoskyddsmyndigheten ska sända resultaten från dessa kontrollundersökningar till regionförvaltningsverket. Institutet för hälsa och välfärd upprättar årligen en rapport om vattenkvaliteten i dessa anläggningar. Tillstånds- och tillsynsverket för social- och hälsovården publicerar rapporten på sin webbplats.

Tillstånds- och tillsynsverket för social- och hälsovården styr de kommunala hälsoskyddsmyndigheterna i frågor som gäller tillsynen över och kvaliteten på hushållsvatten. Därtill styr och övervakar regionförvaltningsverket hälsoskyddet inom sitt verksamhetsområde.

2.1.8 Samarbete och utbyte av information mellan myndigheter

Direktivet om nät- och informationssäkerhet förpliktar de myndigheter som ansvarar för informationssäkerheten att samarbeta i den mån som behövs för att övervaka efterlevnaden av skyldigheterna enligt direktivet. I Finland finns bestämmelser om de allmänna grunderna för samarbetet mellan myndigheter i förvaltningslagen. Enligt förvaltningslagens 10 § ska varje myndighet inom ramen för sin behörighet och i den omfattning ärendet kräver på andra myndigheters begäran bistå dessa i skötsel av en förvaltningsuppgift, och även i övrigt sträva efter att främja samarbetet mellan myndigheterna. Om handräckning mellan myndigheterna föreskrivs särskilt.

I offentlighetslagen föreskrivs om myndigheters utlämnande av sekretessbelagda uppgifter. Enligt lagens 26 § får en myndighet lämna ut uppgifter ur en sekretessbelagd myndighetshandling om i lag särskilt tagits in uttryckliga bestämmelser om rätten att lämna ut eller att få uppgifter, eller när sekretessplikt har föreskrivits till skydd för någons intressen och denne samtycker till att uppgifter lämnas ut.

Enligt samma paragraf får en myndighet lämna ut uppgifter ur en sekretessbelagd handling för handräckning som myndigheten lämnar samt för något annat uppdrag som myndigheten givit eller någon uppgift som i övrigt handhas för myndighetens räkning om detta är nödvändigt för att uppdraget eller uppgiften ska kunna skötas.Myndigheten ska på förhand försäkra sig om att uppgifterna kommer att hemlighållas och skyddas på behörigt sätt. Bestämmelser om myndigheters rätt eller skyldighet att samarbeta och utbyta sekretessbelagda uppgifter med andra myndigheter finns i speciallagar som reglerar flera olika myndigheters verksamhet.

2.1.9 Påföljder

Enligt grundlagen ska all utövning av offentlig makt bygga på lag. I lag ska således föreskrivas om myndigheternas befogenheter och om påföljderna för överträdelse av lagen. Ett flertal lagar innehåller bestämmelser om tillsynsmyndighetens rätt att ge den som bryter mot lagen en anmärkning eller ålägga den att rätta till felet, eller påföra andra administrativa sanktioner såsom påföljdsavgifter. Exempelvis föreskrivs i 330 § i informationssamhällsbalken att tillsynsmyndigheterna när de sköter uppgifter enligt den lagen kan meddela den som bryter mot lagen eller mot bestämmelser som utfärdats eller föreskrifter, beslut eller tillståndsvillkor som meddelats med stöd av lagen en anmärkning samt ålägga denne att inom en skälig tid avhjälpa sitt fel eller sin försummelse. Enligt järnvägslagens 86 § kan Trafiksäkerhetsverket ge ett järnvägsföretag eller en annan järnvägsoperatör eller bannätsförvaltare som avses i lagen en anmärkning eller varning, om denne handlar i strid med järnvägslagen eller de bestämmelser som utfärdats med stöd av den. Vidare får Trafiksäkerhetsverket enligt 87 § ålägga en järnvägsoperatör eller en bannätsförvaltare att avhjälpa fel eller försummelser samt ålägga denne förpliktelser eller förbjuda en åtgärd, om denne trots en anmärkning eller varning handlar i strid med järnvägslagen. Enligt VI avd. 1 kap. 4 § i lagen om transportservice kan Trafiksäkerhetsverket ålägga den som bryter mot den lagen, mot EU-förordningar som gäller verksamhet som omfattas av lagen eller mot bestämmelser som utfärdats eller föreskrifter som meddelats med stöd av lagen, att rätta till felet eller försummelsen. I 19 § i lagen om sjöfartskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet föreskrivs att om hamninnehavaren inte iakttar bestämmelserna i förordningen om sjöfartsskydd eller be-

stämmelserna i den lagen ska Trafiksäkerhetsverket, efter att ha hört den som gjort sig skyldig till försummelsen, meddela behövliga anvisningar och förelägganden för avhjälpande av bristerna eller missförhållandena. Verket får fastställa en frist för avhjälpandet av bristerna eller missförhållandena. Enligt 33 § i lagen om Finansinspektionen kan Finansinspektionen förbjuda verkställigheten av tillsynsobjekts och andra finansmarknadsaktörers beslut och av åtgärder som tillsynsobjekt och andra finansmarknadsaktörer har planerat eller ålägga tillsynsobjekt och andra finansmarknadsaktörer att upphöra med ett förfarande, om beslutet, åtgärden eller förfarandet strider mot de bestämmelser om finansmarknaden som tillämpas på tillsynsobjektet eller finansmarknadsaktören eller mot föreskrifter som har meddelats med stöd av dem, mot tillståndsvillkor eller mot stadgar som gäller tillsynsobjektets eller finansmarknadsaktörens verksamhet. Enligt 29 § i lagen om vattentjänster kan tillsynsmyndigheten förbjuda den som bryter mot lagen eller med stöd av den utfärdade bestämmelser att fortsätta eller upprepa överträdelsen eller ålägga denne att fullgöra sin skyldighet.

Enligt 67 § i förvaltningslagen kan en myndighet förena ett förbud, ett åläggande eller ett krav som den har meddelat med vite, hot om tvångsutförande eller hot om avbrytande eller med någon annan administrativ påföljd enligt vad som föreskrivs särskilt. Bestämmelser om sådana administrativa påföljder finns i 332 § i informationssamhällsbalken, 151 § i luftfartslagen, 87 § i järnvägslagen, VI avd. 1 kap. 4 § i lagen om transportservice, 31 § i lagen om tillsyn över el- och naturgasmarknaden, 33 a § i lagen om Finansinspektionen, 30 § i lagen om vattentjänster, 20 f § i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården samt i 52 § i lagen om produkter och utrustning för hälso- och sjukvård.

2.2 Den internationella utvecklingen samt lagstiftningen i utlandet och i EU

2.2.1 EU-lagstiftningen

År 2013 lade kommissionen fram meddelandet *EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd* (JOIN(2013) 1 final). Ett av syftena med strategin är att utveckla informationssamhällets stabilitet genom att förbättra beredskapen, samarbetet, kunnandet och informationsutbytet när det gäller nät- och informationssäkerheten. Som ett led i genomförandet av strategin lade kommissionen samtidigt fram ett förslag till direktiv om nät- och informationssäkerhet.

Direktivets övergripande syfte är att öka nivån på skyddet mot incidenter, risker och hot avseende nät- och informationssäkerheten. Syftet är att uppnå en hög säkerhetsnivå för nät- och informationssystem i EU genom att förbättra beredskapen på nationell nivå, öka samarbetet på EU-nivå och föreskriva riskhanterings- och rapporteringsskyldigheter för leverantörer av samhällsviktiga tjänster och vissa leverantörer av digitala tjänster.

Genom direktivet åläggs medlemsstaterna att upprätta en nationell strategi för säkerhet i nätverks- och informationssystem samt att fastställa myndighetsuppgifter enligt direktivet för att garantera informationssäkerheten och hantera risker inom olika sektorer. Medlemsstaterna åläggs också att samarbeta sinsemellan i nya samarbetsgrupper på EU-nivå för att dela information om säkerhetsöverträdelser samt bästa nationella praxis.

Definition av myndighetsuppgifter

Enligt direktivet om nät- och informationssäkerhet ska medlemsstaterna upprätta en nationell strategi för säkerhet i nätverks- och informationssystem samt att fastställa myndighetsuppgifter enligt direktivet för att garantera informationssäkerheten och hantera risker inom olika sek-

torer. Medlemsstaterna åläggs också att samarbeta sinsemellan i nya samarbetsgrupper på EU-nivå för att dela information om säkerhetsöverträdelser samt bästa nationella praxis.

Behörig myndighet

Enligt artikel 8.1 i direktivet ska varje medlemsstat utse en eller flera nationella behöriga myndigheter för säkerhet i nätverks- och informationssystem, åtminstone för de sektorer som avses i bilaga II och de tjänster som avses i bilaga III. Medlemsstaterna får tilldela en eller flera befintliga myndigheter denna roll. Enligt artikel 8.2 ska de behöriga myndigheterna övervaka tillämpningen av direktivet på nationell nivå. Enligt artiklarna 15 och 17 ska de behöriga myndigheterna ha de befogenheter och medel de behöver för att bedöma huruvida leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster uppfyller sina skyldigheter enligt direktivet och effekterna därav på säkerheten i nätverks- och informationssystem. Enligt artiklarna 14 och 16 ska incidenter som definieras i direktivet rapporteras till behöriga myndigheter eller till CSIRT-enheter (Computer security incident response teams).

Gemensamma nationella kontaktpunkter

Varje medlemsstat ska utöver behöriga myndigheter utse en gemensam nationell kontaktpunkt för säkerhet i nätverks- och informationssystem. Medlemsstaterna får tilldela en befintlig myndighet denna roll. Den gemensamma kontaktpunkten ska utöva en sambandsfunktion för att säkerställa gränsöverskridande samarbete mellan medlemsstaternas myndigheter. Den gemensamma kontaktpunkten bör inte direkt ta emot några rapporter om incidenter, såvida den inte också fungerar som behörig myndighet eller som en CSIRT-enhet. En behörig myndighet eller en CSIRT-enhet bör dock kunna ge den gemensamma kontaktpunkten i uppgift att vidarebefordra incidentrapporter till de gemensamma kontaktpunkterna i andra berörda medlemsstater. Den gemensamma kontaktpunkten ska förse samarbetsgruppen med en sammanfattande rapport som innehåller uppgifter om antalet mottagna incidentrapporter samt information om de rapporterade incidenternas art, såsom vilka typer av säkerhetsöverträdelser det rör sig om eller hur allvarliga eller långvariga de varit.

CSIRT-enheter

Varje medlemsstat ska enligt direktivet utse en eller flera CSIRT-enheter. Enheten ska uppfylla kraven i bilaga I till direktivet. CSIRT-enheterna ansvarar för hanteringen av incidenter och risker. CSIRT-enheters uppgifter ska omfatta minst följande:

- övervakning av incidenter på nationell nivå,
- tillhandahållande av tidiga varningar, larm, meddelanden och informationsspridning till relevanta aktörer om risker och incidenter,
- åtgärder till följd av incidenter,
- tillhandahållande av dynamisk risk- och incidentanalys och situationsmedvetenhet,
- deltagande i CSIRT-nätverket.

Vidare ska CSIRT-enheter bygga upp samarbetsrelationer med den privata sektorn och främja antagandet och användningen av gemensam eller standardiserad praxis för förfaranden för hantering av incidenter och risker samt för klassificeringssystem.

EU-samarbete

I direktivet om nät- och informationssäkerhet föreskrivs att det på EU-nivå inrättas en samarbetsgrupp för att stödja och underlätta strategiskt samarbete och utbyte av information mellan medlemsstaterna och skapa förtroende och tillit, och i syfte att uppnå en hög gemensam nivå på säkerheten i nätverks- och informationssystem i unionen. Samarbetsgruppen består av företrädare för medlemsstaterna, kommissionen och Europeiska unionens byrå för nät- och informationssäkerhet (Enisa, European Union Agency for Network and Information Security). Samarbetsgruppens uppgifter anges i direktivet.

I direktivet föreskrivs också om inrättandet av ett nätverk på EU-nivå för nationella CSIRT-enheter. CSIRT-nätverket består av företrädare för medlemsstaternas CSIRT-enheter och incidenthanteringsorganisationen för EU:s institutioner och byråer (CERT-EU). Nätverkets uppgifter anges i direktivet.

Identifiering av leverantörer av samhällsviktiga tjänster

Enligt direktivet om nät- och informationssäkerhet ska medlemsstaterna för varje sektor som avses i direktivet identifiera de leverantörer av samhällsviktiga tjänster som är etablerade på deras territorium. De sektorer som ingår i direktivets tillämpningsområde definieras i bilaga II till direktivet.

BILAGA II

TYPER AV ENHETER ENLIGT ARTIKEL 4.4

Sektor	Delsektor	Typ av enhet
1. Energi	a) Elektricitet	- Elföretag enligt definitionen i artikel 2.35 i Europaparlamentets och rådets direktiv 2009/72/EG som bedriver ”leverans eller handel” enligt definitionen i artikel 2.19 i det direktivet - Systemansvariga för distributionssystemet enligt definitionen i artikel 2.6 i direktiv 2009/72/EG - Systemansvariga för överföringssystemet enligt definitionen i artikel 2.4 i direktiv 2009/72/EG

	b) Olja	- Operatörer av oljeledningar - Operatörer av oljeproduktion, raffinaderier, bearbetningsanläggningar, lagring och överföring
	c) Gas	- Gashandelsföretag eller gashandlare enligt definitionen i artikel 2.8 i Europaparlamentets och rådets direktiv 2009/73/EG - Systemansvariga för distributionssystemet enligt definitionen i artikel 2.6 i direktiv 2009/73/EG - Systemansvariga för överföringssystemet enligt definitionen i artikel 2.4 i direktiv 2009/73/EG - Systemansvariga för lagringssystemet enligt definitionen i artikel 2.10 i direktiv 2009/73/EG - Systemansvariga för en LNG-anläggning enligt definitionen i artikel 2.12 i direktiv 2009/73/EG - Naturgasföretag enligt definitionen i artikel 2.1 i direktiv 2009/73/EG - Operatörer av raffinaderier och bearbetningsanläggningar för naturgas

2. Transporter	a) Lufttransport	- Lufttrafikföretag enligt definitionen i artikel 3.4 i Europaparlamentets och rådets förordning (EG) nr 300/2008 - Flygplatsens ledningsenheter enligt definitionen i artikel 2.2 i Europaparlamentets och rådets direktiv 2009/12/EG, flygplatser enligt definitionen i artikel 2.1 i det direktivet, inbegripet de huvudflygplatser som förtecknas i avsnitt 2 i bilaga II till Europaparlamentets och rådets förordning (EU) nr 1315/2013, och enheter som driver kringliggande installationer vid flygplatser - Operatörer inom trafikstyrning och trafikledning som tillhandahåller flygkontrolltjänst enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EG) nr 549/2004
	b) Järnvägstransport	- Infrastrukturförvaltare enligt definitionen i artikel 3.2 i Europaparlamentets och rådets direktiv 2012/34/EU - Järnvägsföretag enligt definitionen i artikel 3.1 i direktiv 2012/34/EU, inbegripet tjänsteleverantörer enligt definitionen i artikel 3.12 i direktiv 2012/34/EU

	c) Sjöfart	- Transportföretag som bedriver persontrafik och godstrafik på inre vattenvägar, till havs och längs kuster, enligt definitionerna för sjötransport i bilaga I till Europaparlamentets och rådets förordning (EG) nr 725/2004, exklusive de enskilda fartyg som drivs av dessa företag - Ledningsenheter för hamnar enligt definitionen i artikel 3.1 i Europaparlamentets och rådets direktiv 2005/65/EG, inbegripet deras hamnanläggningar enligt definitionen i artikel 2.11 i förordning (EG) nr 725/2004, och enheter som sköter anläggningar och utrustning i hamnar - Operatörer av sjötrafikinformationstjänster enligt definitionen i artikel 3 o i Europaparlamentets och rådets direktiv 2002/59/EG
	d) Vägtransport	- Vägmyndigheter enligt definitionen i artikel 2.12 i kommissionens delegerade förordning (EU) 2015/962 med ansvar för trafikstyrning och trafikledning - Operatörer av intelligenta transportsystem enligt definitionen i artikel 4.1 i Europaparlamentets och rådets direktiv 2010/40/EU
3. Bankverksamhet		- Kreditinstitut enligt definitionen i artikel 4.1 i Europaparlamentets och rådets förordning (EU) nr 575/2013

4. Finansmarknadsinfrastruktur		- Operatörer av handelsplatser enligt definitionen i artikel 4.24 i Europaparlamentets och rådets direktiv 2014/65/EU - Centrala motparter enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 648/2012
5. Hälso- och sjukvårdssektorn	Hälso- och sjukvårdsmiljöer (inklusive sjukhus och privata kliniker)	- Vårdgivare enligt definitionen i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU
6. Leverans och distribution av dricksvatten		- Leverantörer och distributörer av dricksvatten enligt definitionen i artikel 2.1 a i rådets direktiv 98/83/EG, dock exklusive distributörer för vilka distribution av dricksvatten endast utgör en del av deras allmänna verksamhet, som består i distribution av andra förnödenheter och varor som inte anses utgöra samhällsviktiga tjänster
7. Digital infrastruktur		- Internetknutpunkter - Leverantörer av DNS-tjänster - Registreringsenheter för toppdomäner

I direktivet anges kriterierna för identifiering av leverantörer av samhällsviktiga tjänster. Enligt direktivet ska leverantörer av samhällsviktiga tjänster tillhandahålla tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet. Denna tjänst ska vara beroende av nätverks- och informationssystem. Ett ytterligare kriterium är att en incident i tjänsten skulle medföra en betydande störning vid tillhandahållandet av tjänsten.

Enligt direktivet ska medlemsstaterna upprätta en förteckning över samhällsviktiga tjänster. Förteckningen över tjänster ska omfatta alla de tjänster som tillhandahålls på en viss medlemsstats territorium och som uppfyller kraven enligt direktivet.

Enligt direktivet kan identifieringen av leverantörer av samhällsviktiga tjänster göras genom att exempelvis anta en förteckning över alla leverantörer av samhällsviktiga tjänster eller genom att anta åtgärder som gör det möjligt att fastställa dessa leverantörer.

När medlemsstaterna bedömer om en incident skulle medföra en betydande störning, vilket är ett av kriterierna för identifiering av leverantörer av samhällsviktiga tjänster, ska de beakta de faktorer som anges i direktivet, t.ex. det antal användare som är beroende av tjänsten och aktörens marknadsandel. Även sektorsspecifika faktorer ska beaktas vid fastställandet av huruvida en incident skulle medföra en betydande störning vid tillhandahållandet av en samhällsviktig tjänst. I direktivets ingress ges följande exempel på detta:

”När det gäller energileverantörer kan sådana faktorer omfatta mängden eller andelen producerad nationell el, för oljeleverantörer mängden olja per dag, för lufttransport, inbegripet flygplatser och lufttrafikföretag, järnvägstransport och kusthamnar andelen nationell trafikmängd och antalet passagerare eller lastningar per år, för bankverksamhet eller finansmarknadsinfrastrukturer deras betydelse för systemet på grundval av samlade tillgångar eller förhållandet mellan dessa tillgångar och BNP, för hälso- och sjukvårdssektorn antalet patienter som leverantören vårdar per år, för produktion, bearbetning och leverans av vatten, volym, antal och typer av användare, inbegripet t.ex. sjukhus, offentlig sektor, organisationer och personer) samt förekomsten av alternativa vattenkällor för samma geografiska område.”

Medlemsstaterna ska regelbundet (minst vartannat år) se över och vid behov uppdatera förteckningen över identifierade leverantörer av samhällsviktiga tjänster. Enligt direktivet krävs det vid identifiering av leverantörer av samhällsviktiga tjänster att leverantören utför en faktisk och reell verksamhet med hjälp av en stabil struktur för att den ska anses vara etablerad i en medlemsstat. Om aktörerna tillhandahåller både samhällsviktiga och andra typer av tjänster ska de omfattas av kraven i direktivet endast när det gäller tjänster som anses vara samhällsviktiga.

Skyldigheter som gäller informationssäkerhet och rapportering

Enligt direktivet ska medlemsstaterna ålägga leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster att hantera risker för säkerheten i deras nätverks- och informationssystem och att rapportera incidenter till behöriga myndigheter eller till CSIRT-enheter.

Skyldigheter för leverantörer av samhällsviktiga tjänster med avseende på hantering av säkerhetsrisker

Enligt direktivet ska medlemsstaterna ålägga leverantörer av samhällsviktiga tjänster att hantera risker för säkerheten i nätverks- och informationssystem samt att rapportera betydande informationssäkerhetsincidenter till myndigheterna. Med säkerhet i nätverks- och informationssystem avses dessa systems förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade eller överförda eller behandlade uppgifter eller hos de besläktade tjänster som erbjuds genom eller är tillgängliga via dessa nätverks- och informationssystem.

De riskhanteringsåtgärder som leverantörer av tjänster åläggs bör inte innebära krav på att någon särskild kommersiell informations- och kommunikationsteknisk produkt utformas, utvecklas eller tillverkas på ett visst sätt.

Leverantörer av tjänster bör säkerställa säkerheten i de nätverks- och informationssystem som de använder. Det rör sig framför allt om privata nätverks- och informationssystem som anting-

en förvaltas av deras interna it-personal eller vilkas säkerhet har lagts ut på entreprenad. Säkerhets- och rapporteringskraven bör gälla oavsett om leverantörerna sköter underhållet av sina nätverks- och informationssystem internt eller lägger ut uppgifterna på entreprenad.

Skyldigheter för leverantörer av digitala tjänster med avseende på hantering av säkerhetsrisker

Enligt artikel 16 ska även leverantörer av digitala tjänster åläggas att hantera risker för säkerheten i deras nätverks- och informationssystem och att rapportera incidenter till behöriga myndigheter eller till CSIRT-enheter.

Leverantörer av digitala tjänster är i enlighet med bilaga III till direktivet internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster. Enligt direktivet finns det avgörande skillnader mellan leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, varför den lagstiftning som gäller leverantörer av digitala tjänster måste vara mer enhetlig.

Medlemsstaterna ska fastställa vilka leverantörer av samhällsviktiga tjänster som omfattas av skyldigheterna enligt direktivet, medan direktivet däremot ska gälla för alla leverantörer av digitala tjänster som omfattas av dess tillämpningsområde. Kommissionen kan också anta genomförandeakter för att harmonisera säkerhets- och rapporteringskraven för leverantörer av digitala tjänster. Medlemsstaterna får inte ålägga leverantörer av digitala tjänster mer långtgående skyldigheter än de som föreskrivs i direktivet.

Rapporteringsskyldighet

Medlemsstaterna ska säkerställa att leverantörer av samhällsviktiga tjänster utan onödigt dröjsmål till den behöriga myndigheten eller CSIRT-enheten rapporterar incidenter som har en betydande inverkan på kontinuiteten i de samhällsviktiga tjänster som de tillhandahåller. Med incident avses i direktivet en händelse med en faktisk negativ inverkan på säkerheten i nätverks- och informationssystem.

Vidare ska medlemsstaterna ålägga leverantörer av digitala tjänster att till den nationella myndigheten rapportera alla incidenter som har en avsevärd inverkan på tillhandahållandet av en tjänst som avses i bilaga III till direktivet och som de erbjuder inom unionen. Rapporterna ska innehålla information som gör det möjligt för den behöriga myndigheten eller CSIRT-enheten att fastställa vilken betydelse eventuell gränsöverskridande inverkan har.

2.2.2 Den internationella utvecklingen

I flera stater och i det internationella samarbetet har informationssäkerheten fått allt större utrymme i politiken under de senaste åren. Strategier för cybersäkerhet har utarbetats t.ex. i så gott som alla EU-medlemsstater, i USA, Australien, Nya Zeeland, Kanada, Japan och Indien. Prioriteringarna i strategierna och organiseringen av den cybersäkerhetsrelaterade myndighetsverksamheten varierar mellan staterna. I vissa stater är myndighetsverksamheten nära sammankopplad med försvarsförvaltningens eller underrättelsemyndigheternas verksamhet och i andra stater med de myndigheter som har tillsyn över kommunikationstjänster. I en del stater har uppgifter som relaterar till cybersäkerhet koncentrerats till en enda myndighet, medan andra stater har fördelat uppgifterna på flera olika myndigheter.

Det nationella genomförandet av direktivet om nät- och informationssäkerhet pågår fortfarande i EU:s medlemsstater, och det kommer sannolikt att påverka utvecklingen av medlemsstaternas lagstiftning på ett betydande sätt.

Tyskland

I Tyskland offentliggjordes en nationell cybersäkerhetsstrategi år 2011. I strategin är skyddet av den kritiska infrastrukturen mot cyberintrång en central prioritering. I cybersäkerhetsstrategin anges som ett mål att bedöma möjligheterna att föreskriva om samarbete i lagstiftningen. I Tyskland har man sedan 2005 bedrivit tvärsektoriellt samarbete mellan den offentliga och den privata sektorn för att förebygga och förbereda sig för cyberintrång och dela information. Detta har skett inom ramen för den så kallade *UP KRITIS*-handlingsplanen. År 2014 utvidgades denna handlingsplan ytterligare. År 2015 trädde ”*it-säkerhetslagen*” (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, IT-Sicherheitsgesetz) i kraft och skapade en lagstiftningsram för samarbete enligt UP KRITIS-handlingsplanen mellan det offentliga och det privata för att förbättra informationssäkerheten i samhällskritiska tjänster. I lagen åläggs vissa aktörer inom den kritiska infrastrukturen att sörja för informationssäkerheten och rapportera incidenter till den övervakande myndigheten. Lagen ger också den övervakande myndigheten behörighet att förrätta inspektioner och påföra sanktioner. Lagen anger inte närmare vad de informationssäkerhetsrelaterade skyldigheterna omfattar, utan det är upp till aktörerna att definiera deras innehåll. Aktörerna ska dock kunna påvisa att nivån på informationssäkerheten är tillräcklig.

Enligt den tyska it-säkerhetslagen är informationssäkerhetsmyndigheten BSI (Bundesamt für Sicherheit in der Informationstechnik, Federal Office for Information Security) behörig tillsynsmyndighet, och den ska även ta emot de rapporter om it-säkerhetsincidenter som avses i lagen. Behörig myndighet i fråga om telekommunikations- och energisektorn och delvis även post- och järnvägssektorn är emellertid BnetzA (Bundesnetzagentur). I egenskap av Tysklands nationella informationssäkerhetsmyndighet har BSI också många andra informationssäkerhetsrelaterade uppgifter. Till myndighetens uppgifter hör bl.a. att främja informationssäkerheten inom statsförvaltningen, att upprätthålla en lägesbild av informationssäkerheten, incidenthanteringsenheten CERT-Bunds verksamhet samt uppgifter som gäller standardisering och certifiering.

Frankrike

Frankrike har strävat efter att förbättra informationssäkerheten i samhällsviktiga funktioner som en del av regleringen om den kritiska infrastrukturen. Bestämmelser om informationssäkerhet togs in i den allmänna lagstiftningen om den kritiska infrastrukturen genom en lagändring 2013 (den s.k. *CIIP-lagen,* loi n° 2013-1168 du 18 décembre 2013*)*. I lagen ingår bestämmelser om riskhanteringsskyldigheter och rapporteringsskyldigheter med anknytning till informationssäkerhet. Informationssäkerhetsincidenter enligt CIIP-lagen ska rapporteras till Frankrikes nationella cybersäkerhetsmyndighet (ANSSI, Agence nationale de la sécurité des systèmes d’information).

CIIP-lagen preciseras av premiärministerns dekret (arrêté du Premier ministre) för varje sektor. Dekreten har beretts av ANSSI utifrån åtgärdsrekommendationer om samarbete mellan det offentliga och det privata.

ANSSI lyder under den franska försvarsförvaltningen. ANSSI är en nationell myndighet för cyberförsvar och nät- och informationssäkerhet (decree n°2011-170) och finns i anslutning till

försvars- och säkerhetsmyndigheten (Secrétariat général de la Défense et de la Sécurité nationale). I samband med ANSSI finns också landets incidenthanteringsenhet (CERT-FR).

Frankrike kommer att lägga fram ett lagförslag om genomförandet av direktivet om nät- och informationssäkerhet under 2017.

Sverige

I Sverige finns ingen nationell lagstiftning som motsvarar direktivet om nät- och informationssäkerhet. I Sverige lämnade den utredare som svarade för beredningen av det nationella genomförandet av direktivet om nät- och informationssäkerhet sin rapport i början av 2017 (Informationssäkerhet för samhällsviktiga och digitala tjänster, Betänkande av Utredningen om genomförande av NIS-direktivet, SOU 2017:36). I rapporten finns åtgärder för genomförande av direktivet och ett förslag till nationell lagstiftning. Utredaren föreslår att det införs en helt ny lag och en kompletterande förordning om informationssäkerhet för samhällsviktiga tjänster i syfte att införliva direktivet om nät- och informationssäkerhet i den svenska lagstiftningen.

I utredarens rapport förslås det att den nationella Myndigheten för samhällsskydd och beredskap (MSB) ska ges ansvaret att bedöma vilka tjänster som är att anse som samhällsviktiga och uppdatera förteckningen över dem. Enligt rapporten ska bedömningen göras med särskild hänsyn till hur en störning skulle påverka tillhandahållandet av tjänsten.

I rapporten föreslås det att incidenter som avses i direktivet om nät- och informationssäkerhet ska rapporteras till MSB. I rapporten föreslås vidare att MSB ska anförtros rollen som nationell kontaktpunkt och CSIRT-enhet. MSB:s lagstadgade uppdrag omfattar dock inte bara cybersäkerhetsfrågor, utan också allmän säkerhet, skydd av civila samt organiseringsuppdrag vid nödlägen och undantagstillstånd. Därför föreslår rapporten att tillsynsmyndigheterna för varje sektor (Statens energimyndighet (energi), Transportstyrelsen (transporter), Finansinspektionen (bankverksamhet och finansmarknadsinfrastruktur), Inspektionen för vård och omsorg (hälso- och sjukvård), Livsmedelsverket (leverans och distribution av dricksvatten), Post- och telestyrelsen (digital infrastruktur och leverantörer av digitala tjänster) ska utses till behöriga tillsynsmyndigheter enligt direktivet.

Storbritannien

Regeringen i Storbritannien har offentliggjort en nationell cybersäkerhetsstrategi för åren 2016–2020. Som en av åtgärderna i strategin inrättades i Storbritannien en ny centraliserad cybersäkerhetsmyndighet vars uppgifter bl.a. är att förbättra informationssäkerheten i den kritiska infrastrukturen, undersöka informationssäkerhetsincidenter, informera om sårbarheter och främja den allmänna medvetenheten om informationssäkerhet (The National Cyber Security Centre). Cybersäkerhetscentret är en del av Förenade kungarikets underrättelse- och säkerhetstjänst GCHQ (Government Communications Headquarters), som bl.a. utför signalspaning för regeringens och arméns behov och ansvarar för informationssäkerheten. Vid cybersäkerhetscentret finns också landets incidenthanteringsenhet (CERT UK). I Storbritannien sköter även dataskyddsmyndigheten (Information Commissioner's Office ICO) informationssäkerhetsrelaterade uppgifter med anknytning till dataskydd och elektronisk kommunikation.

I Storbritannien finns ingen nationell lagstiftning som motsvarar direktivet om nät- och informationssäkerhet. Trots Storbritanniens utträde ur EU kommer direktivet sannolikt att införlivas i den nationella lagstiftningen. Storbritannien har i augusti 2017 inlett ett offentligt sam-

råd om genomförande av direktivet. I en promemoria som publicerats som stöd för det offentliga samrådet (Security of Network and Information Systems, Public Consultation) fastställs preliminära riktlinjer för det nationella genomförandet.

USA

I USA finns ett flertal olika strategier som innehåller politiska och strategiska riktlinjer om cybersäkerhet. Även federala lagar och lagar, föreskrifter och praxis på delstatsnivå innehåller en del bestämmelser om informationssäkerhet. En del av lagstiftningen gäller vissa specifika funktioner medan andra sträcker sig över flera olika samhällssektorer (t.ex. skyldigheten att rapportera informationssäkerhetsincidenter). Det finns också informationssäkerhetsrelaterad myndighetsverksamhet på både federal nivå och delstatsnivå. Trots den gällande lagstiftningen finns det på federal nivå inga egentliga bestämmelser om informationssäkerhetsrelaterade skyldigheter för samhällsviktiga aktörer. I stället har man strävat efter att förbättra informationssäkerheten i samhällsviktiga tjänster i samarbete med företagen. Det nationella institutet för standarder och teknik (National Institute of Standards and Technology, NIST) har tagit fram en rekommendation för att förbättra informationssäkerheten i kritisk infrastruktur (Framework for Improving Critical Infrastructure Cybersecurity, 2014). Rekommendationen innehåller konkreta åtgärdsförslag som gäller riskhantering samt anvisningar som grundar sig på gällande informationssäkerhetsstandarder. Utarbetandet av rekommendationen hade ett nära samband med ett presidentdekret av president Obama (Executive order 13636 – Improving Critical Infrastructure Cybersecurity), som medför skyldigheter för statliga ämbetsverk att t.ex. utveckla ett teknikneutralt och frivilligt cybersäkerhetsramverk, att främja och uppmuntra införandet av cybersäkra rutiner, att öka och förbättra informationsdelningen om cybersäkerhetshot och se till att den sker i god tid, att inkludera ett starkt skydd för privatliv och medborgerliga rättigheter i alla initiativ och projekt samt att skydda kritisk infrastruktur och undersöka hur den gällande regleringen kan utnyttjas för att främja cybersäkerheten.

2.3 Bedömning av nuläget

2.3.1 Informationssäkerhetsstrategin

Direktivet om nät- och informationssäkerhet förutsätter att varje medlemsstat utarbetar en nationell strategi som anger ramarna, visionen, målen och prioriteringarna för nät- och informationssäkerhet på nationell nivå.

I informationssäkerhetsstrategin, som godkändes av kommunikationsministeriet i mars 2016, betonas att utgångspunkten enligt rättsordningen i Finland kan anses vara att ramarna, målen och prioriteringarna för nät- och informationssäkerheten i första hand ska fastställas i den gällande lagstiftningen. Enligt rättsstatsprincipen i grundlagen ska all utövning av offentlig makt bygga på lag. Även det myndighetsansvar som gäller informationssäkerhet ska bygga på lagstiftning. I strategin anges mål för att säkerställa lagstiftningens kvalitet till den del som lagstiftningen kan påverka nät- och informationssäkerheten och därmed framväxten av en tillväxtmiljö för digital affärsverksamhet. Åtgärderna ska genomföras av de myndigheter och andra aktörer som åläggs ansvaret i strategin. Ansvarsfördelningen grundar sig på den gällande lagstiftningen om myndigheternas befogenheter. Genom strategin genomförs artikel 7 i direktivet om nät- och informationssäkerhet.

2.3.2 Åtgärder till följd av it-säkerhetsincidenter och undersökning av dem

För att kunna vidta åtgärder till följd av it-säkerhetsincidenter och undersöka dem har Kommunikationsverket ett omfattande uppdrag enligt informationssamhällsbalken.

Uppgifterna för CSIRT-enheter enligt artikel 9 i direktivet om nät- och informationssäkerhet ingår i princip i Kommunikationsverkets uppgifter enligt informationssamhällsbalken. De nuvarande uppgifterna för Kommunikationsverkets CERT-enhet motsvarar till stor del en CSIRT-enhets uppgifter, men de begränsas inte enbart till tillämpningsområdet för direktivet om nät- och informationssäkerhet. CERT-enheten tillhandahåller hjälp för hantering av it-säkerhetsincidenter för alla finländare, personer bosatta i Finland och juridiska personer med verksamhet i Finland. Vem som helst kan underrätta Kommunikationsverket om it-säkerhetsincidenter eller hot om sådana som riktar sig mot Finland eller finländarna. Dessutom är Kommunikationsverket på uppdrag av finansministeriet Finlands GovCERT, dvs. den myndighet som hanterar it-säkerhetsincidenter och hot som riktar sig mot statsförvaltningen. Med hjälp av finansiering från Försörjningsberedskapscentralen tillhandahåller Kommunikationsverket dessutom CERT-tjänster för företag som är etablerade i Finland och som är kritiska för försörjningsberedskapen.

Kommunikationsverkets verksamhet uppfyller redan i dagsläget de krav som ställs på CSIRT-enheter i artikel 9 och bilaga I till direktivet om nät- och informationssäkerhet, inklusive förmågan att vidta åtgärder mot incidenter dygnet runt, analysera incidenter, skapa en lägesbild, ge tidiga varningar och sprida information om informationssäkerhetsrisker. Kommunikationsverket har också aktiva relationer med den privata sektorn. Relationerna bygger på frivillighet och konfidentiellt samarbete. Kommunikationsverket kan i syfte att upprätthålla informationssäkerheten erbjuda tjänsteleverantörerna stöd för att identifiera incidenter samt ge dem information om återhämtning efter incidenter och varningar om risker. Verket erbjuder också möjligheter till nätverksbildning med andra aktörers it-säkerhetsexperter. Rapporteringen av incidenter och utbytet av information grundar sig på ömsesidigt förtroende mellan aktörerna och analyserna av informationen på aktörernas samtycke. Kommunikationsverket har dessutom välfungerande kontakter med CSIRT- eller CERT-enheterna i de övriga EU-länderna.

De gemensamma kontaktpunkterna enligt artikel 8 i direktivet ska utöva en sambandsfunktion för att säkerställa gränsöverskridande samarbete mellan medlemsstaternas myndigheter.

Det är ändamålsenligt att den gemensamma kontaktpunkten finns i samband med CSIRT-enheten vid Kommunikationsverket.

Även om de myndighetsuppgifter som beskrivs ovan i princip redan ingår i Kommunikationsverkets nuvarande lagstadgade uppgifter i och med det breda tillämpningsområdet för direktivet om nät- och informationssäkerhet, bör man precisera Kommunikationsverkets rätt att samarbeta med andra myndigheter och i direktivet avsedda samarbetsorgan.

2.3.3 Samhällsviktiga tjänster och leverantörer av samhällsviktiga tjänster

Enligt direktivet om nät- och informationssäkerhet ska medlemsstaterna för varje sektor och delsektor som hör till direktivets tillämpningsområde identifiera de leverantörer av samhällsviktiga tjänster som är etablerade på deras territorium. De sektorer och delsektorer som ingår i direktivets tillämpningsområde definieras i bilaga II till direktivet.

I direktivets artikel 5 anges kriterierna för identifiering av leverantörer av samhällsviktiga tjänster. Enligt direktivet ska leverantörer av samhällsviktiga tjänster tillhandahålla tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet. Denna

tjänst ska vara beroende av nätverks- och informationssystem. Ett ytterligare kriterium är att en incident i tjänsten skulle medföra en betydande störning enligt artikel 6 vid tillhandahållandet av tjänsten. Direktivet ger medlemsstaterna ett avsevärt handlingsutrymme när det gäller att definiera vilka tjänster som är samhällsviktiga.

Enligt ingressen till direktivet kan leverantörer av samhällsviktiga tjänster identifieras genom att anta en förteckning över samhällsviktiga tjänster eller genom att anta nationella åtgärder som gör det möjligt att fastställa vilka enheter som omfattas av skyldigheter när det gäller säkerhet i nätverks- och informationssystem.

Såsom det konstaterats i beskrivningen av nuläget har begreppen kritisk infrastruktur eller samhällsviktiga funktioner inte definierats på lagstiftningsnivå i Finland, och den gällande lagstiftningen innehåller inga egentliga förfaranden enligt vilka t.ex. myndigheter som utövar övervakning och tillsyn direkt skulle kunna identifiera sådana leverantörer av samhällsviktiga tjänster som avses i direktivet om nät- och informationssäkerhet. Med beaktande av befintliga administrativa strukturer och gällande lagstiftning är det naturligast att identifieringen av leverantörer av samhällsviktiga tjänster sker i samband med införandet av den lagstiftning som genomför direktivet om nät- och informationssäkerhet.

Enligt direktivet om nät- och informationssäkerhet ska en leverantör av samhällsviktiga tjänster tillhandahålla en tjänst som är viktig för samhällets funktion. Enligt direktivet får medlemsstaterna avgöra vilka tjänster och leverantörer som är viktiga.

Identifieringen av vilka tjänster som är samhällsviktiga inom varje sektor och delsektor som anges i direktivet är beroende av sektorsspecifika särdrag. Graden av väsentlighet beror bl.a. på hur viktiga tjänsterna är för medborgare och företag, hur beroende industrin är av tjänsterna och hur många olika konkurrerande tjänster som finns tillgängliga på marknaden. Samhällsviktiga tjänster kan bestå av en bredare uppsättning tjänster än de som är kritiska med avseende på försörjningsberedskapen eller hör till den kritiska infrastrukturen.

Enligt direktivet ska en samhällsviktig tjänst dessutom vara beroende av nätverks- och informationssystem. Enligt direktivet får medlemsstaterna även här bedöma graden av beroende. Vid bedömningen bör medlemsstaterna beakta på vilket sätt tjänsten tillhandahålls. Utgångsantagandet är att en stor del av tjänsterna i dagsläget på ett eller annat sätt är beroende av kommunikationsnät och informationssystem.

Ett ytterligare kriterium enligt direktivet är att en incident i tjänsten skulle medföra en betydande störning vid tillhandahållandet av tjänsten. Enligt direktivet ska medlemsstaterna när de bedömer om en störning är betydande beakta det antal användare som är beroende av tjänsten, hur beroende andra samhällsviktiga tjänster är av den tjänst som aktören tillhandahåller, vilken inverkan incidenter skulle kunna ha på ekonomisk och samhällelig verksamhet eller allmän säkerhet, aktörens marknadsandel, hur stort geografiskt område som skulle kunna påverkas av en incident samt tillgången till alternativa sätt för att tillhandahålla tjänsten. De skyldigheter som räknas upp i direktivet är sådana att de bör bedömas nationellt med avseende på varje sektor och tjänst.

Kommunikationsministeriet tillsatte i oktober 2016 en tvärsektoriell arbetsgrupp för att stödja det nationella genomförandet av direktivet om nät- och informationssäkerhet. Arbetsgruppen föreslog i sin slutrapport att leverantörerna av samhällsviktiga tjänster enligt direktivet ska fastställas på lagnivå. För att man ska kunna specificera vilka som omfattas av skyldigheterna bör man bedöma vilka tjänster som på nationell nivå ska betraktas som viktiga för att upprätt-

hålla samhällelig verksamhet enligt direktivet, inom de sektorer som hör till direktivets tillämpningsområde. Därefter bör man undersöka om leverantörerna av dessa tjänster redan med stöd av den gällande lagstiftningen är skyldiga att sörja för att informationssäkerheten är på minst samma nivå som förutsätts i direktivet. Om svaret är ja behöver nya skyldigheter inte föreskrivas. I fråga om de tjänster vars leverantörer i ljuset av direktivet inte har ålagts tillräckliga skyldigheter i den gällande lagstiftningen ska denna identifiering däremot göras som en del av införandet av nya skyldigheter.

Energi

Enligt direktivet om nät- och informationssäkerhet ska leverantörer av samhällsviktiga tjänster identifieras inom sektorn energi och delsektorerna elektricitet, olja och gas.

Samhällets funktion är i dag ytterst beroende av olika elektriska system. Så gott som alla samhällsviktiga tjänster behöver också el för att kunna produceras. Eldistributionen har en så betydande roll när det gäller tillhandahållandet av samhällsviktiga tjänster och deras kontinuitet att den alltid bör betraktas som en väsentlig tjänst för kunderna oberoende av t.ex. distributionsnätets storlek.

Elnätet i Finland omfattar stamnätet, lokalnäten och distributionsnäten. I stamnätet överförs el från produktionsområdena och utlandet till förbrukningscentrum. Merparten av den el som förbrukas i Finland överförs via stamnätet. En del av de kraftverk som producerar el är anslutna direkt till stamnätet. Detsamma gäller stora förbrukare såsom stora fabriker. Kraftverk kan också vara anslutna till region- eller distributionsnätet. Exempelvis får elektrifierade banavsnitt och Helsingfors-Vanda flygplats sin ström från stamnätet. I Finland finns 77 innehavare av eldistributionsnät och 11 innehavare av högspänningsdistributionsnät. Systemansvarig stamnätsinnehavare är Fingrid Oyj.

I fråga om eldistribution kan som sådana i artikel 5.2 i direktivet avsedda tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet i princip betraktas

1) överföringstjänster i stamnätet och systemtjänster som tillhandahålls av den systemansvariga stamnätsinnehavaren,

2) eldistribution i distributionsnät, dock inte eldistribution i slutna distributionsnät,

3) eldistribution i högspänningsdistributionsnät, dock inte eldistribution i slutna distributionsnät.

Inom delsektorn gas är naturgas en betydande komponent i energiförbrukningen i Finland. Naturgas utgör cirka åtta procent av Finlands energiförsörjning. Naturgas används särskilt för samproduktion av fjärrvärme och el. Ett annat viktigt användningsområde för naturgas är industriella tillverkningsprocesser. År 2016 användes 23,8 terawattimmar naturgas i Finland.

För användningen av naturgas är det väsentligt att överföringen av naturgas och överföringsnätet fungerar störningsfritt. Överföringstjänster i överföringsnätet och systemtjänster som tillhandahålls av den systemansvariga stamnätsinnehavaren i enlighet med naturgasmarknadslagen kan därför i princip betraktas som sådana i artikel 5.2 i direktivet avsedda tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet.

Inom delsektorn olja har det inte identifierats några viktiga tjänster eller tillhandahållare av sådana som uppfyller kriterierna i direktivet.

Transporter

Tjänster inom sektorn transporter kan grovt taget delas in i tre nivåer; trafikledningstjänster, förvaltning av viktig infrastruktur samt tillhandahållande av trafiktjänster. Tjänsternas karaktär varierar inom olika nivåer av trafiksystemet.

Trafikledningstjänster

Trafikledning är en väsentlig del av ett fungerande trafiksystem och påverkar direkt säkerheten i hela trafiksystemet. Störningar i trafikledningen kan direkt leda till att trafiksäkerheten äventyras eller att trafiken avbryts. Dessutom är trafikledningsfunktionerna beroende av ett fåtal aktörer. Trafikledningen kommer framöver att få allt större betydelse för trafiksystemets funktion och säkerhet då intelligent automatisering av trafiken blir vanligare.

Inom luftfarten är det flygtrafiktjänsten som svarar för trafikledningen. Med flygtrafiktjänst avses enligt 160 § i luftfartslagen flygtrafiklednings-, kommunikations-, navigations- och övervakningstjänst, flygvädertjänst och flygbriefingtjänst. I Finland tillhandahålls flygtrafiktjänster av bolaget Air Navigation Services Finland Oy (ANS Finland), som ägs helt av staten. ANS Finland ansvarar för specialtjänster som hänför sig till flygtrafiktjänsten, såsom luftrumsplanering, områdeskontroll, tjänster för statlig luftfart och flygräddning. Statsrådet har utsett Meteorologiska institutet till nationell leverantör av flygvädertjänster enligt 108 § i luftfartslagen.

Enligt 36 § i järnvägslagen ansvarar bannätsförvaltaren för ledningen av järnvägstrafiken på sitt bannät. Förvaltaren kan ordna trafikledningstjänsterna själv eller upphandla dem hos offentliga eller privata serviceproducenter. Trafikverket ansvarar för övervakningen och samordningen av den operativa verksamheten i samband med ledningen av järnvägstrafiken. Den operativa ledningen av järnvägstrafiken köps från Finrail Oy.

Inom sjötrafiken ansvarar fartygstrafikservicen för trafikledningen. Enligt lagen om fartygstrafikservice avses med fartygstrafikservice (Vessel Traffic Service, VTS) sådan övervakning och ledning av fartygstrafiken som har beredskap att samverka med trafiken och reagera på föränderliga trafiksituationer. VTS-myndigheten har hand om fartygstrafikservicen. Trafikverket är VTS-myndighet enligt lagen om fartygstrafikservice.

Inom vägtrafiken har trafikledningen delvis en annorlunda roll än inom övriga trafikformer. Åtminstone tills vidare leds trafiken i betydande utsträckning genom trafikregler och sådana trafikanordningar som inte är beroende av kommunikationsnät och informationssystem (vägmarkeringar, vägmärken).

I princip kan trafikledningstjänster betraktas som sådana i artikel 5.2 i direktivet avsedda tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet. Här är det således flygtrafiktjänster, ledning av järnvägstrafik och fartygstrafikservice som betraktas som viktiga tjänster. Ledning av vägtrafiken ska tills vidare inte betraktas som en samhällsviktig tjänst enligt direktivet om nät- och informationssäkerhet. När den intelligenta automatiseringen av trafiken utvecklas bör detta dock bedömas på nytt.

Förvaltning av viktig infrastruktur

Förutom av trafikledning är tillhandahållandet av ett flertal trafiktjänster beroende av viktig trafikinfrastruktur och det är sällan möjligt att tillhandahålla trafiktjänsterna på ett alternativt sätt om den viktiga infrastrukturen är ur bruk. Den viktiga trafikinfrastrukturen omfattar särskilt flygplatser, hamnar, järnvägar och vägnätet.

Flygplatserna har en betydande ställning i Finland när det gäller passagerartrafiken, och antalet flygpassagerare ökar hela tiden. År 2016 översteg antalet flygpassagerare i Finland 16 miljoner. Finavias flygplatser hade åtta procent fler passagerare än året innan. Mängden godstrafik på Finavias flygplatser uppgick till sammanlagt 183 442 ton år 2016. Flygfrakten står för cirka tio procent av utrikeshandelns värde.

På flygplatserna tillhandahålls tjänsterna av flera olika leverantörer. Det är dock flygplatsoperatören, som ansvarar för förvaltningen av flygplatsen, som har den viktigaste rollen när det gäller underhåll av infrastrukturen. I luftfartslagen föreskrivs om förutsättningarna för beviljande av intyg över godkännande av trafikflygplats. Flygplatsoperatören ansvarar också för exempelvis genomförandet av de åtgärder och arrangemang som förutsätts på flygplatsen för luftfartsskyddet. Flygplatsoperatören har också skyldigheter med avseende på beredskap.

Förutom flygplatser omfattar den viktiga infrastrukturen även hamnar. År 2014 gick 96 miljoner ton av utrikeshandelns transporter som sjötransporter och cirka 11 miljoner ton som landtransporter. Räknat i tonkilometer skickas 96 procent av alla godstransporter inom Finlands utrikeshandel som sjötransporter. Näringslivet och hela det övriga samhället är således ytterst beroende av hamnarnas funktion. Precis som på flygplatserna tillhandahålls tjänster i hamnarna av flera olika leverantörer. Hamninnehavarna ansvarar för driften av hamnar och hamnanläggningar. Bestämmelser om hamninnehavarens ansvar finns i lagen om sjöfartskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet.

Även järnvägarna är viktiga för både person- och godstransporter. År 2016 uppgick antalet passagerare på järnvägarna till cirka 82 miljoner. Antalet godstransporter på järnvägarna uppgick år 2014 till 37 miljoner ton och transportarbetet uppgick till cirka 9,6 miljarder tonkilometer. Bannätsförvaltaren ska förvalta, utveckla och underhålla bannätet. Med statlig bannätsförvaltare avses enligt järnvägslagen Trafikverket. Med privat spåranläggning avses en spåranläggning som inte är statsägd och inte förvaltas av Trafikverket. Dessa spåranläggningar kan förvaltas av t.ex. kommuner, hamnar eller företag. Privata spåranläggningar kan i sig vara viktiga för t.ex. vissa industrianläggningar eller hamnar. Förvaltningen av dem är emellertid inte samhällsviktig verksamhet på samma sätt som i fråga om statliga järnvägar.

Även vägnätet är en viktig del av trafikinfrastrukturen. Väsentligt vid förvaltningen av vägnätet med avseende på informationssäkerheten är framför allt de digitala informationssystem som anknyter till väginfrastrukturen. Sådana informationssystem är i synnerhet ITS-system enligt ITS-direktivet. I Finland har ITS-direktivet införlivats i lagen om transportservice. Bestämmelser om införande av intelligenta transportsystem finns i III avd. 2 kap. 6 § i lagen om transportservice. För närvarande kan nödsamtalssystemet eCall och Trafikverkets tjänster Digiroad (väg- och gatuinformation) och Digitraffic (trafikinformation) betraktas som intelligenta trafiksystem enligt ITS-direktivet. Systemet eCall förvaltas av Nödcentralsverket.

Digiroad är ett nationellt informationssystem som förvaltas av Trafikverket och som innehåller samlade uppgifter om hela det finländska väg- och gatunätets mittlinjesgeometri och om vägnätets viktigaste egenskaper. Digiroad visar en beskrivning av trafiknätet i digital form. Digitraffic är Trafikverkets tjänst som ger aktuell trafikinformation om vägnätet, järnvägs- och sjötrafiken i Finland.

I princip kan förvaltning av den viktiga trafikinfrastrukturen betraktas som en sådan i artikel 5.2 i direktivet avsedd tjänst som är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet. Här är det således förvaltningen av flygplatser, hamnar och statens bannät samt förvaltningen av ITS-system enligt ITS-direktivet som betraktas som viktiga tjänster.

Trafiktjänster

Inom transportområdet tillhandahålls förutom trafikledning och trafikinfrastruktur många slags trafiktjänster (t.ex. av lufttrafikföretag, rederier, järnvägsoperatörer). Trafiktjänster är emellertid samhällsviktiga i ett annat avseende än de ovan beskrivna tjänster som gäller trafikledning och förvaltning av infrastruktur. Trafiktjänster kan tillhandahållas av flera konkurrerande aktörer. Dessutom kan det finnas alternativa sätt att ordna tjänsten. Även om det i fråga om vissa transportslag är ett fåtal eller rentav bara en aktör som tillhandahåller inhemska tjänster (t.ex. flygtrafiken och järnvägstrafiken), finns det ändå i regel alternativa sätt att ordna tjänsten tack vare antingen internationell konkurrens eller alternativa transportformer. Trafiktjänsterna håller i ökande grad på att bli mer internationella. Exempelvis inom luftfarten har detta redan lett till en strävan att reglera det globala gemensamma luftfartssystemet genom harmoniserade internationella regler. När det gäller dem som tillhandahåller trafiktjänster bör följaktligen även informationssäkerheten framöver utvecklas på ett mer fokuserat och enhetligt sätt, som en del av beredningen av internationella avtalsförpliktelser och EU-rättsakter. På så sätt skulle man kunna undvika eventuella störningar i trafiksystemets funktion, säkerhet och nationella konkurrensvillkor som beror på skillnader i den internationella regleringen.

Bankverksamhet och finansmarknadsinfrastruktur

För sektorerna bankverksamhet och finansmarknadsinfrastruktur anges i bilaga II till direktivet om nät- och informationssäkerhet inga delsektorer inom vilka samhällsviktiga tjänster enligt direktivet bör identifieras. I bilagan till direktivet anges som typer av enheter kreditinstitut, operatörer av handelsplatser enligt definitionen i artikel 4.24 i Europaparlamentets och rådets direktiv 2014/65/EU samt centrala motparter. Inom sektorerna bankverksamhet och finansmarknadsinfrastruktur betraktas i Finland kreditinstitutsverksamhet enligt kreditinstitutslagen och börsverksamhet enligt lagen om handel med finansiella instrument som sådana i artikel 5.2 i direktivet avsedda tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet. I Finland finns inga centrala motparter som hör till direktivets tillämpningsområde.

Hälso- och sjukvårdssektorn

Syftet med hälso- och sjukvården är att främja och upprätthålla befolkningens hälsa, välfärd, arbets- och funktionsförmåga och sociala trygghet och att minska hälsoskillnader. Det är väsentligt för samhällets funktion att hälso- och sjukvården fungerar utan störningar och avbrott. Tjänsteleverantörer inom hälso- och sjukvårdsområdet är de som tillhandahåller offentliga och privata socialvårdstjänster och hälso- och sjukvårdstjänster. Ur ett informationssäkerhetsperspektiv skulle informationssäkerhetsrelaterade störningar i sådana system som behandlar patienternas klientuppgifter eller som ingår i produkter som används inom hälso- och sjukvården kunna ha de största negativa konsekvenserna för samhället. Därför ska elektronisk behandling av klientuppgifter inom hälsovården och underhåll och användning av produkter för hälso- och sjukvård vid tillhandahållandet av offentliga och privata tjänster inom social- och hälsovården anses vara sådana i artikel 5.2 i direktivet avsedda tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet.

Leverans och distribution av dricksvatten

Fungerande vattentjänster har en avgörande betydelse för samhällets grundläggande funktioner. Vattentjänsterna hör vid sidan av elförsörjningen till de viktigaste tjänsterna i samhället, och de bör fungera under alla omständigheter. Vattentjänsterna har stor betydelse i synnerhet för hushållens dricksvatten och inom hygienhanteringen, hälso- och sjukvården, livsmedelsindustrin och den övriga industrin.

Vattentjänstverken sköter ett samhälles vattentjänster. Vattentjänster ska betraktas som sådana i artikel 5.2 i direktivet avsedda tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet.

Digital infrastruktur

Ett teleföretag enligt informationssamhällsbalken är en aktör som tillhandahåller nättjänster eller kommunikationstjänster för en grupp av användare som inte har avgränsats på förhand, dvs. bedriver allmän televerksamhet. Definitionen av teleföretag är bred och omfattar de viktigaste funktionerna inom den digitala infrastrukturen, inklusive internetknutpunkter, åtminstone i den mån de används för att koppla samman allmänna kommunikationsnät, samt tillhandahållande av domännamnssystem när verksamheten hänför sig till internetaccesstjänster.

Även om allmän televerksamhet inom området digital infrastruktur skulle kunna betraktas som en samhällsviktig tjänst omfattas teleföretagen i regel inte av skyldigheterna enligt direktivet om nät- och informationssäkerhet. Dessutom finns det redan bestämmelser om teleföretagens hantering av informationssäkerhetsrisker och skyldigheten att rapportera störningar i informationssamhällsbalken.

Vid sidan av allmän televerksamhet kan även förvaltning av toppdomänregister anses vara viktigt för den digitala infrastrukturen. I Finland är det fråga om registret för toppdomänerna fi och ax. Förvaltning av toppdomänregister kan i princip betraktas som en sådan i artikel 5.2 i direktivet avsedd tjänst som är viktig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet.

2.3.4 Krav som gäller tjänsteleverantörernas verksamhet med avseende på informationssäkerhetsrisker och rapportering

Energi

Inom delsektorn elektricitet har som sådana samhällsviktiga tjänster som avses i artikel 5.2 i direktivet ovan identifierats

1) överföringstjänster i stamnätet och systemtjänster som tillhandahålls av den systemansvariga stamnätsinnehavaren

2) eldistribution i distributionsnät, dock inte eldistribution i slutna distributionsnät

3) eldistribution i högspänningsdistributionsnät, dock inte eldistribution i slutna distributionsnät

Enligt artikel 5 i direktivet ska tillhandahållandet av en samhällsviktig tjänst som avses i direktivet även vara beroende av nätverks- och informationssystem. Ett ytterligare kriterium är att en incident i tjänsten skulle medföra en betydande störning vid tillhandahållandet av tjänsten. Eldistribution kan i princip alltid anses vara beroende av nätverks- och informationssystem, eftersom elnäten i dag är långt automatiserade system vars funktionssäkerhet har en väsentlig betydelse för att tillgången till energi ska tryggas. Informationssäkerhetsrelaterade störningar i eldistributionen kan få betydande negativa konsekvenser, inte bara för eldistributionen utan också för tillhandahållandet av andra samhällsviktiga tjänster. Konsekvenserna kan vara betydande oberoende av distributionsnätets storlek. Inom delsektorn elektricitet kan således den systemansvariga stamnätsinnehavaren och eventuella andra stamnätsinnehavare, alla distributionsnätsinnehavare oavsett storlek samt innehavare av högspänningsdistributionsnät, dock inte slutna distributionsnät, betraktas som leverantörer av samhällsviktiga tjänster enligt direktivet.

Inom delsektorn naturgas har i naturgasmarknadslagen avsedda överföringstjänster i överföringsnätet och systemtjänster som tillhandahålls av den systemansvariga stamnätsinnehavaren ovan betraktats som sådana samhällsviktiga tjänster som avses i direktivet. Dessa tjänster är i princip alltid beroende av nätverks- och informationssystem, eftersom naturgasnäten i dag är långt automatiserade system vars funktionssäkerhet har en väsentlig betydelse för att tillgången till energi ska tryggas. Dessutom skulle betydande störningar i dessa tjänsters informationssäkerhet kunna få omfattande negativa konsekvenser för kontinuiteten i överföringen av naturgas. Som leverantörer av samhällsviktiga tjänster enligt direktivet om nät- och informationssäkerhet kan således betraktas den systemansvariga överföringsnätsinnehavaren och eventuella andra överföringsnätsinnehavare.

Även om vissa riskhanteringsrelaterade skyldigheter ingår i elmarknadslagen och naturgasmarknadslagen finns det inga bestämmelser om skyldigheten för de leverantörer som definieras ovan att hantera risker som riktar sig mot kommunikationsnät och informationssystem. Lagarna innehåller inte heller bestämmelser om rapportering av störningar, bortsett från det som föreskrivs i elmarknadslagens 59 § om information till användarna. Därför bör det i elmarknadslagen och naturgasmarknadslagen tas in bestämmelser som ålägger leverantörer av samhällsviktiga tjänster att sörja för hanteringen av risker i samband med kommunikationsnät och informationssystem samt att rapportera betydande störningar i systemens informationssäkerhet till Energimyndigheten.

Transporter

Inom transportområdet har följande tjänster ovan definierats som sådana samhällsviktiga tjänster som avses i artikel 5.2 a i direktivet om nät- och informationssäkerhet:

1) flygtrafiktjänster,

2) trafikledningstjänster för järnvägstrafik,

3) fartygstrafikservice,

4) flygplatsförvaltning,

5) förvaltning av statens bannät,

6) hamnförvaltning, och

7) förvaltning av ett sådant ITS-system som avses i ITS-direktivet.

Flygtrafiktjänster, trafikledningstjänster för järnvägstrafik, fartygstrafikservice, förvaltning av statens bannät och förvaltning av sådana ITS-system som avses i ITS-direktivet kan i princip alltid anses vara beroende av nätverks- och informationssystem. Betydande störningar i dessa tjänsters informationssäkerhet kan få omfattande negativa konsekvenser för trafiksystemens säkerhet och kontinuitet. Därför ska alla leverantörer av dessa tjänster anses vara sådana leverantörer av samhällsviktiga tjänster som avses i direktivet om nät- och informationssäkerhet.

Förvaltningen av flygplatser och hamnar avviker till viss del från ovannämnda tjänster. Storleken på flygplatserna och hamnarna varierar. Därför varierar också deras beroende av nätverks- och informationssystem liksom hur stora konsekvenser en störning i informationssäkerheten kan få för tillgången till samhällsviktiga tjänster. Exempelvis hanterar de tio största hamnarna cirka 80 procent av sjötransporternas totala volym. Störningar som drabbar dessa hamnar kan få betydligt större konsekvenser är störningar som drabbar mindre hamnar. Därför bör inte alla hamninnehavare eller flygplatsoperatörer anses vara sådana leverantörer av samhällsviktiga tjänster som avses i direktivet om nät- och informationssäkerhet. Bedömningen av vem som ska omfattas av skyldigheterna bör framför allt göras med beaktande av kriterierna i artikel 6 i direktivet. Genom förordning av statsrådet kan det utfärdas närmare bestämmelser om hur skyldigheterna ska riktas till de leverantörer av samhällsviktiga tjänster som avses i direktivet.

Inom transportområdet kan således följande aktörer anses vara sådana leverantörer av samhällsviktiga tjänster som avses i direktivet om nät- och informationssäkerhet:

- leverantörer av flygtrafiktjänster,

- bolag som tillhandahåller trafikledningstjänster för järnvägstrafik och förvaltaren av statens bannät,

- leverantörer av fartygstrafikservice,

- förvaltare av sådana ITS-system som avses i III avd. 2 kap. 6 § i lagen om transportservice,

- innehavare av samhällsviktiga hamnar (fastställs genom förordning av statsrådet),

- operatörer av samhällsviktiga flygplatser (fastställs genom förordning av statsrådet).

Även om den lagstiftning som reglerar riskhanteringen för leverantörer av samhällsviktiga transporttjänster i sig också kan anses innehålla skyldigheter som tangerar kommunikationsnätens och informationssystemens säkerhet, ingår det inte i de gällande lagarna om de olika transportslagen några egentliga skyldigheter att sörja för hanteringen av säkerhetsrisker i samband med kommunikationsnät och informationssystem. Om informationssäkerheten äventyras kan även trafiksäkerheten eller de samhällsviktiga tjänsternas kontinuitet äventyras. Därför bör skyldigheterna att hantera risker i samband med kommunikationsnät och informationssystem och att till Trafiksäkerhetsverket anmäla betydande störningar i ett systems informationssäkerhet införas i luftfartslagen, i fråga om leverantörer av

-flygtrafiktjänster och flygplatsoperatörer,

-järnvägslagen, i fråga om bolag som tillhandahåller trafikledningstjänster för järnvägstrafik och förvaltaren av statens bannät,

- lagen om fartygstrafikservice, i fråga om leverantörer av fartygstrafikservice,

- lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet, i fråga om hamninnehavare,

- lagen om transportservice, i fråga om förvaltare av sådana ITS-system som avses i III avd. 2 kap. 6 § i lagen i fråga.

Bankverksamhet och finansmarknadsinfrastruktur

Såsom ovan konstaterats utgörs inom sektorn bankverksamhet och finansmarknadsinfrastruktur sådana samhällsviktiga tjänster som avses i artikel 5.2 a i direktivet om nät- och informationssäkerhet av kreditinstitutsverksamhet enligt kreditinstitutslagen och börsverksamhet enligt lagen om handel med finansiella instrument.

I kreditinstitutslagen finns heltäckande bestämmelser om skyldigheter som gäller den operativa riskhanteringen i samband med kreditinstitutverksamhet. Dessa skyldigheter har dessutom kompletterats med Finansinspektionens föreskrifter om hantering av operativa risker. Både i fråga om de skyldigheter som gäller riskhantering och de skyldigheter som gäller rapportering av störningar kan det anses att ovannämnda skyldigheter direkt uppfyller de krav i artikel 14 i direktivet som gäller säkerhet i nätverks- och informationssystem som används av leverantörer av samhällsviktiga tjänster. Dessa krav omfattar alla kreditinstitut med verksamhet i Finland.

Börsverksamhet kan anses vara beroende av nätverks- och informationssystem på det sätt som avses i direktivet om nät- och informationssäkerhet. Dessutom kan informationssäkerhetsrelaterade störningar som drabbar verksamheten få omfattande negativa konsekvenser för börsverksamheten. När det gäller finansmarknadsinfrastrukturer ska börsen därför anses vara en sådan leverantör av samhällsviktiga tjänster som avses i artikel 5 i direktivet.

När det gäller bedrivande av börsverksamhet ingår i 3 kap. (1 och 2.2 §) i regeringens proposition till riksdagen med förslag till lag om ändring av lagen om investeringstjänster, lag om handel med finansiella instrument och vissa lagar i samband med dem (RP 151/2017 rd) av den 26 oktober 2017 bestämmelser om riskhanteringskrav och rapportering av störningar. Skyldigheterna uppfyller de krav i artikel 14 i direktivet som gäller säkerhet i nätverks- och informationssystem som används av leverantörer av samhällsviktiga tjänster.

Hälso- och sjukvårdssektorn

Inom hälso- och sjukvårdssektorn utgörs sådana samhällsviktiga tjänster som avses i artikel 5.2 a i direktivet om nät- och informationssäkerhet av elektronisk behandling av klientuppgifter inom hälsovården och av underhåll och användning av produkter för hälso- och sjukvård vid tillhandahållandet av offentliga och privata tjänster inom social- och hälsovården.

I lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården och i lagen om produkter och utrustning för hälso- och sjukvård ingår informationssäkerhetsrelaterade skyldigheter i fråga om system som används för behandling av klientuppgifter, krav som gäller produkter för hälso- och sjukvård samt skyldigheter att anmäla störningar till tillsynsmyndigheten. Både i fråga om de skyldigheter som gäller riskhantering och de skyldigheter som

gäller rapportering av störningar kan det anses att ovannämnda skyldigheter uppfyller de krav i artikel 14 i direktivet som gäller säkerhet i nätverks- och informationssystem som används av leverantörer av samhällsviktiga tjänster.

Leverans och distribution av dricksvatten

Inom leverans och distribution av dricksvatten kan vattentjänster anses vara sådana samhällsviktiga tjänster som avses i artikel 5.2 a i direktivet om nät- och informationssäkerhet. Enligt lagen om vattentjänster sköter vattentjänstverken ett samhälles vattentjänster. Alla vattentjänstverk kan anses vara beroende av nätverks- och informationssystem på det sätt som avses i artikel 5.2 b i direktivet. Däremot kan inte alla incidenter som drabbar vattentjänstverk anses vara en sådan betydande störning som avses i artikel 5.2 c. Med stöd av kriterierna i artikel 6 i direktivet kan vattentjänstverk som levererar minst 5 000 kubikmeter vatten per dygn och anläggningar som levererar vatten till dessa anses vara sådana leverantörer av samhällsviktiga tjänster som avses i direktivet. Informationssäkerhetsrelaterade störningar som drabbar denna typ av tjänster utgör alltid en sådan betydande störning i tillhandahållandet av vattentjänster som avses i direktivet. I Finland finns det uppskattningsvis cirka 40 vattentjänstverk som levererar minst 5 000 kubikmeter vatten per dygn och deras kunder utgör mer än hälften av Finlands befolkning. Dessa vattentjänstverk har dessutom klassificerats som vattentjänstverk av kritisk betydelse för försörjningsberedskapen.

I lagen om vattentjänster ingår bestämmelser om vattentjänstverkens skyldigheter när det gäller att hantera säkerhetsrisker i samband med leveransen och distributionen av dricksvatten. Beredskapsskyldigheten enligt 15 a § i lagen om vattentjänster omfattar även skyldigheten att bereda sig inför risker som gäller informationssystem. I fråga om de skyldigheter som gäller riskhanteringen kan det anses att ovannämnda skyldigheter direkt uppfyller de krav i artikel 14 i direktivet som gäller säkerhet i nätverks- och informationssystem som används av leverantörer av samhällsviktiga tjänster. Däremot innehåller lagen om vattentjänster inte någon skyldighet att anmäla störningar i systemens informationssäkerhet till tillsynsmyndigheten, varför det i lagen bör införas en sådan särskild skyldighet för vattentjänstverk som levererar minst 5 000 kubikmeter vatten per dygn och anläggningar som levererar vatten till dessa.

Digital infrastruktur

När det gäller digital infrastruktur anses förvaltning av toppdomänregister vara en sådan samhällsviktig tjänst som avses i artikel 5.2 a i direktivet om nät- och informationssäkerhet. Informationssamhällsbalken innehåller skyldigheter för förvaltare av toppdomänregister att sörja för informationssäkerheten. Enligt lagen är Kommunikationsverket den myndighet som förvaltar ett register över domännamn under toppdomänen fi. Ålands landskapsregering förvaltar ett register över domännamn under toppdomänen ax. Skyldigheterna i informationssamhällsbalken kan anses uppfylla de krav i artikel 14 i direktivet som gäller säkerhet i nätverks- och informationssystem som används av leverantörer av samhällsviktiga tjänster.

Leverantörer av digitala tjänster

I den gällande lagstiftningen finns inga bestämmelser om hur sådana leverantörer av samhällsviktiga tjänster (molntjänster, sökmotorer, internetbaserade marknadsplatser) som avses i direktivet om nät- och informationssäkerhet ska hantera informationssäkerhetsrisker eller anmäla störningar i informationssäkerheten. Därför bör skyldigheterna att hantera risker i samband med kommunikationsnät och informationssystem och att till Kommunikationsverket anmäla betydande störningar i ett systems informationssäkerhet införas i informationssamhälls-

balken. I direktivet om nät- och informationssäkerhet åläggs medlemsstaterna inte någon motsvarande skyldighet att bedöma en tjänsts betydelse i fråga om tillhandahållandet av digitala tjänster, utan skyldigheterna i direktivet gäller alla tjänsteleverantör som omfattas av direktivets tillämpningsområde. I enlighet med vad som anges i direktivet bör skyldigheterna dock inte gälla små företag och mikroföretag.

2.3.5 Tillsyn över riskhanterings- och rapporteringsskyldigheter

Såsom ovan anges innehåller den gällande lagstiftningen skyldigheter i fråga om hanteringen av säkerhetsrisker och rapporteringen av incidenter och störningar. För övervakningen av dessa skyldigheter ansvarar en enligt lag behörig myndighet. Vanligen föreskrivs det också om tillsynsmyndigheternas befogenheter i fråga om skötseln av tillsynsuppgifterna, såsom rätten att få uppgifter och utföra inspektioner. Tillsynsmyndigheterna kan också meddela beslut som är bindande för deras tillsynsobjekt. Det vore därför naturligt att kommunikationsnätens och informationssystemens säkerhet övervakas av samma myndighet som övervakar efterlevnaden av andra säkerhetsrelaterade skyldigheter som gäller tillhandahållandet av en tjänst. Även den arbetsgrupp som stöder genomförandet av direktivet om nät- och informationssäkerhet har utifrån sin bedömning föreslagit att de så kallade sektorspecifika tillsynsmyndigheterna ska vara sådana behöriga myndigheter som avses i direktivet.

Det föreslås att krav på nät- och informationssäkerhet som gäller eldistributionen ska införas i elmarknadslagen medan krav som gäller naturgasdistributionen ska införas i naturgasmarknadslagen. Enligt lagen om tillsyn över el- och naturgasmarknaden övervakar Energimyndigheten att el- och naturgasmarknadslagarna följs, varför det vore naturligt att myndigheten också ska övervaka efterlevnaden av de skyldigheter som gäller informationssäkerheten.

För transporternas del har de säkerhetsrelaterade tillsynsuppgifterna i fråga om olika transportslag huvudsakligen koncentrerats till Trafiksäkerhetsverket. Vissa leverantörer av transportservice måste dessutom redan i dag anmäla vissa incidenter och störningar som äventyrar trafiksäkerheten till Trafiksäkerhetsverket. Informationssäkerhetsrelaterade skyldigheter som gäller samhällsviktiga tjänster inom transportområdet införs i speciallagar om de olika transportslagen, varför det är motiverat att Trafiksäkerhetsverket ges behörighet att övervaka efterlevnaden av dessa skyldigheter.

När det gäller banksektorn övervakar Finansinspektionen med stöd av den gällande lagstiftningen efterlevnaden av de skyldigheter i fråga om systemens informationssäkerhet som ingår i den operativa riskhanteringen. Kreditinstituten ska också anmäla störningar i informationssäkerheten till Finansinspektionen.

Tillstånds- och tillsynsverket för social- och hälsovården övervakar den elektroniska behandlingen av klientuppgifter inom hälsovården och kvalitetskraven i fråga om produkter för hälso- och sjukvård. Tjänsteleverantörerna ska också anmäla vissa informationssäkerhetsrelaterade störningar till verket.

I lagen om vattentjänster ingår bestämmelser om vattentjänstverkens skyldigheter när det gäller att hantera säkerhetsrisker i samband med leveransen och distributionen av dricksvatten. Tillsynsmyndigheter enligt lagen om vattentjänster är närings-, trafik- och miljöcentralen samt den kommunala miljövårdsmyndigheten och den kommunala hälsoskyddsmyndigheten, var och en av dem inom sitt ansvarsområde. Inom sektorn för leverans och distribution av dricksvatten finns det inte någon motsvarande gemensam sektorspecifik tillsynsmyndighet som inom andra sektorer som omfattas av direktivet. För att säkerställa kontinuiteten i distribution-

en av dricksvatten och för att myndigheterna ska kunna utöva effektiv tillsyn bör det finnas bestämmelser om att störningar i informationssäkerheten ska anmälas till närings-, trafik- och miljöcentralen.

De ovannämnda tillsynsmyndigheternas behörighet inom olika sektorer beror på de lagar i vilka behörigheten regleras, varför den varierar. En myndighet har behörighet att övervaka att de skyldigheter som gäller informationssäkerheten fullgörs och att ålägga en aktör att åtgärda lagstridig verksamhet endast om detta föreskrivs i lag. Om behörigheten kan föreskrivas allmänt (t. ex. att Energimyndigheten övervakar att skyldigheterna enligt elmarknadslagen fullgörs) eller specifikt (att en viss myndighet övervakar skyldigheter som föreskrivs i en viss paragraf). Det ska även finnas särskilda bestämmelser om en myndighets rätt att förstärka sitt beslut med administrativa påföljder, exempelvis vite.

För att säkerställa tillräckliga befogenheter behövs det vissa preciseringar av bestämmelserna om tillsynsmyndigheternas lagstadgade uppgifter, myndigheternas rätt till information, förutsättningarna för behandling av uppgifter och de administrativa påföljderna.

3 Målsättning och de viktigaste förslagen

3.1 Målsättning

Digitaliseringen innebär en industriell och samhällelig omvälvning och en global, allt snabbbare fortskridande megatrend. Den revolutionerar verksamhetssätten inom alla delar av livet. Införandet av digitala verksamhetssätt kan emellertid leda till att förtroendet för verksamhetssätten minskar. Detta medför att fördelarna med den digitala utvecklingen inte kan utnyttjas till fullo. Syftet med propositionen är därför att öka medborgarnas och företagens förtroende för de digitala verksamhetssätten och att förbättra informationssäkerheten för samhällsviktiga tjänster som är av betydelse för medborgarna. Detta är viktigt eftersom dessa tjänster i allt högre grad är beroende av kommunikationsnät och informationssystem.

I propositionen föreslås för vissa leverantörer av samhällsviktiga tjänster en skyldighet att hantera riskerna i samband med kommunikationsnät och informationssystem. Målet är att säkerställa att tjänsteleverantörerna inkluderar hanteringen av informationssäkerhetsrisker i den allmänna hanteringen av säkerhetsrisker i verksamheten.

Störningar i informationssäkerheten kan äventyra tjänstens säkerhet eller kontinuitet. I den gällande lagstiftningen föreskrivs redan om skyldigheter som omfattar samhällsviktiga tjänster, genom vilka man kan säkerställa att tjänsterna tillhandahålls på ett säkert sätt. De behöriga myndigheterna övervakar att dessa skyldigheter fullgörs. Målet med propositionen är att öka den behöriga tillsynsmyndighetens kännedom om störningar i kommunikationsnät och informationssystem, vilka kan äventyra den kvalitet som enligt lag förutsätts av tjänsten, tjänstens säkerhetsnivå eller exempelvis en störningsfri tjänst. Målet med propositionen är också att göra det möjligt för de behöriga myndigheterna att behandla och bedöma betydelsen av störningar i informationssäkerheten, så att nödvändiga korrigerande åtgärder kan vidtas.

3.2 Alternativ

Under beredningen har olika alternativ för genomförandet utvärderats genom att de jämförts mot målen i regeringsprogrammet och i den informationssäkerhetsstrategi som godkänts i enlighet med genomförandeplanen för regeringsprogrammet. De olika alternativen utvärderades

av den arbetsgrupp som inrättats som stöd för genomförandet av direktivet om nät- och informationssäkerhet.

I samband med genomförandet av direktivet utvärderades möjligheten att stifta en helt ny speciallag om nät- och informationssäkerhet. Alternativet utvärderas även av den arbetsgrupp som tillsatts av ministeriet. Som stöd för arbetsgruppens arbete gjordes en utredning av vilka informationssäkerhetsrelaterade skyldigheter eller andra riskhanterings- och säkerhetsrelaterade skyldigheter de sektorer som omfattas av tillämpningsområdet för direktivet om nät- och informationssäkerhet för närvarande har enligt den gällande nationella lagstiftningen, EU-lagstiftningen och internationella förpliktelser. En av de viktigaste slutsatserna av utredningen var att den nationella lagstiftningen om informationssäkerhet är fragmenterad. Det finns relativt många säkerhets- och riskhanteringsskyldigheter för de sektorer som omfattas av direktivets tillämpningsområde, men även denna lagstiftning är mycket splittrad. För merparten av de sektorer som omfattas av tillämpningsområdet finns det vissa skyldigheter som gäller riskhanteringen eller nivån på informationssäkerheten. De säkerhetsrelaterade skyldigheterna är dock för det mesta kopplade till enskilda funktioner, och inte direkt till en hel sektor eller en viss typ av aktör. De skyldigheter som gäller riskhanteringen är delvis mycket fritt formulerade så att det av bestämmelsen inte direkt framgår om en viss skyldighet även kan anses gälla informationssystemens säkerhet. Nästan alla sektorer omfattas av rapporteringsskyldigheter, men endast några sektorer är skyldiga att rapportera störningar i informationssäkerheten. Utifrån den utredning som gjordes om den sektorspecifika lagstiftningen och arbetsgruppens bedömning och med beaktande av de mål som fastställts för det nationella genomförandet ansåg arbetsgruppen att utgångspunkten ska vara att skyldigheterna i direktivet införlivas i den nationella sektorspecifika lagstiftningen. Att genomföra direktivet i form av en separat speciallag skulle enligt arbetsgruppen inte på samma sätt uppfylla de mål som ställts för genomförandet av direktivet, utan det skulle i stället kunna medföra överlappande skyldigheter och rapporteringspraxis.

Dessutom kan inte hanteringen av informationssäkerhetsrisker anses avvika från övrig riskhantering på ett sådant sätt att en separat lag kan anses befogad. I fråga om flera av de sektorer som omfattas av direktivets tillämpningsområde har bestämmelserna samlats i en sektorspecifik lag. Till exempel finns bestämmelser om skyldigheter som gäller eldistributionen huvudsakligen i elmarknadslagen medan ordnandet av vattentjänster huvudsakligen regleras i lagen om vattentjänster. Om en separat lag skulle stiftas om de skyldigheter som gäller informationssäkerheten skulle risken för överlappande lagstiftning öka, och det skulle ge en bild av att hanteringen av informationssäkerhetsrisker utgör en separat helhet. För de tjänsteleverantörer som omfattas av direktivets tillämpningsområde blir det mer åskådligt om tillsynen över de skyldigheter som gäller hanteringen av informationssäkerhetsrisker och rapporteringen av störningar inte delas upp i olika lagar, vilket kan ge upphov till överlappande reglering.

Ett annat alternativ som undersöktes var att föra in bestämmelserna om nät- och informationssäkerhet i informationssamhällsbalken. Detta ansågs emellertid inte vara något bra alternativ eftersom det för de leverantörer av samhällsnyttiga tjänster som omfattas av direktivets tillämpningsområde, t.ex. innehavare av eldistributionsnät, kan vara svårt att förstå att informationssamhällsbalken innehåller skyldigheter som gäller dem. Denna lösning skulle också ha avvikit från den lösning som redan tillämpas inom exempelvis finanssektorn, där de skyldigheter som gäller informationssäkerheten har inkluderats i den sektorspecifika speciallagstiftningen som en del av hanteringen av operativa risker.

Mot bakgrund av det som anges ovan ansågs det bästa alternativet för genomförandet av direktivet vara att inkludera de skyldigheter som gäller informationssäkerheten i den sektorspecifika speciallagstiftningen.

Till Kommunikationsverkets särskilda uppgifter hör allmänna uppgifter som främjar informationssäkerheten. Vid beredningen av lagförslaget utreddes också om Kommunikationsverket skulle kunna vara en i direktivet avsedd behörig myndighet inom alla sektorer som omfattas av direktivets tillämpningsområde. Såsom ovan anges finns det emellertid redan flera tillsynsmyndigheter i Finland inom direktivets tillämpningsområde, varav de viktigaste är Energimyndigheten, Finansinspektionen, Trafiksäkerhetsverket, Tillstånds- och tillsynsverket för social- och hälsovården, närings-, trafik- och miljöcentralerna samt Kommunikationsverket. I Finland har inte endast en myndighet, t.ex. Kommunikationsverket, utsetts att övervaka efterlevnaden av de skyldigheter som gäller hanteringen av informationssäkerhetsrisker. Däremot har tillsynsmyndigheterna vanligen behörighet att utöva tillsyn över de verksamheter som fastställts för dem i lag. Till exempel övervakar Finansinspektionen att dess tillsynsobjekt fullgör skyldigheterna i fråga om den operativa riskhanteringen. Dessa omfattar även de säkerhetskrav som fastställts för informationssystemen. Tillsynsobjekten anmäler också eventuella störningar i informationssäkerheten till Finansinspektionen. Vanligen föreskrivs det också om tillsynsmyndigheternas befogenheter i fråga om skötseln av tillsynsuppgifterna, såsom rätten att få uppgifter och utföra inspektioner. Tillsynsmyndigheterna kan också meddela beslut som är bindande för deras tillsynsobjekt. Om de myndighetsuppgifter som gäller hanteringen av informationssäkerhetsrisker i fortsättningen skulle koncentreras till en enda myndighet skulle detta kunna leda till överlappningar i tillsynsbefogenheterna och i tjänsteleverantörernas rapporteringsskyldigheter. I och med att tjänster digitaliseras i hela samhället behöver dessutom myndigheterna inom varje sektor större insikt i informationssäkerhetens betydelse för den verksamhet som de övervakar. I annat fall kan informationssäkerheten bli ett värde i sig och inte en del av tillhandahållandet och övervakningen av tjänsterna som planerats med tanke på tjänsternas säkerhet och kontinuitet. Ett annat problem skulle vara att det inte alltid tydligt framgår om en störning i en tjänst beror på t.ex. en störning i ett informationssystems säkerhet eller om det är fråga om en annan säkerhetsrelaterad störning. Förutom till informationssäkerheten kan störningar t.ex. i fråga om transporter sannolikt även ha nära anknytning till trafiksäkerheten. Det vore därför ändamålsenligt om den behöriga myndighetens uppgifter sköts av den myndighet som enligt den gällande lagstiftningen redan övervakar de skyldigheter som gäller hanteringen av säkerhetsrisker inom dess ansvarsområde.

När det gäller den nationella kontaktpunkten enligt direktivet om nät- och informationssäkerhet har man vid beredningen avvägt om uppgifterna ska skötas av statsrådets lägescentral eller av Kommunikationsverket. Enligt 12 § 7 punkten i reglementet för statsrådet hör till statsrådets kanslis ansvarsområde statsrådets gemensamma lägesbild, beredskap och säkerhet samt den allmänna samordningen av hanteringen av störningssituationer. Därför skulle även statsrådets lägescentral kunna vara gemensam kontaktpunkt. Enligt den bedömning som den arbetsgrupp som stöder genomförandet av direktivet om nät- och informationssäkerhet har gjort är den gemensamma kontaktpunktens uppgifter dock så operativa till sin karaktär och dess verksamhet så nära knuten till de uppgifter som direktivets CSIRT-enheter har att det naturliga vore att Kommunikationsverket är en sådan gemensam kontaktpunkt som avses i direktivet.

3.3 De viktigaste förslagen

Det föreslås att det i luftfartslagen, järnvägslagen, lagen om fartygstrafikservice, lagen om sjöfartskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet, lagen om transportservice, elmarknadslagen, naturgasmarknadslagen och lagen om vattentjänster in-

förs bestämmelser om skyldigheten för leverantörer av samhällsviktiga tjänster att sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som de använder och bestämmelser om skyldigheten att till tillsynsmyndigheten och i vissa fall till allmänheten rapportera allvarliga incidenter med anknytning till informationssäkerheten. Lagarna innehåller inte några närmare bestämmelser om hur riskhanteringen ska ordnas, utan till denna del kan aktörerna välja de metoder för att hantera informationssäkerhetsriskerna som är bäst lämpade för deras affärsverksamhet, system och övriga riskhantering.

Skyldigheterna enligt luftfartslagen gäller leverantörer av flygtrafiktjänster samt operatörer av samhällsviktiga flygplatser. Skyldigheterna enligt järnvägslagen gäller förvaltaren av statens bannät samt bolag som tillhandahåller trafikledningstjänster. Skyldigheterna enligt lagen om fartygstrafikservice gäller leverantörer av fartygstrafikservice. Skyldigheterna enligt lagen om sjöfartskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet gäller innehavare av samhällsviktiga hamnar. Skyldigheterna enligt lagen om transportservice gäller förvaltare av intelligenta trafiksystem. Skyldigheterna enligt elmarknadslagen gäller nätinnehavare. Skyldigheterna enligt naturgasmarknadslagen gäller överföringsnätsinnehavare och skyldigheterna enligt lagen om vattentjänster vattentjänstverk som levererar minst eller tar emot avloppsvatten 5 000 kubikmeter vatten per dygn. Bestämmelserna i lagen om vattentjänster kompletteras samtidigt så att de nämnda verken utöver betydande störningar i informationssäkerheten även ska meddela andra betydande störningar i vattentjänsterna till myndigheten.

I informationssamhällsbalken införs motsvarande skyldigheter i fråga om vissa leverantörer av digitala tjänster. Skyldigheterna enligt informationssamhällsbalken gäller tillhandahållare av internetbaserade marknadsplatser, sökmotortjänster och molntjänster.

Vidare föreskrivs om tillsynsmyndigheternas rätt att vid behov samarbeta kring tillsynen över de skyldigheter som gäller informationssäkerheten och att vid behov utbyta sekretessbelagd information. För tillsynsmyndigheterna föreskrivs också skyldigheten att vid behov informera andra EU-medlemsstater om störningar i informationssäkerheten, om störningen har en betydande inverkan på tillhandahållandet av samhällsviktiga tjänster i medlemsstaten i fråga. För Kommunikationsverket föreskrivs skyldigheten att vid behov samarbeta med de myndigheter i de övriga medlemsstaterna som övervakar nät- och informationssäkerheten, med enheterna för hantering av it-säkerhetsincidenter och med den samarbetsgrupp som avses i artikel 10 i EU:s direktiv om nät- och informationssäkerhet.

4 Propositionens konsekvenser

4.1 Ekonomiska konsekvenser

Propositionen har inga betydande ekonomiska konsekvenser för sådana leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster som avses i direktivet om nät- och informationssäkerhet och i denna proposition. Även om de skyldigheter som föreslås för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster när det gäller hanteringen av informationssäkerhetsrisker och rapporteringen av störningar är nya, ingår redan liknande riskhanteringsskyldigheter i den gällande lagstiftningen. Dessutom får tjänsteleverantörerna själva avgöra vilka konkreta åtgärder de vidtar för att ordna riskhanteringen. Detta gör det möjligt för leverantörerna att i sin övergripande riskhantering inkludera sådana åtgärder som de nya skyldigheterna kräver. Rapporteringen av störningar i informationssäkerheten kan för tjänsteleverantörerna medföra kostnader som t.ex. hänför sig till informationssystemen. Med beaktande av anmälningsskyldigheterna i den gällande lagstiftningen kan de nya rappor-

teringsskyldigheter som nu föreslås dock inte anses ha några betydande ekonomiska konsekvenser för tjänsteleverantörerna.

It-säkerhetsincidenter kan få omfattande negativa ekonomiska konsekvenser, framför allt om ett företags verksamhet avbryts eller uppgifter som är viktiga för verksamheten försvinner. Den föreslagna skyldigheten att sörja för hanteringen av säkerhetsrisker i samband med kommunikationsnät och informationssystem förbättrar tjänsteleverantörernas beredskap för kränkningar av informationssäkerheten. Dessutom ökar skyldigheten att anmäla kränkningar av informationssäkerheten kunskapen om sådana kränkningar och skapar förutsättningar för att effektivare sprida information om exempelvis sårbarheter i informationssäkerheten, vilket är till nytta för alla aktörer och förbättrar informationssäkerheten.

4.2 Konsekvenser för myndigheterna

I propositionen föreslås att flera sektorspecifika tillsynsmyndigheter ska tilldelas uppgifter som rör övervakning av informationssäkerheten. Efterlevnaden av de skyldigheter som gäller leverantörer av digitala tjänster ska övervakas av Kommunikationsverket, de skyldigheter som gäller tjänsteleverantörer inom transportsektorn av Trafiksäkerhetsverket, skyldigheterna inom finanssektorn av Finansinspektionen, skyldigheterna inom energisektorn av Energimyndigheten och de skyldigheter som gäller leverans och distribution av dricksvatten av närings-, trafik- och miljöcentralen. Myndigheternas uppgift är att övervaka tjänsteleverantörernas hantering av informationssäkerhetsrisker och att ta emot anmälningar om störningar i informationssäkerheten. Den gällande sektorspecifika lagstiftningen innehåller, såsom angetts i beskrivningen av nuläget, skyldigheter som liknar de nu föreslagna riskhanterings- och rapporteringsskyldigheterna och som övervakas av de sektorspecifika tillsynsmyndigheterna. De förslag som läggs fram kan därför inte anses orsaka betydande resursbehov eller kostnader för tillsynsmyndigheterna, utan utgångspunkten är att uppgifterna kan skötas med nuvarande resurser.

För Kommunikationsverket föreslås förutom tillsynsuppgifter vissa allmänna informationssäkerhetsrelaterade uppgifter i enlighet med direktivet om nät- och informationssäkerhet. Till dessa uppgifter hör att vara CSIRT-enhet inom de sektorer som anges i direktivets bilagor II och III och att vara gemensam kontaktpunkt. CSIRT-enhetens uppgifter motsvarar i princip Kommunikationsverkets nuvarande lagstadgade uppgifter, vilka inte utökas nämnvärt genom förslaget. Den gemensamma kontaktpunktens uppgifter är nya och innebär att stå i kontakt med andra EU-medlemsstater och att lämna in sammanfattande rapporter till den samarbetsgrupp som avses i direktivet. De kostnader som uppgifterna orsakar är inte betydande, utan utgångspunkten är att uppgifterna kan skötas med nuvarande resurser.

4.3 Samhälleliga konsekvenser

Genom propositionen förbättras informationssäkerheten för samhällsviktiga tjänster och vissa digitala tjänster. En högre säkerhetsnivå är viktig för att säkerställa kontinuiteten i de samhällsviktiga tjänsterna, för att förbättra säkerheten i samhället och framför allt för att öka medborgarnas och företagens förtroende för digitala verksamhetssätt.

Den föreslagna skyldigheten att hantera informationssäkerhetsrisker i samband med samhällsviktiga tjänster bidrar till att förbättra säkerheten för dessa tjänster och beredskapen för störningar i informationssäkerheten. Sådana störningar är t.ex. dataintrång, nätfiske och andra it-säkerhetsincidenter, såsom omfattande överbelastningsattacker eller vitt utbredda utpressningsvirus, som under 2016 och 2017 har orsakat betydande störningar även i tillgången till samhällsviktiga tjänster. I Storbritannien spreds exempelvis i maj 2017 ett utpressningsvirus

till ett stort antal datorer vid hälsovårdsanstalterna (National Health Service), vilket ledde till att tusentals patientbesök och operationer måste avbokas.

Den föreslagna skyldigheten att anmäla störningar i informationssäkerheten till tillsynsmyndigheterna förbättrar tillsynsmyndigheternas lägesbild över informationssäkerheten och ökar olika sektorers kunskaper om informationssäkerhet. Genom att myndigheternas kunskaper och lägesbild förbättras ökar informationssäkerheten i hela samhället liksom förmågan att stå emot störningar i informationssäkerheten.

Kommunikationsministeriet kommer att bedöma vilka konsekvenser den föreslagna lagstiftningen fått för informationssäkerheten för samhällsviktiga tjänster två år efter det att lagstiftningen trätt i kraft.

5 Beredningen av propositionen

5.1 Beredningsskeden och beredningsmaterial

I oktober 2016 tillsatte kommunikationsministeriet en arbetsgrupp som stöder genomförandet av direktivet om nät- och informationssäkerhet. Arbetsgruppens uppgift var att stödja kommunikationsministeriet i beredningen av genomförandet av direktivet, att utvärdera olika regleringsalternativ och att främja det samarbete som direktivet förutsätter mellan de olika sektorer som omfattas av tillämpningsområdet. Förutom kommunikationsministeriet var följande aktörer representerade i arbetsgruppen: arbets- och näringsministeriet, finansministeriet, social- och hälsovårdsministeriet, Kommunikationsverket, Trafiksäkerhetsverket, Trafikverket, Försörjningsberedskapscentralen, Finansinspektionen, Energimyndigheten, Tillstånds- och tillsynsverket för social- och hälsovården, FiCom ry, Finlands Näringsliv EK, Teknologiindustrin rf, Finsk Energiindustri rf och Finansbranschens Centralförbund FC. Miljöministeriet utsåg inte någon medlem i arbetsgruppen. Arbetsgruppen sammanträdde nio gånger. Fem av sammanträdena delades upp sektorsvis enligt följande: transportsektorn, finanssektorn, hälso- och sjukvårdssektorn, energisektorn och den digitala sektorn. Under de sektorsvisa sammanträdena fokuserade man på att utvärdera den gällande lagstiftningen om hantering av säkerhetsrisker inom de olika sektorerna och olika alternativ för genomförandet av direktivet om nät- och informationssäkerhet. I sin slutrapport (kommunikationsministeriets publikationer 9/2017) från april 2016 föreslog arbetsgruppen allmänna riktlinjer för genomförandet av direktivet.

Utöver sammanträdena i arbetsgruppen fördes bilaterala diskussioner med finansministeriet, social- och hälsovårdsministeriet, jord- och skogsbruksministeriet samt arbets- och näringsministeriet. I maj 2017 skickades också en begäran om åtgärder till ministerierna, som gällde definitionen av leverantörer av samhällsviktiga tjänster och ordnandet av myndighetstillsynen inom olika förvaltningsområden.

För intressentgrupperna ordnade kommunikationsministeriet dessutom i december 2016 ett öppet diskussionsmöte om genomförandet av direktivet. Beredningen och genomförandet av direktivet har också presenterats vid många evenemang inom de olika sektorerna, för ledningsgruppen för den digitala säkerheten inom den offentliga förvaltningen (VAHTI) och för den arbetsgrupp som tillsattes i augusti 2015 för att samordna genomförandet av spetsprojektet för att skapa en tillväxtmiljö för digital affärsverksamhet.

Under beredningen samarbetade ministeriet på EU-nivå med de andra medlemsstaterna inom ramen för den samarbetsgrupp och det CSIRT-nätverk som nämns i direktivet om nät- och informationssäkerhet.

5.2 Remissyttranden och hur de har beaktats

Utkastet till proposition har beretts vid kommunikationsministeriet. Kommunikationsministeriet sände förslaget på remiss i oktober 2017. Sammanlagt 27 yttranden lämnades in. Yttranden lämnades in av justitieministeriet, jord- och skogsbruksministeriet, social- och hälsovårdsministeriet, arbets- och näringsministeriet, finansministeriet, inrikesministeriet, landskapet Åland, Trafiksäkerhetsverket, Kommunikationsverket, Institutet för hälsa och välfärd, Finansinspektionen, Tillstånds- och tillsynsverket för social- och hälsovården, sekretariatet för Säkerhetskommittén, Finlands Kommunförbund, Logistiikkayritysten liitto, CSC-Tieteen tietotekniikan keskus, OP Gruppen, Finlands Vattenverksförening, Suomen Varustamot, Finanssiala ry, Finrail Oy, Tietoliikenteen ja tietotekniikan keskusliitto, Finlands Näringsliv, Suomen Satamaliitto, Teknologiindustrin rf, Tieto Abp, Microsoft Oy och Nasdaq Helsinki Oy. I sju av yttrandena hade remissinstansen inga egentliga kommentarer till propositionen.

Alla remissinstanser ställde sig positiva till de allmänna målen för propositionen och genomförandet av direktivet om nät- och informationssäkerhet liksom till de genomförandealternativ som valts. Remissinstanserna var särskilt nöjda med det sektorsvisa tillvägagångssättet och med att man vid direktivets nationella genomförande har strävat efter att undvika ytterligare nationell reglering. Propositionens definitioner av leverantörer av samhällsviktiga tjänster ansågs till största delen vara motiverade.

I yttrandena föreslogs vissa enstaka ändringar och kompletteringar till de föreslagna lagarna samt kompletteringar till motiveringarna. Förslagen gällde framför allt den föreslagna definitionen av molntjänst i informationssamhällsbalken, definitionen av leverantörer av samhällsviktiga tjänster inom finanssektorn, myndigheternas rätt att utbyta sekretessbelagd information samt myndigheternas verksamhet i fråga om leverans och distribution av dricksvatten. En närmare redogörelse för responsen i yttrandena finns i det sammandrag av remissvaren som publicerats på kommunikationsministeriets webbplats.

Utifrån responsen i yttrandena har den föreslagna regleringen av vattentjänster vidareberetts i samarbete med jord- och skogsbruksministeriet, social- och hälsovårdsministeriet, Tillstånds- och tillsynsverket för social- och hälsovården samt Finlands Vattenverksförening. Även förslagen om myndigheternas rätt att lämna ut sekretessbelagd information till varandra har kompletterats. Förutom i lagförslagen har det även gjorts behövliga kompletteringar i motiveringarna utifrån den inkomna responsen.

6 Samband med andra propositioner

Ämbetsverksreformen inom kommunikationsministeriets förvaltningsområde och bolagiseringen av Trafikverkets trafikledningsuppgifter

Den 25 april 2017 tillsatte kommunikationsministeriet ett projekt för att bereda regeringens proposition till riksdagen med förslag till lagar om Trafik- och X-verk samt lagstiftning och förordningar som har samband dem och regeringens proposition till riksdagen med förslag till lag om bolagisering av Trafikverkets trafikledningsfunktion. Syftet med projektet är att föra samman Trafiksäkerhetsverket och Kommunikationsverket samt Trafikverkets uppgifter till ett ämbetsverk, dock på så sätt att Trafikverkets trafikledningsfunktion bolagiseras till ett av staten helägt bolag med specialuppgifter och Trafikverket även i fortsättningen är den myndighet som ansvar för trafikledarna.

Syftet med reformen är att förbättra förvaltningsområdets förmåga att svara på förändringar i kundernas behov och i omvärlden, att utveckla och stärka den strategiska styrningen av förvaltningsområdet och att uppnå synergifördelar. Ett annat syfte är att ytterligare öka förvaltningens produktivitet och effektivitet genom en mångsidigare och effektivare resursanvändning.

Bolagiseringen av trafikledningsfunktionerna siktar dessutom på att förtydliga myndighetsuppgifterna och göra regleringen inom trafik- och transportsektorn smidigare. Genom reformen vill man också främja utnyttjandet av information som rör trafik och transport inom den privata sektorn och stödja uppkomsten av ny affärsverksamhet. Målet är att den information som samlas in genom trafikledningen ska komma till nytta för hela samhället på ett mer effektivt sätt än hittills.

6.1 Propositionens samband med Ålands självstyrelse

Enligt 18 § 21 punkten i självstyrelselagen för Åland (1144/1991) har landskapet lagstiftningsbehörighet i fråga om vägar och kanaler, vägtrafik, spårbunden trafik, båttrafik och farleder för den lokala sjötrafiken.

Enligt 18 § 22 punkten i självstyrelselagen för Åland har landskapet med vissa begränsningar lagstiftningsbehörighet i fråga om näringsverksamhet. Landskapet Ålands behörighet i el- och energifrågor har i samband med lagstiftningskontrollen av ellagen för landskapet Åland (ÅFS 1982:38) härletts från 13 § 1 mom. 9 punkten i den tidigare självstyrelselagen för Åland (670/1951), som motsvarade 18 § 22 punkten om näringsverksamhet i den gällande självstyrelselagen för Åland (RP 73/1990 rd s. 69). Den fördelning av behörigheten mellan riket och landskapet som föreskrivs i självstyrelselagen innebär att elmarknadslagen inte tillämpas i landskapet Åland till den del landskapet har lagstiftningsbehörighet i frågor som gäller elmarknaden.

Enligt 27 § i självstyrelselagen för Åland har landskapet lagstiftningsbehörighet i fråga om handelssjöfart, luftfart samt statsmyndigheternas organisation och verksamhet.

DETALJMOTIVERING

1 Lagförslag

1.1 Lagen om ändring av informationssamhällsbalken

247 a *§. Skyldighet för den som tillhandahåll av internetbaserade marknadsplatser, sökmotortjänster och molntjänster att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem.* Den föreslagna paragrafen är ny. I paragrafen föreskrivs det om skyldigheten för tillhandahållare av internetbaserade marknadsplatser, sökmotortjänster och molntjänster att sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som de använder.

Med en internetbaserad marknadsplats enligt 1 mom. avses en sådan tjänst enligt artikel 4.17 i direktivet om nät- och informationssäkerhet genom vilken användarna kan ingå internetbaserade köpeavtal eller tjänsteavtal med näringsidkare. Användarna kan vara sådana konsumenter som anges i artikel 4.1 a i Europaparlamentets och rådets direktiv 2013/11/EU eller sådana näringsidkare som anges i artikel 4.1 b i samma direktiv. Tjänsten kan erbjuda möjlighet att ingå avtal med näringsidkare på den egna webbplatsen eller på en annan webbplats som använder de databehandlingstjänster som den internetbaserade marknadsplatsen tillhandahåller. Definitionen omfattar inte onlinetjänster som endast används som en länk till en tredje parts tjänster, via vilka ett avtal till sist kan ingås. Definitionen omfattar således inte onlinetjänster som jämför priser på vissa varor eller tjänster från olika näringsidkare och sedan leder användaren vidare till den näringsidkare som valts för köp av varan. Datatjänster som tillhandahålls av internetbaserade marknadsplatser kan inbegripa behandling av transaktioner, sammanställning av data eller profilering av användare. Internetbaserade marknadsplatser är exempelvis applikationsbutiker, som fungerar som onlinebutiker och möjliggör digital distribution av applikationer eller programvara från tredje part, via antingen en webbplats eller en applikation. Som internetbaserade marknadsplatser betraktas inte företag som säljer sina varor eller tjänster direkt till konsumenter eller näringsidkare via internet.

Med sökmotortjänst avses en tjänst enligt artikel 4.18 i direktivet om nät- och informationssäkerhet som utifrån användarens sökning letar fram belägg bland ett icke definierat antal webbplatser och som sökresultat ger användaren länkar till olika webbplatser. Med icke definierat antal webbplatser avses att sökningen kan riktas till ett obegränsat antal webbplatser eller alternativt begränsas till exempelvis webbplatser på ett visst språk. Sökningen kan dock inte begränsa sig till innehållet på bara en enskild webbplats, oberoende av om sökfunktionen erbjuds av en utomstående sökmotor. Definitionen omfattar inte heller onlinetjänster som jämför priset på vissa varor eller tjänster från olika näringsidkare och sedan leder användaren vidare till den näringsidkare som valts för köp av varan.

Med molntjänst avses en tjänst enligt artikel 4.19 i direktivet om nät- och informationssäkerhet som möjliggör tillgång till delbara datatekniska resurser över nätet. Dessa datatekniska resurser omfattar resurser i form av nätverk, servrar eller annan infrastruktur, lagring, applikationer och tjänster. Med delbara resurser avses datatekniska resurser som leverantören av molntjänster fördelar på ett flexibelt sätt, oberoende av resursernas geografiska läge, enligt fluktuationerna i efterfrågan, och som avsätts och utnyttjas beroende på efterfrågan för att tillgängliga resurser snabbt ska kunna utökas och minskas i takt med arbetsbördan. Vidare tillhandahålls tjänsterna flera användare som delar en gemensam åtkomst till tjänsten, där behandlingen dock genomförs separat för varje användare, även om tjänsten tillhandahålls från

samma elektroniska utrustning. En molntjänst kan innefatta exempelvis anskaffning av programvara i form av en tjänst (Software as a Service), anskaffning av en server eller lagringsutrymme i form av en tjänst (Infrastructure as a Service) eller tillhandahållande av plattformar för applikationsutveckling i form av en tjänst (Platform as a Service).

Ett informationssystem enligt *1 mom*. kan bestå t.ex. av sådan teleterminalutrustning som avses i 3 § 25 punkten i denna lag eller av data som förvaras, behandlas, söks eller överförs i dessa system. De kommunikationsnät och informationssystem som avses i paragrafen består framför allt av privata kommunikationsnät och informationssystem som antingen förvaltas av tjänsteleverantörens interna it-personal eller vilkas säkerhet har lagts ut på entreprenad. Med riskhantering avses lämpliga organisatoriska och tekniska åtgärder som vidtas för att säkerställa kommunikationsnätens och informationssystemens förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade eller överförda eller behandlade uppgifter eller hos andra tjänster som erbjuds genom eller är tillgängliga via dessa system. Riskhanteringen ska innefatta lämpliga åtgärder för att förebygga och minimera den effekt som informationssäkerhetsrelaterade störningar i de system som används vid tillhandahållandet av tjänsterna har på tjänsternas kontinuitet. Åtgärderna inom riskhanteringen kan bestå av t.ex. att upprätta säkerhetsplaner, testa dessa i praktiken eller utföra kvalitetsrevisioner, använda dataskydds- och krypteringsprodukter samt iaktta vissa välkända standarder för informationssäkerhet, såsom ICO/IEC 27001:2013. Med risk avses en rimligen identifierbar omständighet eller händelse med en potentiell negativ inverkan på säkerheten i kommunikationsnät och informationssystem. Riskhanteringen ska dokumenteras. Målet med dokumenteringen är att främja en konsekvent riskhantering och aktörens medvetna lösningar på hur de åtgärder som behövs för riskhanteringen ska dimensioneras. Dokumenteringen gör det också möjligt för myndigheterna att vid behov i efterskott bedöma huruvida skyldigheterna enligt denna paragraf har iakttagits. Dokumenteringen kan bestå t.ex. av skriftliga riskbedömningar, säkerhetsföreskrifter eller handlingsplaner eller av intyg över utförda säkerhetsrevisioner. Dokumenteringen kan inkluderas i andra planer för hantering av säkerhetsrisker eller beredskapsplaner.

Enligt *2 mom*. ska det vid riskhanteringen tas hänsyn till systems och anläggningars säkerhet, hantering av kränkningar av informationssäkerheten och störningar, hantering av driftskontinuitet, övervakning, revision och testning samt efterlevnad av internationella standarder. Närmare bestämmelser om parametrarna enligt 2 mom. finns i kommissionens genomförandeförordning som antagits på grundval av direktivet om nät- och informationssäkerhet.

Enligt *3 mom*. gäller den i 1 mom. avsedda riskhanteringsskyldigheten inte sådana mikroföretag eller små företag som avses i artikel 16.11 i direktivet om nät- och informationssäkerhet. Syftet med denna begränsning är att skyldigheterna inte ska gälla sådana mikroföretag och små företag som avses i kommissionens rekommendation 2003/361/EG om definitionen av mikroföretag samt små och medelstora företag.

Genom de föreslagna bestämmelserna genomförs artikel 16.1 och 16.2 i direktivet om nät- och informationssäkerhet.

275 §. *Störningsanmälningar till Kommunikationsverket.* Det föreslås att paragrafen ändras. Det föreslagna nya *1 mom*. motsvarar i övrigt 1 mom. i gällande lag, men enligt förslaget ska det till momentet fogas en ny bestämmelse om att Kommunikationsverket årligen ska sända kommissionen och Europeiska byrån för nät- och kommunikationssäkerhet en sammanfattande informationsrapport över störningsanmälningarna. Skyldigheten motsvarar 3 mom. i gällande lag.

I det föreslagna nya *2 mom*. föreskrivs det om skyldigheten för tillhandahållare av internetbaserade marknadsplatser, sökmotortjänster och molntjänster att göra en anmälan till Kommunikationsverket om dess tjänster utsätts för en betydande störning i informationssäkerheten. Med störning i informationssäkerheten avses en händelse som har en faktisk negativ inverkan på säkerheten i systemen i fråga. Denna definition motsvarar definitionen av begreppet incident i direktivet om nät- och informationssäkerhet. För att fastställa om en störning är betydande ska hänsyn tas framför allt till hur många användare som påverkas av störningen, hur länge störningen varar och hur stort geografiskt område som påverkas av störningen, enligt vad som närmare föreskrivs i Europeiska kommissionens genomförandeakt som antagits på grundval av direktivet om nät- och informationssäkerhet.

I det nya *3 mom*. föreskrivs om Kommunikationsverkets rätt att ålägga den som tillhandahåller tjänsten att informera allmänheten om störningen eller, efter att ha hört den anmälningspliktiga, att själv informera om störningen. Kommunikationsverket ska innan allmänheten informeras ge den som tillhandahåller tjänsten tillfälle att bli hörd. Kommunikationsverket ska i första hand sträva efter att ge den som tillhandahåller tjänsten möjlighet att själv informera om störningen.

Det föreslagna *4 mom*. motsvarar i övrigt 2 mom. i gällande lag, men momentet ska dessutom ge Kommunikationsverket befogenhet att meddela föreskrifter också om innehållet i och utformningen av de störningsanmälningar som avses i det nya 2 mom. samt hur de ska lämnas in. Kommunikationsverket ska inte ges befogenhet att meddela föreskrifter om när en sådan störning som avses i det nya 2 mom. är betydande, eftersom denna befogenhet enligt direktivet om nät- och informationssäkerhet hör till kommissionen.

Det föreslås att *5 mom*. ska innehålla en skyldighet för Kommunikationsverket att bedöma om en sådan störning som avses i 2 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna. Syftet är att säkerställa att de berörda medlemsstaterna informeras om störningen i sådana fall där en störning får gränsöverskridande konsekvenser inom Europeiska unionen och Kommunikationsverket anser att det är nödvändigt att rapportera om störningen till en annan medlemsstat.

Genom de föreslagna bestämmelserna genomförs artikel 16.3, 16.4, 16.6 och 16.7 i direktivet om nät- och informationssäkerhet.

304 §. *Kommunikationsverkets särskilda uppgifter*. Syftet med de föreslagna ändringarna i paragrafen är att föreskriva om uppgifter som ska åläggas Kommunikationsverket och som anknyter till de uppgifter som fastställs i artikel 9 i direktivet om nät- och informationssäkerhet när det gäller att reagera på och undersöka kränkningar av informationssäkerheten. Kommunikationsverkets nuvarande uppgifter när det gäller att reagera på och undersöka kränkningar av informationssäkerheten omfattar redan sådana kränkningar av informationssäkerheten som drabbar nättjänster, kommunikationstjänster och mervärdestjänster. Genom de föreslagna ändringarna utvidgas Kommunikationsverkets uppgifter när det gäller att reagera på och undersöka kränkningar av informationssäkerheten så att de även omfattar kränkningar av informationssäkerheten i informationssystem. Ett informationssystem enligt denna paragraf kan bestå t.ex. av sådan teleterminalutrustning som avses i 3 § 25 punkten i denna lag eller av data som förvaras, behandlas, söks eller överförs i dessa system. Uppgifterna i anslutning till kränkningar av informationssäkerheten i informationssystem hänger samman med CSIRT-enheternas uppgifter enligt artikel 9 i direktivet om nät- och informationssäkerhet.

313 §. *Behandling av tillsynsärenden vid Kommunikationsverket*. Till *2 mom. 2 punkten* fogas en bestämmelse om att Kommunikationsverket har rätt att lämna ett ärende utan prövning, om ärendet endast har en ringa betydelse med tanke på riskhanteringen av de tjänster som avses i 247 a §. Syftet är att ge Kommunikationsverket rätt att behandla en i 275 § 2 mom. i denna lag avsedd anmälan om störning i informationssäkerheten som ett ärende för utredning och utbyte av information enligt 304 § 1 mom. 7 och 10 punkten i lagen i sådana fall där ärendet endast har en ringa betydelse med tanke på riskhanteringen i fråga om de tjänster som avses i bestämmelsen. Tillsyn ska utövas endast i det fall att störningen kan vara förknippad med en sådan försummelse av de riskhanteringsskyldigheter som fastställs i 247 a § och det är av väsentlig betydelse att man ingriper i försummelsen med tanke på riskhanteringen för den aktuella aktören eller för tillhandahållare av motsvarande tjänster i allmänhet.

308 §. *Myndighetssamarbete.* Enligt förslaget ska det till paragrafen fogas ett nytt *3 mom.* där det föreskrivs om Kommunikationsverkets skyldighet att vid behov samarbeta med olika myndigheter i andra medlemsstater inom området nät- och informationssäkerhet. Samarbete med andra medlemsstaters tillsynsmyndigheter inom området nät- och informationssäkerhet kan innebära ett samarbete t.ex. i sådana fall där en aktör tillhandahåller tjänster i flera medlemsstater. Med enheter för hantering av it-säkerhetsincidenter avses CSIRT-enheter enligt artikel 9 i direktivet om nät- och informationssäkerhet. Samarbete med CSIRT-aktörer innefattar t.ex. deltagande i ett CSIRT-nätverk enligt artikel 12 i direktivet om nät- och informationssäkerhet. Därtill föreskrivs det om samarbete med en samarbetsgrupp enligt direktivet om nät- och informationssäkerhet och om en skyldighet att till samarbetsgruppen lämna en sammanfattande rapport över störningsanmälningar enligt artiklarna 14 och 16 i direktivet om nät- och informationssäkerhet.

318 §. *Utlämnande av information från myndigheter*. Enligt förslaget ska det till paragrafen fogas ett nytt *2 mom*. där det fastställs att Kommunikationsverket har rätt att lämna ut information till tillsynsmyndigheter som är centrala med avseende på direktivet om nät- och informationssäkerhet. Syftet är att säkerställa att olika myndigheter som övervakar de skyldigheter som följer av direktivet om nät- och informationssäkerhet kan utbyta information som är betydande med tanke på deras tillsynsuppgifter. Denna information kan innefatta exempelvis uppgifter om störningar i informationssäkerheten. Genom de föreslagna bestämmelserna genomförs artikel 10 i direktivet om nät- och informationssäkerhet.

1.2 Lagen om ändring av luftfartslagen

128 a §. *Skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem.* Den föreslagna paragrafen är ny. I paragrafen föreskrivs det om skyldigheten för leverantörer av flygtrafiktjänster samt samhällsviktiga flygplatsoperatörer att sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som de använder. Närmare bestämmelser om när en i paragrafen avsedd flygplats ska betraktas som samhällsviktig utfärdas genom förordning av statsrådet.

Med kommunikationsnät enligt 1 mom. avses sådana kommunikationsnät som anges i 3 § 39 punkten i informationssamhällsbalken. Ett informationssystem enligt 1 mom. kan bestå t.ex. av sådan teleterminalutrustning som avses i 3 § 25 punkten i informationssamhällsbalken eller av data som förvaras, behandlas, söks eller överförs i dessa system. De kommunikationsnät och informationssystem som avses i paragrafen består framför allt av privata kommunikationsnät och informationssystem som antingen förvaltas av tjänsteleverantörens interna it-

personal eller vilkas säkerhet har lagts ut på entreprenad. Riskhanteringsskyldigheten enligt 1 mom. gäller endast sådana kommunikationsnät och informationssystem som är betydande med tanke på säkerheten inom luftfarten. Som betydande kommunikationsnät och informationssystem för säkerheten inom luftfarten ska betraktas åtminstone sådana system som är viktiga med tanke på serviceutbudets kontinuitet eller som, om de drabbas av störningar, kan medföra en risk för säkerheten inom luftfarten.

Med riskhantering avses lämpliga organisatoriska och tekniska åtgärder som vidtas för att säkerställa kommunikationsnätens och informationssystemens förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade eller överförda eller behandlade uppgifter eller hos andra tjänster som erbjuds genom eller är tillgängliga via dessa system. Riskhanteringen ska innefatta lämpliga åtgärder för att förebygga och minimera den effekt som informationssäkerhetsrelaterade störningar i de system som används vid tillhandahållandet av tjänsterna har på tjänsternas kontinuitet. Åtgärderna inom riskhanteringen kan bestå av t.ex. att upprätta säkerhetsplaner, testa dessa i praktiken eller utföra kvalitetsrevisioner, använda dataskydds- och krypteringsprodukter samt iaktta vissa välkända standarder för informationssäkerhet, såsom ICO/IEC 27001:2013. Med risk avses en rimligen identifierbar omständighet eller händelse med en potentiell negativ inverkan på säkerheten i kommunikationsnät och informationssystem. Riskhanteringen ska dokumenteras. Målet med dokumenteringen är att främja en konsekvent riskhantering och aktörens medvetna lösningar på hur de åtgärder som behövs för riskhanteringen ska dimensioneras. Dokumenteringen gör det också möjligt för myndigheterna att vid behov i efterskott bedöma huruvida skyldigheterna enligt denna paragraf har iakttagits. Dokumenteringen kan bestå t.ex. av skriftliga riskbedömningar, säkerhetsföreskrifter eller handlingsplaner eller av intyg över utförda säkerhetsrevisioner. Dokumenteringen kan inkluderas i andra planer för hantering av säkerhetsrisker eller beredskapsplaner.

I *2 mom*. föreskrivs det om tjänsteleverantörers skyldighet att lämna Trafiksäkerhetsverket sådana uppgifter som behövs för tillsynen över iakttagandet av skyldigheterna.

I *3 mom*. föreskrivs det om Trafiksäkerhetsverkets befogenhet att utöva tillsyn över de skyldigheter som fastställs i 1 mom. och rättighet att ålägga en i 1 mom. avsedd tjänsteleverantör att vidta korrigerande åtgärder för att eliminera en betydande risk för säkerheten inom luftfarten.

I *4 mom*. fastställs att Trafiksäkerhetsverket har rätt att lämna ut sekretessbelagd information till Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter. Denna information kan innefatta exempelvis uppgifter om informationssäkerhetshändelser.

Enligt bemyndigandet att utfärda förordning i 5 mom. utfärdas genom förordning av statsrådet närmare bestämmelser om när en i 1 mom. avsedd flygplatsoperatör ska betraktas som samhällsviktig. Syftet är att man genom en förordning med hjälp av ändamålsenliga gränsvärden kan fastställa i fråga om vilka flygplatser riskhanteringsskyldigheten ska tillämpas på flygplatsoperatören, eftersom det inte är ändamålsenligt att betrakta alla flygplatsoperatörer som leverantörer av samhällsviktiga tjänster enligt direktivet om nät- och informationssäkerhet. När det bedöms huruvida det är fråga om en samhällsviktig aktör ska de kriterier som anges i artikel 5.2 i direktivet om nät- och informationssäkerhet beaktas.

Genom de föreslagna bestämmelserna genomförs artikel 10, artikel 14.1 och 14.2 samt artikel 15.1 och 15.3 i direktivet om nät- och informationssäkerhet när det gäller sektor 2 delsektor a i bilaga II till direktivet.

128 b §. *Rapportering av informationssäkerhetshändelser.* Den föreslagna paragrafen är ny. I paragrafen föreskrivs det om skyldigheten för en i 128 a § avsedd aktör att underrätta Trafiksäkerhetsverket om betydande informationssäkerhetshändelser.

I *1 mom*. föreskrivs det om skyldigheten att underrätta Trafiksäkerhetsverket om en betydande händelse. Med händelse avses vilken som helst händelse som har en faktisk negativ inverkan på säkerheten i systemen i fråga. Denna definition motsvarar definitionen av begreppet incident i direktivet om nät- och informationssäkerhet. En händelse ska anses vara betydande om den kan utgöra en sådan betydande risk för flygsäkerheten som avses i artikel 4 i händelseförordningen. För att fastställa om en händelse är betydande ska hänsyn tas framför allt till hur många användare som påverkas av händelsen, hur länge den varar och hur stort geografiskt område som påverkas av den. Paragrafens 2 mom. bygger på samma grunder som det 275 § 3 mom. som föreslås ingå i informationssamhällsbalken.

Det föreslås att *3 mom*. ska innehålla en skyldighet för Trafiksäkerhetsverket att bedöma om en sådan störning som avses i det nya 2 mom. har en betydande inverkan på kontinuiteten i de samhällsviktiga tjänsterna i en annan medlemsstat i Europeiska unionen och vid behov rapportera om störningen till de berörda medlemsstaterna. Syftet är att säkerställa att de berörda medlemsstaterna informeras om störningen i sådana fall där en störning får gränsöverskridande konsekvenser inom Europeiska unionen och Trafiksäkerhetsverket anser att det är nödvändigt att rapportera om störningen till en annan medlemsstat. En rapport kan lämnas t.ex. när en störning kan utgöra en betydande risk för säkerheten inom luftfarten i en annan medlemsstat. Trafiksäkerhetsverket kan begära att Kommunikationsverket ska vidarebefordra rapporten till en sådan gemensam kontaktpunkt i en annan medlemsstat som avses i artikel 8 i direktivet om nät- och informationssäkerhet.

I *4 mom*. föreskrivs om Trafiksäkerhetsverkets rätt att meddela närmare föreskrifter om innehållet i och utformningen av den i paragrafen avsedda rapporten samt hur den ska lämnas in. I föreskrifterna kan det anges i närmare detalj t.ex. när en sådan händelse som avses i 1 mom. ska betraktas som betydande och i vilken form uppgifterna ska lämnas.

Genom de föreslagna bestämmelserna genomförs artikel 14.3–14.6 i direktivet om nät- och informationssäkerhet när det gäller sektor 2 delsektor a i bilaga II till direktivet.

1.3 Lagen om ändring av järnvägslagen

41 a §. *Skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten*. Den föreslagna paragrafen är ny. I paragrafen föreskrivs det om skyldigheten för förvaltaren av statens bannät samt bolag som tillhandahåller trafikledningstjänster att dels sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som de använder, dels underrätta Trafiksäkerhetsverket om en betydande störning i informationssäkerheten i anslutning till deras system.

Med kommunikationsnät enligt *1 mom*. avses sådana kommunikationsnät som anges i 3 § 39 punkten i informationssamhällsbalken. Ett informationssystem enligt 1 mom. kan bestå t.ex. av sådan teleterminalutrustning som avses i 3 § 25 punkten i informationssamhällsbalken eller av data som förvaras, behandlas, söks eller överförs i dessa system. De kommunikationsnät

och informationssystem som avses i paragrafen består framför allt av privata kommunikationsnät och informationssystem som antingen förvaltas av tjänsteleverantörens interna it-personal eller vilkas säkerhet har lagts ut på entreprenad. Riskhanteringsskyldigheten enligt 1 mom. gäller endast sådana kommunikationsnät och informationssystem som är betydande med tanke på säkerheten inom järnvägstrafiken. Som betydande kommunikationsnät och informationssystem för säkerheten inom järnvägstrafiken ska betraktas åtminstone sådana system som är viktiga med tanke på serviceutbudets kontinuitet eller som, om de drabbas av störningar, kan medföra en risk för säkerheten inom järnvägssystemet.

Med riskhantering avses lämpliga organisatoriska och tekniska åtgärder som vidtas för att säkerställa kommunikationsnätens och informationssystemens förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade eller överförda eller behandlade uppgifter eller hos andra tjänster som erbjuds genom eller är tillgängliga via dessa system. Riskhanteringen ska innefatta lämpliga åtgärder för att förebygga och minimera den effekt som informationssäkerhetsrelaterade störningar i de system som används vid tillhandahållandet av tjänsterna har på tjänsternas kontinuitet. Åtgärderna inom riskhanteringen kan bestå av t.ex. att upprätta säkerhetsplaner, testa dessa i praktiken eller utföra kvalitetsrevisioner, använda dataskydds- och krypteringsprodukter samt iaktta vissa välkända standarder för informationssäkerhet, såsom ICO/IEC 27001:2013. Med risk avses en rimligen identifierbar omständighet eller händelse med en potentiell negativ inverkan på säkerheten i kommunikationsnät och informationssystem. Riskhanteringen ska dokumenteras. Målet med dokumenteringen är att främja en konsekvent riskhantering och aktörens medvetna lösningar på hur de åtgärder som behövs för riskhanteringen ska dimensioneras. Dokumenteringen gör det också möjligt för myndigheterna att vid behov i efterskott bedöma huruvida skyldigheterna enligt denna paragraf har iakttagits. Dokumenteringen kan bestå t.ex. av skriftliga riskbedömningar, säkerhetsföreskrifter eller handlingsplaner eller av intyg över utförda säkerhetsrevisioner. Dokumenteringen kan inkluderas i andra planer för hantering av säkerhetsrisker eller beredskapsplaner.

I *2 mom*. föreskrivs det om skyldigheten att underrätta Trafiksäkerhetsverket om en betydande störning i informationssäkerheten. Med störning i informationssäkerheten avses en händelse som har en faktisk negativ inverkan på säkerheten i systemen i fråga. Denna definition motsvarar definitionen av begreppet incident i direktivet om nät- och informationssäkerhet. En störning ska anses vara betydande om den kan medföra en motsvarande betydande säkerhetsrisk i järnvägssystemet som den som avses i 39 § 2 mom. i järnvägslagen. För att fastställa om en störning är betydande ska hänsyn tas framför allt till hur många användare som påverkas av störningen, hur länge den varar och hur stort geografiskt område som påverkas av den.

Paragrafens *3 mom.* bygger på samma grunder som det 275 § 3 mom. som föreslås ingå i informationssamhällsbalken.

Det föreslås att *4 mom*. ska innehålla en skyldighet för Trafiksäkerhetsverket att bedöma om en sådan störning som avses i 2 mom. har en betydande inverkan på kontinuiteten i de samhällsviktiga tjänsterna i en annan medlemsstat i Europeiska unionen och vid behov rapportera om störningen till de berörda medlemsstaterna. Syftet är att säkerställa att de berörda medlemsstaterna informeras om störningen i sådana fall där en störning får gränsöverskridande konsekvenser inom Europeiska unionen och Trafiksäkerhetsverket anser att det är nödvändigt att rapportera om störningen till en annan medlemsstat. En rapport kan lämnas t.ex. när en störning kan utgöra en betydande risk för säkerheten inom järnvägssystemet i en annan medlemsstat. Trafiksäkerhetsverket kan begära att Kommunikationsverket ska vidarebefordra rap-

porten till en sådan gemensam kontaktpunkt i en annan medlemsstat som avses i artikel 8 i direktivet om nät- och informationssäkerhet.

I *5 mom.* fastställs att Trafiksäkerhetsverket har rätt att lämna ut sekretessbelagd information till Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter. Denna information kan innefatta exempelvis uppgifter om störningar i informationssäkerheten.

I *6 mom*. föreskrivs om Trafiksäkerhetsverkets rätt att meddela närmare föreskrifter om innehållet i och utformningen av den i paragrafen avsedda rapporten samt hur den ska lämnas in. I föreskrifterna kan det anges i närmare detalj t.ex. när en sådan störning i informationssäkerheten som avses i 2 mom. ska betraktas som betydande och i vilken form uppgifterna ska lämnas.

Genom de föreslagna bestämmelserna genomförs artikel 14.1–14.6 och artikel 10 i direktivet om nät- och informationssäkerhet när det gäller sektor 2 delsektor b i bilaga II till direktivet.

1.4 Lagen om ändring av lagen om fartygstrafikservice

16 §. *Upprätthållande av fartygstrafikservice.* Enligt förslaget ska det till paragrafen fogas ett nytt 5 mom. där det föreskrivs om skyldigheten för leverantörer av fartygstrafikservice att sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som de använder.

Med kommunikationsnät enligt 5 *mom*. avses sådana kommunikationsnät som anges i 3 § 39 punkten i informationssamhällsbalken. Ett informationssystem enligt 5 mom. kan bestå t.ex. av sådan teleterminalutrustning som avses i 3 § 25 punkten i informationssamhällsbalken eller av data som förvaras, behandlas, söks eller överförs i dessa system. De kommunikationsnät och informationssystem som avses i paragrafen består framför allt av privata kommunikationsnät och informationssystem som antingen förvaltas av tjänsteleverantörens interna it-personal eller vilkas säkerhet har lagts ut på entreprenad. Riskhanteringsskyldigheten enligt 1 mom. gäller endast sådana kommunikationsnät och informationssystem som är betydande med tanke på säkerheten inom sjöfarten. Som betydande kommunikationsnät och informationssystem för säkerheten inom sjöfarten ska betraktas åtminstone sådana system som är viktiga med tanke på serviceutbudets kontinuitet eller som, om de drabbas av störningar, kan medföra en risk för säkerheten inom sjöfarten. Skyldigheten gäller VTS-myndighetens uppgifter, som hänför sig till den operativa verksamheten i anslutning till trafikstyrning.

Med riskhantering avses lämpliga organisatoriska och tekniska åtgärder som vidtas för att säkerställa kommunikationsnätens och informationssystemens förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade eller överförda eller behandlade uppgifter eller hos andra tjänster som erbjuds genom eller är tillgängliga via dessa system. Riskhanteringen ska innefatta lämpliga åtgärder för att förebygga och minimera den effekt som informationssäkerhetsrelaterade störningar i de system som används vid tillhandahållandet av tjänsterna har på tjänsternas kontinuitet. Åtgärderna inom riskhanteringen kan bestå av t.ex. att upprätta säkerhetsplaner, testa dessa i praktiken eller utföra kvalitetsrevisioner, använda dataskydds- och krypteringsprodukter samt iaktta vissa välkända standarder för informationssäkerhet, såsom ICO/IEC 27001:2013. Med risk avses en rimligen identifierbar omständighet eller händelse med en potentiell negativ inverkan på säkerheten i kommunikationsnät och informationssystem. Riskhanteringen ska dokumenteras. Målet med dokumenteringen är att främja en konsekvent risk-

hantering och aktörens medvetna lösningar på hur de åtgärder som behövs för riskhanteringen ska dimensioneras. Dokumenteringen gör det också möjligt för myndigheterna att vid behov i efterskott bedöma huruvida skyldigheterna enligt denna paragraf har iakttagits. Dokumenteringen kan bestå t.ex. av skriftliga riskbedömningar, säkerhetsföreskrifter eller handlingsplaner eller av intyg över utförda säkerhetsrevisioner. Dokumenteringen kan inkluderas i andra planer för hantering av säkerhetsrisker eller beredskapsplaner.

Genom de föreslagna bestämmelserna och de bestämmelser som föreslås i lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet genomförs artikel 14.1 och 14.2 i direktivet om nät- och informationssäkerhet när det gäller sektor 2 delsektor c i bilaga II till direktivet.

18 a §. *Skyldighet att anmäla störningar i informationssäkerheten.* Den föreslagna paragrafen är ny. I paragrafen föreskrivs det om anmälan om störningar i informationssäkerheten och om Trafiksäkerhetsverkets rätt att meddela föreskrifter om detta.

I *1 mom*. föreskrivs det om skyldigheten att underrätta Trafiksäkerhetsverket om en betydande störning i informationssäkerheten. Med störning i informationssäkerheten avses en händelse som har en faktisk negativ inverkan på säkerheten i systemen i fråga. Denna definition motsvarar definitionen av begreppet incident i direktivet om nät- och informationssäkerhet. En störning som kan ha en betydande inverkan på säkerheten inom sjöfarten ska betraktas som betydande. För att fastställa om en störning är betydande ska hänsyn tas framför allt till hur många användare som påverkas av störningen, hur länge störningen varar och hur stort geografiskt område som påverkas av störningen.

Paragrafens *2 mom*. bygger på samma grunder som det 275 § 3 mom. som föreslås ingå i informationssamhällsbalken.

Det föreslås att *3 mom*. ska innehålla en skyldighet för Trafiksäkerhetsverket att bedöma om en sådan störning som avses i 2 mom. har en betydande inverkan på kontinuiteten i de samhällsviktiga tjänsterna i en annan medlemsstat i Europeiska unionen och vid behov rapportera om störningen till de berörda medlemsstaterna. Syftet är att säkerställa att de berörda medlemsstaterna informeras om störningen i sådana fall där en störning får gränsöverskridande konsekvenser inom Europeiska unionen och Trafiksäkerhetsverket anser att det är nödvändigt att rapportera om störningen till en annan medlemsstat. En rapport kan lämnas t.ex. när en störning kan ha en betydande inverkan på säkerheten inom sjöfarten i en annan medlemsstat. Trafiksäkerhetsverket kan begära att Kommunikationsverket ska vidarebefordra rapporten till en sådan gemensam kontaktpunkt i en annan medlemsstat som avses i artikel 8 i direktivet om nät- och informationssäkerhet.

I *4 mom*. föreskrivs om Trafiksäkerhetsverkets rätt att meddela närmare föreskrifter om innehållet i och utformningen av den i paragrafen avsedda rapporten samt hur den ska lämnas in. I föreskrifterna kan det anges i närmare detalj t.ex. när en sådan störning i informationssäkerheten som avses i 1 mom. ska betraktas som betydande och i vilken form uppgifterna ska lämnas.

I *5 mom.* fastställs att Trafiksäkerhetsverket har rätt att lämna ut sekretessbelagd information till Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter. Denna information kan innefatta exempelvis uppgifter om störningar i informationssäkerheten.

Genom de föreslagna bestämmelserna och de bestämmelser som föreslås i lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet genomförs artikel 14.3–14.6 och artikel 10 i direktivet om nät- och informationssäkerhet när det gäller sektor 2 delsektor c i bilaga II till direktivet.

28 §. *Tillsyn.* Enligt förslaget ska det till paragrafen fogas ett nytt 4 mom. där det föreskrivs om tillsynen över den riskhantering som avses i 16 § 5 mom. Trafiksäkerhetsverket kan ålägga VTS-myndigheten att vidta korrigerande åtgärder för att eliminera en betydande risk som inverkar på säkerheten inom sjöfarten. Med betydande risk avses en betydande inverkan enligt det föreslagna 18 a § 1 mom. Vidare föreskrivs det om Trafiksäkerhetsverkets möjlighet att förena åläggandet med vite.

Genom de föreslagna bestämmelserna och de bestämmelser som föreslås i lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet genomförs artikel 15.1 och 15.3 samt artikel 21 i direktivet om nät- och informationssäkerhet när det gäller sektor 2 delsektor c i bilaga II till direktivet.

1.5 Lagen om ändring av lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet

7 e §. *Hamninnehavares skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten*. Den föreslagna paragrafen är ny. I paragrafen föreskrivs det om skyldigheten för innehavare av samhällsviktiga hamnar att dels sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som de använder.

Med kommunikationsnät enligt *1 mom.* avses sådana kommunikationsnät som anges i 3 § 39 punkten i informationssamhällsbalken. Ett informationssystem enligt 1 mom. kan bestå t.ex. av sådan teleterminalutrustning som avses i 3 § 25 punkten i informationssamhällsbalken eller av data som förvaras, behandlas, söks eller överförs i dessa system. De kommunikationsnät och informationssystem som avses i paragrafen består framför allt av privata kommunikationsnät och informationssystem som antingen förvaltas av tjänsteleverantörens interna itpersonal eller vilkas säkerhet har lagts ut på entreprenad. Riskhanteringsskyldigheten enligt 1 mom. gäller endast sådana kommunikationsnät och informationssystem som är betydande med tanke på säkerheten inom sjöfarten. Som betydande kommunikationsnät och informationssystem för säkerheten inom sjöfarten ska betraktas åtminstone sådana system som är viktiga med tanke på serviceutbudets kontinuitet eller som, om de drabbas av störningar, kan medföra en risk för säkerheten inom sjöfarten.

Med riskhantering avses lämpliga organisatoriska och tekniska åtgärder som vidtas för att säkerställa kommunikationsnätens och informationssystemens förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade eller överförda eller behandlade uppgifter eller hos andra tjänster som erbjuds genom eller är tillgängliga via dessa system. Riskhanteringen ska innefatta lämpliga åtgärder för att förebygga och minimera den effekt som informationssäkerhetsrelaterade störningar i de system som används vid tillhandahållandet av tjänsterna har på tjänsternas kontinuitet. Åtgärderna inom riskhanteringen kan bestå av t.ex. att upprätta säkerhetsplaner, testa dessa i praktiken eller utföra kvalitetsrevisioner, använda dataskydds- och krypteringsprodukter samt iaktta vissa välkända standarder för informationssäkerhet, såsom ICO/IEC 27001:2013. Med risk avses en rimligen identifierbar omständighet eller händelse med en potentiell negativ inverkan på säkerheten i kommunikationsnät och informationssystem. Risk-

hanteringen ska dokumenteras. Målet med dokumenteringen är att främja en konsekvent riskhantering och aktörens medvetna lösningar på hur de åtgärder som behövs för riskhanteringen ska dimensioneras. Dokumenteringen gör det också möjligt för myndigheterna att vid behov i efterskott bedöma huruvida skyldigheterna enligt denna paragraf har iakttagits. Dokumenteringen kan bestå t.ex. av skriftliga riskbedömningar, säkerhetsföreskrifter eller handlingsplaner eller av intyg över utförda säkerhetsrevisioner. Dokumenteringen kan inkluderas i andra planer för hantering av säkerhetsrisker eller beredskapsplaner.

I *2 mom*. föreskrivs det om Trafiksäkerhetsverkets befogenhet att utöva tillsyn över de skyldigheter som fastställs i 1 mom. och rättighet att ålägga en i 1 mom. avsedd tjänsteleverantör att vidta korrigerande åtgärder för att eliminera en betydande risk för säkerheten inom sjöfarten. Trafiksäkerhetsverket kan förena åläggandet med vite.

I *3 mom*. fastställs att Trafiksäkerhetsverket har rätt att lämna ut sekretessbelagd information till Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter. Denna information kan innefatta exempelvis uppgifter om informationssäkerhetshändelser.

Enligt bemyndigandet att utfärda förordning i *4 mom*. utfärdas genom förordning av statsrådet närmare bestämmelser om när en i 1 mom. avsedd hamn ska betraktas som samhällsviktig. Syftet är att man genom en förordning med hjälp av ändamålsenliga gränsvärden kan fastställa i fråga om vilka hamnar riskhanteringsskyldigheten ska tillämpas på hamninnehavaren, eftersom det inte är ändamålsenligt att betrakta alla hamninnehavare som leverantörer av samhällsviktiga tjänster enligt direktivet om nät- och informationssäkerhet. När det bedöms huruvida det är fråga om en samhällsviktig aktör ska de kriterier som anges i artikel 5.2 i direktivet om nät- och informationssäkerhet beaktas.

Genom de föreslagna bestämmelserna och de föreslagna ändringarna i lagen om fartygstrafikservice genomförs artikel 10, artikel 14.1 och 14.2 samt artiklarna 15.3 och 21 i direktivet om nät- och informationssäkerhet när det gäller sektor 2 delsektor c i bilaga II till direktivet.

7 f §. *Rapportering av störningar i informationssäkerheten. Den föreslagna paragrafen är ny.*

I *1 mom.* föreskrivs det om skyldigheten att underrätta Trafiksäkerhetsverket om en betydande störning i informationssäkerheten. Med störning i informationssäkerheten avses en händelse som har en faktisk negativ inverkan på säkerheten i systemen i fråga. Denna definition motsvarar definitionen av begreppet incident i direktivet om nät- och informationssäkerhet. En störning som kan ha en betydande inverkan på säkerheten inom sjöfarten ska betraktas som betydande. För att fastställa om en händelse är betydande ska hänsyn tas framför allt till hur många användare som påverkas av händelsen, hur länge den varar och hur stort geografiskt område som påverkas av den.

Paragrafens *2 mom*. bygger på samma grunder som det 275 § 3 mom. som föreslås ingå i informationssamhällsbalken.

Det föreslås att *3 mom.* ska innehålla en skyldighet för Trafiksäkerhetsverket att bedöma om en sådan störning som avses i 2 mom. har en betydande inverkan på kontinuiteten i de samhällsviktiga tjänsterna i en annan medlemsstat i Europeiska unionen och vid behov rapportera om störningen till de berörda medlemsstaterna. Syftet är att säkerställa att de berörda medlemsstaterna informeras om störningen i sådana fall där en störning får gränsöverskridande konsekvenser inom Europeiska unionen och Trafiksäkerhetsverket anser att det är nödvändigt

att rapportera om störningen till en annan medlemsstat. En rapport kan lämnas t.ex. när en störning kan ha en betydande inverkan på säkerheten inom sjöfarten i en annan medlemsstat. Trafiksäkerhetsverket kan begära att Kommunikationsverket ska vidarebefordra rapporten till en sådan gemensam kontaktpunkt i en annan medlemsstat som avses i artikel 8 i direktivet om nät- och informationssäkerhet.

I *4 mom*. föreskrivs om Trafiksäkerhetsverkets rätt att meddela närmare föreskrifter om innehållet i och utformningen av den i paragrafen avsedda rapporten samt hur den ska lämnas in. I föreskrifterna kan det anges i närmare detalj t.ex. när en sådan störning i informationssäkerheten som avses i 1 mom. ska betraktas som betydande och i vilken form uppgifterna ska lämnas.

Genom de föreslagna bestämmelserna och de föreslagna ändringarna i lagen om fartygstrafikservice genomförs artikel 14.3–14.6 i direktivet om nät- och informationssäkerhet när det gäller sektor 2 delsektor c i bilaga II till direktivet.

1.6 Lagen om ändring av lagen om transportservice

AVDELNING III. TJÄNSTER

2 kap. Informationens och informationssystemens interoperabilitet

7 §. *Skyldighet för den som tillhandahålle intelligenta trafiksystem att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten.* Den föreslagna paragrafen är ny. I paragrafen föreskrivs det om skyldigheten för den som tillhandahåller ett intelligent trafiksystem att dels sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som de använder, dels underrätta Trafiksäkerhetsverket om en betydande störning i informationssäkerheten i anslutning till deras system. Med intelligenta trafiksystem avses sådana system som anges i lagens 2 kap. 6 § och i artikel 4.1 i Europaparlamentets och rådets direktiv 2010/40/EU om ett ramverk för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportslag.

Med kommunikationsnät enligt *1 mom*. avses sådana kommunikationsnät som anges i 3 § 39 punkten i informationssamhällsbalken. Ett informationssystem enligt 1 mom. kan bestå t.ex. av sådan teleterminalutrustning som avses i 3 § 25 punkten i informationssamhällsbalken eller av data som förvaras, behandlas, söks eller överförs i dessa system. De kommunikationsnät och informationssystem som avses i paragrafen består framför allt av privata kommunikationsnät och informationssystem som antingen förvaltas av tjänsteleverantörens interna it-personal eller vilkas säkerhet har lagts ut på entreprenad. Riskhanteringsskyldigheten gäller endast sådana kommunikationsnät och informationssystem som är betydande med tanke på säkerheten inom ett intelligent trafiksystem. Som betydande kommunikationsnät och informationssystem för säkerheten inom ett intelligent trafiksystem ska betraktas åtminstone sådana system som är viktiga med tanke på serviceutbudets kontinuitet.

Med riskhantering avses lämpliga organisatoriska och tekniska åtgärder som vidtas för att säkerställa kommunikationsnätens och informationssystemens förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade eller överförda eller behandlade uppgifter eller hos andra tjänster som erbjuds genom eller är tillgängliga via dessa system. Riskhanteringen ska innefatta lämpliga åtgärder för att förebygga och minimera den effekt som informationssäkerhetsrelate-

rade störningar i de system som används vid tillhandahållandet av tjänsterna har på tjänsternas kontinuitet. Åtgärderna inom riskhanteringen kan bestå av t.ex. att upprätta säkerhetsplaner, testa dessa i praktiken eller utföra kvalitetsrevisioner, använda dataskydds- och krypteringsprodukter samt iaktta vissa välkända standarder för informationssäkerhet, såsom ICO/IEC 27001:2013. Med risk avses en rimligen identifierbar omständighet eller händelse med en potentiell negativ inverkan på säkerheten i kommunikationsnät och informationssystem. Riskhanteringen ska dokumenteras. Målet med dokumenteringen är att främja en konsekvent riskhantering och aktörens medvetna lösningar på hur de åtgärder som behövs för riskhanteringen ska dimensioneras. Dokumenteringen gör det också möjligt för myndigheterna att vid behov i efterskott bedöma huruvida skyldigheterna enligt denna paragraf har iakttagits. Dokumenteringen kan bestå t.ex. av skriftliga riskbedömningar, säkerhetsföreskrifter eller handlingsplaner eller av intyg över utförda säkerhetsrevisioner. Dokumenteringen kan inkluderas i andra planer för hantering av säkerhetsrisker eller beredskapsplaner.

I *2 mom*. föreskrivs det om skyldigheten att underrätta Trafiksäkerhetsverket om en betydande störning i informationssäkerheten. Med störning i informationssäkerheten avses en händelse som har en faktisk negativ inverkan på säkerheten i systemen i fråga. Denna definition motsvarar definitionen av begreppet incident i direktivet om nät- och informationssäkerhet. En störning ska anses vara betydande om den kan utgöra en betydande risk för säkerheten inom ett intelligent trafiksystem. För att fastställa om en störning är betydande ska hänsyn tas framför allt till hur många användare som påverkas av störningen, hur länge den varar och hur stort geografiskt område som påverkas av den.

Paragrafens *3 mom*. bygger på samma grunder som det 275 § 3 mom. som föreslås ingå i informationssamhällsbalken.

Det föreslås att *4 mom*. ska innehålla en skyldighet för Trafiksäkerhetsverket att bedöma om en sådan störning som avses i 2 mom. har en betydande inverkan på kontinuiteten i de samhällsviktiga tjänsterna i en annan medlemsstat i Europeiska unionen och vid behov rapportera om störningen till de berörda medlemsstaterna. Syftet är att säkerställa att de berörda medlemsstaterna informeras om störningen i sådana fall där en störning får gränsöverskridande konsekvenser inom Europeiska unionen och Trafiksäkerhetsverket anser att det är nödvändigt att rapportera om störningen till en annan medlemsstat. En rapport kan lämnas t.ex. när en störning kan ha en betydande inverkan på säkerheten inom ett intelligent trafiksystem i en annan medlemsstat. Trafiksäkerhetsverket kan begära att Kommunikationsverket ska vidarebefordra rapporten till en sådan gemensam kontaktpunkt i en annan medlemsstat som avses i artikel 8 i direktivet om nät- och informationssäkerhet.

I *5 mom*. fastställs att Trafiksäkerhetsverket har rätt att lämna ut sekretessbelagd information till Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter. Denna information kan innefatta exempelvis uppgifter om störningar i informationssäkerheten.

I *6 mom*. föreskrivs om Trafiksäkerhetsverkets rätt att meddela närmare föreskrifter om innehållet i och utformningen av den i paragrafen avsedda rapporten samt hur den ska lämnas in. I föreskrifterna kan det anges i närmare detalj t.ex. när en sådan störning i informationssäkerheten som avses i 2 mom. ska betraktas som betydande och i vilken form uppgifterna ska lämnas.

Genom de föreslagna bestämmelserna genomförs artikel 14.1–14.6 och artikel 10 i direktivet om nät- och informationssäkerhet när det gäller sektor 2 delsektor d i bilaga II till direktivet.

1.7 Lagen om ändring av elmarknadslagen

29 a §. *Nätinnehavares skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten*. Den föreslagna paragrafen är ny. I paragrafen föreskrivs det om skyldigheten för nätinnehavare att dels sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som de använder, dels underrätta Energimyndigheten om en betydande störning i informationssäkerheten i anslutning till deras system. Bestämmelserna i paragrafen ska tillämpas på alla nätinnehavare med undantag av innehavare av ett slutet distributionsnät.

Med kommunikationsnät enligt *1 mom*. avses sådana kommunikationsnät som anges i 3 § 39 punkten i informationssamhällsbalken. Ett informationssystem enligt 1 mom. kan bestå t.ex. av sådan teleterminalutrustning som avses i 3 § 25 punkten i informationssamhällsbalken eller av data som förvaras, behandlas, söks eller överförs i dessa system. De kommunikationsnät och informationssystem som avses i paragrafen består framför allt av privata kommunikationsnät och informationssystem som antingen förvaltas av tjänsteleverantörens interna it-personal eller vilkas säkerhet har lagts ut på entreprenad. Riskhanteringsskyldigheten enligt 1 mom. gäller sådana informationssystem och kommunikationsnät som är betydande med tanke på eldistributionens kontinuitet.

Med riskhantering avses lämpliga organisatoriska och tekniska åtgärder som vidtas för att säkerställa kommunikationsnätens och informationssystemens förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade eller överförda eller behandlade uppgifter eller hos andra tjänster som erbjuds genom eller är tillgängliga via dessa system. Riskhanteringen ska innefatta lämpliga åtgärder för att förebygga och minimera den effekt som informationssäkerhetsrelaterade störningar i de system som används vid tillhandahållandet av tjänsterna har på tjänsternas kontinuitet. Åtgärderna inom riskhanteringen kan bestå av t.ex. att upprätta säkerhetsplaner, testa dessa i praktiken eller utföra kvalitetsrevisioner, använda dataskydds- och krypteringsprodukter samt iaktta vissa välkända standarder för informationssäkerhet, såsom ICO/IEC 27001:2013. Med risk avses en rimligen identifierbar omständighet eller händelse med en potentiell negativ inverkan på säkerheten i kommunikationsnät och informationssystem. Riskhanteringen ska dokumenteras. Målet med dokumenteringen är att främja en konsekvent riskhantering och aktörens medvetna lösningar på hur de åtgärder som behövs för riskhanteringen ska dimensioneras. Dokumenteringen gör det också möjligt för myndigheterna att vid behov i efterskott bedöma huruvida skyldigheterna enligt denna paragraf har iakttagits. Dokumenteringen kan bestå t.ex. av skriftliga riskbedömningar, säkerhetsföreskrifter eller handlingsplaner eller av intyg över utförda säkerhetsrevisioner. Dokumenteringen kan inkluderas i andra planer för hantering av säkerhetsrisker eller beredskapsplaner, såsom exempelvis den beredskapsplan som avses i 28 §.

I *2 mom*. föreskrivs det om skyldigheten att underrätta Energimyndigheten om en betydande störning i informationssäkerheten. Med störning i informationssäkerheten avses en händelse som har en faktisk negativ inverkan på säkerheten i systemen i fråga. Denna definition motsvarar definitionen av begreppet incident i direktivet om nät- och informationssäkerhet. En störning ska anses vara betydande om den kan leda till att eldistributionen i distributionsnätet avbryts i en betydande omfattning. Tröskeln för att göra anmälan när en störning kan leda till att eldistributionen avbryts i en betydande omfattning motsvarar den tröskel för att göra anmälan som anges i 59 § i elmarknadslagen. För att fastställa om en störning är betydande ska hänsyn tas framför allt till hur många användare som påverkas av störningen, hur länge den varar och hur stort geografiskt område som påverkas av den.

Paragrafens *3 mom*. bygger på samma grunder som det 275 § 3 mom. som föreslås ingå i informationssamhällsbalken.

Det föreslås att *4 mom*. ska innehålla en skyldighet för Energimyndigheten att bedöma om en sådan störning som avses i 2 mom. har en betydande inverkan på kontinuiteten i de samhällsviktiga tjänsterna i en annan medlemsstat i Europeiska unionen och vid behov rapportera om störningen till de berörda medlemsstaterna. Syftet är att säkerställa att de berörda medlemsstaterna informeras om störningen i sådana fall där en störning får gränsöverskridande konsekvenser inom Europeiska unionen och Energimyndigheten anser att det är nödvändigt att rapportera om störningen till en annan medlemsstat. En rapport kan lämnas t.ex. när en störning kan ha en betydande inverkan på eldistributionens kontinuitet i en annan medlemsstat. Energimyndigheten kan begära att Kommunikationsverket ska vidarebefordra rapporten till en sådan gemensam kontaktpunkt i en annan medlemsstat som avses i artikel 8 i direktivet om nät- och informationssäkerhet.

I *5 mom*. föreskrivs om Energimyndighetens rätt att meddela närmare föreskrifter om innehållet i och utformningen av den i paragrafen avsedda rapporten samt hur den ska lämnas in. I föreskrifterna kan det anges i närmare detalj t.ex. när en sådan störning i informationssäkerheten som avses i 2 mom. ska betraktas som betydande och i vilken form uppgifterna ska lämnas.

Genom de föreslagna bestämmelserna genomförs artikel 14.1–14.6 i direktivet om nät- och informationssäkerhet när det gäller sektor 1 delsektor a i bilaga II till direktivet.

62 §. *Specialbestämmelser som gäller slutna distributionsnät.* Enligt förslaget ska det till paragrafen fogas en bestämmelse om att den föreslagna 29 a § inte ska tillämpas på slutna distributionsnät och innehavare av slutna distributionsnät. Skyldigheten att sörja för informationssäkerheten ska inte tillämpas på innehavare av ett slutet distributionsnät, eftersom eldistributionen i ett slutet distributionsnät inte kan anses vara en samhällsviktig tjänst på det sätt som avses i direktivet om nät- och informationssäkerhet.

1.8 Lagen om ändring av naturgasmarknadslagen

34 a §. *Överföringsnätinnehavares skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten*. Den föreslagna paragrafen är ny. I paragrafen föreskrivs det om skyldigheten för överföringsnätinnehavare att dels sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som de använder, dels underrätta Energimyndigheten om en betydande störning i informationssäkerheten i anslutning till deras system.

Med kommunikationsnät enligt *1 mom.* avses sådana kommunikationsnät som anges i 3 § 39 punkten i informationssamhällsbalken. Ett informationssystem enligt 1 mom. kan bestå t.ex. av sådan teleterminalutrustning som avses i 3 § 25 punkten i informationssamhällsbalken eller av data som förvaras, behandlas, söks eller överförs i dessa system. De kommunikationsnät och informationssystem som avses i paragrafen består framför allt av privata kommunikationsnät och informationssystem som antingen förvaltas av tjänsteleverantörens interna itpersonal eller vilkas säkerhet har lagts ut på entreprenad. Riskhanteringsskyldigheten enligt 1 mom. gäller sådana informationssystem och kommunikationsnät som är betydande med tanke på naturgasöverföringens kontinuitet.

Med riskhantering avses lämpliga organisatoriska och tekniska åtgärder som vidtas för att säkerställa kommunikationsnätens och informationssystemens förmåga att vid en viss tillförlit-

lighetsnivå motstå åtgärder som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade eller överförda eller behandlade uppgifter eller hos andra tjänster som erbjuds genom eller är tillgängliga via dessa system. Riskhanteringen ska innefatta lämpliga åtgärder för att förebygga och minimera den effekt som informationssäkerhetsrelaterade störningar i de system som används vid tillhandahållandet av tjänsterna har på tjänsternas kontinuitet. Åtgärderna inom riskhanteringen kan bestå av t.ex. att upprätta säkerhetsplaner, testa dessa i praktiken eller utföra kvalitetsrevisioner, använda dataskydds- och krypteringsprodukter samt iaktta vissa välkända standarder för informationssäkerhet, såsom ICO/IEC 27001:2013. Med risk avses en rimligen identifierbar omständighet eller händelse med en potentiell negativ inverkan på säkerheten i kommunikationsnät och informationssystem. Riskhanteringen ska dokumenteras. Målet med dokumenteringen är att främja en konsekvent riskhantering och aktörens medvetna lösningar på hur de åtgärder som behövs för riskhanteringen ska dimensioneras. Dokumenteringen gör det också möjligt för myndigheterna att vid behov i efterskott bedöma huruvida skyldigheterna enligt denna paragraf har iakttagits. Dokumenteringen kan bestå t.ex. av skriftliga riskbedömningar, säkerhetsföreskrifter eller handlingsplaner eller av intyg över utförda säkerhetsrevisioner. Dokumenteringen kan inkluderas i andra planer för hantering av säkerhetsrisker eller beredskapsplaner.

I *2 mom*. föreskrivs det om skyldigheten att underrätta Energimyndigheten om en betydande störning i informationssäkerheten. Med störning i informationssäkerheten avses en händelse som har en faktisk negativ inverkan på säkerheten i systemen i fråga. Denna definition motsvarar definitionen av begreppet incident i direktivet om nät- och informationssäkerhet. En störning ska anses vara betydande om den kan leda till att överföringen av naturgas i överföringsnätet avbryts i en betydande omfattning. För att fastställa om en störning är betydande ska hänsyn tas framför allt till hur många användare som påverkas av störningen, hur länge den varar och hur stort geografiskt område som påverkas av den.

Paragrafens *3 mom*. bygger på samma grunder som det 275 § 3 mom. som föreslås ingå i informationssamhällsbalken.

Det föreslås att *4 mom.* ska innehålla en skyldighet för Energimyndigheten att bedöma om en sådan störning som avses i 2 mom. har en betydande inverkan på kontinuiteten i de samhällsviktiga tjänsterna i en annan medlemsstat i Europeiska unionen och vid behov rapportera om störningen till de berörda medlemsstaterna. Syftet är att säkerställa att de berörda medlemsstaterna informeras om störningen i sådana fall där en störning får gränsöverskridande konsekvenser inom Europeiska unionen och Energimyndigheten anser att det är nödvändigt att rapportera om störningen till en annan medlemsstat. En rapport kan lämnas t.ex. när en störning kan ha en betydande inverkan på naturgasdistributionens kontinuitet i en annan medlemsstat. Energimyndigheten kan begära att Kommunikationsverket ska vidarebefordra rapporten till en sådan gemensam kontaktpunkt i en annan medlemsstat som avses i artikel 8 i direktivet om nät- och informationssäkerhet.

I *5 mom*. föreskrivs om Energimyndighetens rätt att meddela närmare föreskrifter om innehållet i och utformningen av den i paragrafen avsedda rapporten samt hur den ska lämnas in. I föreskrifterna kan det anges i närmare detalj t.ex. när en sådan störning i informationssäkerheten som avses i 2 mom. ska betraktas som betydande och i vilken form uppgifterna ska lämnas.

Genom de föreslagna bestämmelserna genomförs artikel 14.1–14.6 i direktivet om nät- och informationssäkerhet när det gäller sektor 1 delsektor c i bilaga II till direktivet.

1.9 Lagen om ändring av 27 och 28 § i lagen om tillsyn över el- och naturgasmarknaden

27 §. *Myndigheternas tillsynssamarbete.* Det föreslås att paragrafen ändras så att den innehåller bestämmelser om Energimyndighetens rätt att utöva tillsynssamarbete med Kommunikationsverket. Tillsynssamarbete kan vara behövligt när det gäller att övervaka de skyldigheter som hänför sig till informationssäkerheten. Vidare ska hänvisningarna till Energimarknadsverket ersättas med hänvisningar till Energimyndigheten. Genom bestämmelsen genomförs artikel 10.1 i direktivet om nät- och informationssäkerhet när det gäller sektor 1 i bilaga II till direktivet.

28 §. *Energimyndighetens rätt att lämna ut uppgifter till andra myndigheter.* Det föreslås att paragrafen ändras så att den innehåller bestämmelser om Energimyndighetens rätt att lämna ut sekretessbelagd information till Kommunikationsverket. Det kan vara nödvändigt att lämna ut sådan information för att kunna övervaka de skyldigheter som hänför sig till informationssäkerheten. Vidare ska hänvisningarna till Energimarknadsverket ersättas med hänvisningar till Energimyndigheten. Genom bestämmelsen genomförs artikel 10.2 och 10.3 i direktivet om nät- och informationssäkerhet när det gäller sektor 1 i bilaga II till direktivet.

1.10 Lagen om ändring av lagen om vattentjänster

15 b §. *Anmälan om störningar i vattentjänster*. Till lagen fogas en ny paragraf om skyldigheten för vattentjänstverket samt närings-, trafik- och miljöcentralen att anmäla om betydande störningar i vattentjänsterna. Genom de föreslagna bestämmelserna genomförs också artikel 14.3–14.6 i direktivet om nät- och informationssäkerhet när det gäller sektor 6 i bilaga II till direktivet.

Enligt 15 a § i den gällande lagen om vattentjänster ansvarar ett vattentjänstverk för att vattentjänsterna för de fastigheter som anslutits till dess ledningsnät är tillgängliga även i störningssituationer. Vattentjänstverket ska i syfte att trygga tjänsterna utarbeta och uppdatera en plan för beredskap för störningssituationer och vidta de åtgärder som behövs enligt planen. Närings-, trafik- och miljöcentralen och den kommunala miljövårdsmyndigheten och hälsoskyddsmyndigheten övervakar att vattentjänstverket fullgör sin planeringsskyldighet. Verken är emellertid enligt lagen om vattentjänster inte skyldiga att underrätta tillsynsmyndigheterna om störningssituationer.

Nuförtiden är vattentjänstverken på grundval av lagstiftningen om miljövård eller hälsoskydd skyldiga att anmäla om vissa störningssituationer i vattentjänsterna. Förfarandet för anmälan om störningar regleras för tillfället på olika sätt i olika lagar, och i fråga om vissa störningar i vattentjänsterna, såsom avbrott i distributionen av hushållsvatten eller avledningen av avloppsvatten, finns det inga bestämmelser över huvud taget. För att det ska bli möjligt att forma en regional lägesbild, identifiera sårbarheter i vattentjänsterna och förbättra riskhanteringen är det därför nödvändigt att verken anmäler alla typer av betydande störningssituationer i vattentjänsterna och att anmälningarna görs till en och samma regionala myndighet.

I *1 mom*. fastställs det följaktligen att ett vattentjänstverk ska göra en anmälan till närings-, trafik- och miljöcentralen om betydande störningssituationer i vattentjänsterna oberoende av varför och på vilket sätt störningen har uppstått. Skyldigheten ska gälla verk som levererar minst 5 000 kubikmeter vatten per dygn. Det finns cirka 40 sådana verk i Finland, och deras kundkrets omfattar över hälften av landets befolkning. Verk av denna storleksklass har också klassificerats som kritiska vattentjänstverk med tanke på försörjningsberedskapen. I fråga om sådana verk som också behandlar avloppsvatten utanför sitt eget ledningsnät ska anmälningsskyldigheten vid behov fastställas utifrån mängden mottaget avloppsvatten oberoende av hur mycket hushållsvatten verket levererar. Av denna anledning föreskrivs att anmälningsskyldig-

heten ska gälla även vattentjänstverk som tar emot minst 5 000 kubikmeter avloppsvatten per dygn.

Endast betydande störningssituationer i vattentjänsterna ska anmälas. Närmare bestämmelser om vilka omständigheter som ska beaktas i bedömningen av huruvida en störning är betydande får utfärdas genom en i 4 mom. avsedd förordning av jord- och skogsbruksministeriet.

Enligt *1 mom*. kan närings-, trafik- och miljöcentralen ålägga ett verk att informera om en störningssituation. I allmänhet räcker det att kunderna och myndigheterna inom verkets verksamhetsområde enligt lagen om vattentjänster samt verkets eventuella kunder utanför verksamhetsområdet informeras om störningen och de åtgärder som den kräver. Det är dock närings-, trafik- och miljöcentralen som överväger från fall till fall vad informationen ska innehålla och hur omfattande den ska vara. Närings-, trafik- och miljöcentralen kan också anse det vara ändamålsenligt att helt eller delvis själv informera om saken.

Enligt *2 mom.* ska den anmälnings- och informationsskyldighet som fastställs för vattentjänstverken i 1 mom. gälla även anläggningar som levererar vatten till eller tar emot avloppsvatten från ett vattentjänstverk.

Enligt *3 mom.* ska närings-, trafik- och miljöcentralen vidarebefordra anmälan om en betydande störning i vattentjänster för kännedom till jord- och skogsbruksministeriet. På så sätt förmedlas informationen vid behov också vidare till statsrådets lägesbildscentral. Närings-, trafik- och miljöcentralen ska dessutom bedöma vilka eventuella konsekvenser störningen får i en annan medlemsstat i Europeiska unionen och vid behov rapportera om störningen till den behöriga myndigheten i den berörda medlemsstaten. En rapport kan lämnas t.ex. när en störning kan ha en betydande inverkan på kontinuiteten i distributionen av hushållsvatten i en annan medlemsstat.

Enligt *1 och 3 mom*. ska vattentjänstverket och närings-, trafik- och miljöcentralen anmäla om betydande störningssituationer i vattentjänsterna oberoende av vilken orsak som ligger bakom dem. Anmälningsskyldigheten gäller således också en sådan i direktivet om nät- och informationssäkerhet avsedd betydande informationssäkerhetsrelaterad störning som drabbar verkets informationssystem eller de kommunikationsnät som verket använder och som kan leda till att distributionen av hushållsvatten avbryts i betydande omfattning eller att uppfyllandet av kvalitetskraven på hushållsvatten äventyras avsevärt. Verkets informationssystem och kommunikationsnät kan bestå av privata kommunikationsnät och informationssystem som antingen förvaltas av tjänsteleverantörens interna it-personal eller vilkas säkerhet har lagts ut på entreprenad. Informationssystemen kan bestå t.ex. av sådan teleterminalutrustning som avses i 3 § 25 punkten i informationssamhällsbalken eller av data som förvaras, behandlas, söks eller överförs i dessa system.

När det gäller genomförandet av direktivet om nät- och informationssäkerhet bygger paragrafens 3 mom. på samma grunder som det 275 § 3 mom. som föreslås ingå i informationssamhällsbalken. Om det är fråga om en sådan it-säkerhetsincident som avses i direktivet kan närings-, trafik- och miljöcentralen begära att Kommunikationsverket ska vidarebefordra anmälan till en sådan gemensam kontaktpunkt i en annan medlemsstat som avses i artikel 8 i direktivet om nät- och informationssäkerhet.

Enligt *4 mom*. får jord- och skogsbruksministeriet utfärda närmare bestämmelser om när en sådan störning i vattentjänster som avses i 1 mom. ska anses vara betydande. Genom förord-

ning kan närmare bestämmelser också utfärdas om innehållet i och utformningen av de anmälningar som avses i 1 mom. och hur de ska lämnas in.

35 §. *Tystnadsplikt.*

Tystnadsplikt. Det föreslås att *2 mom. ändras så att den som utför uppgifter som avses i lagen får lämna ut sekretessbelagd information* också till Kommunikationsverket när detta är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter. Denna information kan innefatta exempelvis uppgifter om sådana informationssäkerhetsrelaterade störningar i vattentjänsterna som avses i 15 b §. Genom den föreslagna bestämmelsen genomförs artikel 10 i direktivet om nät- och informationssäkerhet när det gäller sektor 6 i bilaga II till direktivet.

1.11 Lagen om ändring av lagen om Finansinspektionen

50 n §. *Verksamhet som behörig myndighet enligt direktivet om nät- och informationssäkerhet.* I paragrafen fastställs att Finansinspektionen verkar som en i artikel 8.1 i direktivet om nät- och informationssäkerhet avsedd behörig myndighet när det gäller sektorerna 3 och 4 i bilaga II till direktivet. Bestämmelsen är förtydligande, eftersom tillsynsuppgifterna enligt direktivet om nät- och informationssäkerhet redan nu kan anses höra till Finansinspektionens uppgifter enligt den gällande lagstiftningen.

52 a §. *Samarbete och utbyte av information vid skötseln av uppgifter enligt direktivet om nät- och informationssäkerhet.* I paragrafen fastställs att Finansinspektionen är skyldig att samarbeta med Kommunikationsverket och andra behövliga myndigheter vid skötseln av uppgifter enligt direktivet om nät- och informationssäkerhet och har rätt att utbyta sekretessbelagd information för detta syfte. Andra behövliga myndigheter förutom Kommunikationsverket kan vara myndigheter som enligt direktivet för nät- och informationssäkerhet är behöriga inom andra sektorer enligt bilaga II till direktivet (inom trafiksektorn Trafiksäkerhetsverket, inom energisektorn Energimyndigheten, inom hälso- och sjukvården Tillstånds- och tillsynsverket för social- och hälsovården samt inom distributionen av dricksvatten närings-, trafik- och miljöcentralen), andra ministerier samt behöriga myndigheter i andra medlemsstater i EU. Denna information kan innefatta exempelvis uppgifter om störningar i informationssäkerheten. Genom den föreslagna bestämmelsen genomförs artikel 10 i direktivet om nät- och informationssäkerhet när det gäller sektorerna 3 och 4 i bilaga II till direktivet.

2 Ikraftträdande

Det föreslås att lagarna ska träda i kraft den 1 maj 2018.

3 Förhållande till grundlagen samt lagstiftningsordning

Skydd för privatlivet. Enligt 10 § 1 mom. i grundlagen är vars och ens privatliv, heder och hemfrid tryggade. I samma moment konstateras att närmare bestämmelser om skydd för personuppgifter utfärdas genom lag. Enligt grundlagsutskottets praxis begränsas lagstiftarens spelrum förutom av denna bestämmelse även av att skyddet för personuppgifter utgör en del av skyddet för privatlivet i samma moment. Propositionen försvagar inte skyddet för privatlivet. Både Europeiska domstolen för de mänskliga rättigheterna och Europeiska unionens domstol har i sin rättspraxis när det gäller artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna respektive artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna ansett att rätten till respekt för privatlivet i fråga om behandlingen av personuppgifter omfattar alla slags uppgifter som rör en

fysisk person som är namngiven eller annars går att identifiera. Begreppet personuppgifter är brett, och även sådana anmälningar om störningar i informationssäkerheten som ska lämnas till tillsynsmyndigheterna kan i vissa fall innehålla personuppgifter. I regel kan det dock anses att så inte är fallet. Vidare ska det noteras att utgångsläget när det gäller skyddet för privatlivet respektive personuppgifter är att juridiska personer inte omfattas av tillämpningsområdet för dessa rättigheter. Om störningsanmälningarna innehåller personuppgifter ska dessa behandlas i enlighet med lagstiftningen om behandling av personuppgifter. Behandling av personuppgifter ska bygga på en behandlingsgrund enligt personuppgiftslagen. Enligt personuppgiftslagen får personuppgifter behandlas om behandlingen föranleds av en uppgift eller förpliktelse som anvisas den registeransvarige i lag eller som påförts honom med stöd av lag. Metadata från elektronisk kommunikation kan behandlas endast i enlighet med informationssamhällsbalken.

Bemyndiganden. Enligt 80 § 1 mom. i grundlagen kan statsrådet utfärda förordningar med stöd av ett bemyndigande i grundlagen eller i någon annan lag. Genom lag ska dock utfärdas bestämmelser om grunderna för individens rättigheter och skyldigheter samt om frågor som enligt grundlagen i övrigt hör till området för lag. När det gäller bemyndigande i lag har grundlagsutskottet i sin praxis ställt krav på exakt och noggrant avgränsad reglering (t.ex. GrUU 33/2004 rd, s. 4-6, GrUU 47/2001 rd, s. 2–3, GrUU 38/2013 rd, s. 3–4,GrUU 11/2016 rd, s. 2–3, GrUU 26/2017 rd, s. 26–28).

Enligt 80 § 2 mom. i grundlagen kan även andra myndigheter genom lag bemyndigas att utfärda rättsnormer i bestämda frågor, om det med hänsyn till föremålet för regleringen finns särskilda skäl och regleringens betydelse i sak inte kräver att den sker genom lag eller förordning. Tillämpningsområdet för ett sådant bemyndigande ska vara exakt avgränsat. Grundlagen bestämmer även att de saker bemyndigandet täcker ska definieras exakt i lagen. När ett bemyndigande bestäms i lag har grundlagsutskottets utlåtanden riktat krav på att bestämmelserna ska vara precisa och exakta (GrUU 16/2002 rd, s. 2, GrUU 19/2002 rd s. 5, GrUU 1/2004 rd, s. 2, GrUU 17/2010 rd, s. 2). I samband med grundlagsreformen angavs som exempel på myndigheternas normgivningsbefogenhet en teknisk reglering som innehåller få detaljer och inte inbegriper prövningsrätt i någon större utsträckning (RP 1/1998 rd, s. 133/II; se även GrUU 16/2002 rd, s. 2/I och GrUU 19/2002 rd, s. 5/I).

I propositionen föreslås det att det ska vara möjligt att genom förordning av statsrådet utfärda närmare bestämmelser om när en flygplats eller hamn måste anses vara samhällsviktig (128 § 5 mom. i lagen om ändring av luftfartslagen samt 7 e § 6 mom. i lagen om ändring av lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet). Genom förordning preciseras vilka flygplatser eller hamnar som ska betraktas som samhällsviktiga. I motiveringen konstateras att när det bedöms huruvida det är fråga om en samhällsviktig aktör ska de kriterier som anges i artikel 5.2 i direktivet om nät- och informationssäkerhet beaktas. Det är motiverat att föreskriva om dessa preciseringar på förordningsnivå, eftersom en reglering på lagnivå blir onödigt detaljerad och fallspecifik. Genom förordning utfärdas inte allmänna rättsregler om frågor som hör till området för lag och föreskrivs inte heller om grunderna för individens rättigheter och skyldigheter. Bemyndigandet att utfärda förordning har dessutom placerats i samband med den grundläggande bestämmelsen på det sätt som grundlagsutskottet förutsätter.

Genom de föreslagna lagarna ges nya bemyndiganden att utfärda föreskrifter enligt följande: Till Kommunikationsverket i 275 § 4 mom. i lagen om ändring av informationssamhällsbalken, till Trafiksäkerhetsverket i 128 b § 4 mom. i lagen om ändring av luftfartslagen, 41 a § 6 mom. i lagen om ändring av järnvägslagen, 18 a § 5 mom. i lagen om ändring av lagen om fartygstrafikservice, 7 f § 4 mom. i lagen om ändring av lagen om sjöfartsskydd på vissa fartyg

och i hamnar som betjänar dem och om tillsyn över skyddet, 7 § 6 mom. i lagen om ändring av lagen om transportservice, till Energimyndigheten i 29 a § 5 mom. i lagen om ändring av lagen om elmarknadslagen och i 34 a § 4 mom. i naturgasmarknadslagen samt till jord- och skogsbruksministeriet bemyndigande att utfärda förordning i 15 b § 3 mom. i lagen om ändring av lagen om vattentjänster.

Bemyndigandena har tagits in i och i sak anknutits till de paragrafer som berör de aktuella frågorna. I föreskrifterna regleras exempelvis formella och tekniska frågor avseende innehållet i anmälningar om störningar i informationssäkerheten samt i närmare detalj det sätt på vilket anmälningarna ska göras. Bemyndigandena gäller reglering som berör frågor av teknisk karaktär och detaljer av ringa betydelse, som inte innefattar utövning av betydande prövningsrätt.

På ovan anförda grunder är tillämpningsområdet för de bemyndiganden som föreslås i propositionen exakt och noggrant avgränsat, och bemyndigandena anses inte stå i strid med grundlagen.

På ovan anförda grunder föreslås det att lagförslagen kan behandlas i vanlig lagstiftningsordning.

Med stöd av vad som anförts ovan föreläggs riksdagen följande lagförslag:

Lagförslag

1.

Lag

om ändring av informationssamhällsbalken

I enlighet med riksdagens beslut

ändras i informationssamhällsbalken (917/2014) 275 §, 304 § 1 mom. 7 och 10 punkten samt 313 § 2 mom. 2 punkten och

fogas till lagen en ny 247 a §, till 308 §, sådan den lyder delvis ändrad i lag 456/2016, ett nytt 3 mom. samt till 318 §, sådan den lyder delvis ändrad i lag 456/2016, ett nytt 2 mom., varvid det nuvarande 2-4 mom. blir 3-5 mom., som följer:

247 a §

Skyldighet för den som tillhandahålle av internetbaserade marknadsplatser, sökmotortjänster och molntjänster att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem

Den som tillhandahåller en internetbaserad marknadsplats, en internetbaserad sökmotortjänst eller en molntjänst ska sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som denne använder. Vid riskhanteringen ska hänsyn tas till

1) systems och anläggningars säkerhet,
2) hantering av hot mot informationssäkerheten och av störningar,
3) driftskontinuitetshantering,
4) övervakning, revision och testning,
5) efterlevnad av internationella standarder.

Den riskhanteringskyldighet som avses i 1 mom. gäller inte sådana mikroföretag och små företag som avses i artikel 16.11 i Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen, nedan *direktivet om nät- och informationssäkerhet*.

275 §

Störningsanmälningar till Kommunikationsverket

Ett teleföretag ska utan dröjsmål göra en anmälan till Kommunikationsverket om dess tjänster utsätts för eller hotas av betydande kränkningar av informationssäkerheten eller av någonting annat som gör att en kommunikationstjänst inte fungerar eller väsentligen stör den. Teleföretaget ska också utan obefogat dröjsmål anmäla hur länge störningen eller hotet beräknas pågå, om vilka verkningar störningen eller hotet har, om avhjälpande åtgärder samt om åtgärder för att förhindra att störningen upprepas. Kommunikationsverket ska årligen sända kommissionen och Europeiska unionens byrå för nät- och informationssäkerhet en sammanfattande informationsrapport om anmälningarna.

En i 247 a § avsedd aktör som tillhandahåller en internetbaserad marknadsplats, en internetbasera sökmotortjänst eller en molntjänst ska utan dröjsmål göra en anmälan till Kommunikationsverket om dess tjänster utsätts för en betydande informationssäkerhetsrelaterad störning.

Om det ligger i allmänt intresse att det görs en anmälan om en störning kan Kommunikationsverket ålägga teleföretaget eller den som tillhandahåller tjänsten att informera om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.

Kommunikationsverket får meddela närmare föreskrifter om när en störning som avses i 1 mom. är betydande samt föreskrifter om innehållet i de anmälningar som avses i 1 och 2 mom. samt anmälningarnas utformning och hur de lämnas in.

Kommunikationsverket ska bedöma om en sådan störning som avses i 2 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna.

304 §

Kommunikationsverkets särskilda uppgifter

Utöver vad som föreskrivs någon annanstans i denna lag ska Kommunikationsverket

— —

7) samla in information om kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster, mervärdestjänster och informationssystem samt om fel och störningar i kommunikationsnät och kommunikationstjänster,

— —

10) utreda kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster, mervärdestjänster och informationssystem,

— —

308 §

Myndighetssamarbete

— —

Kommunikationsverket ska samarbeta med de myndigheter som utövar tillsyn över nät- och informationssäkerheten i övriga medlemsstater i Europeiska unionen, med enheter för hantering av it-säkerhetsincidenter samt med den samarbetsgrupp som avses i artikel 11 i direktivet om nät- och informationssäkerhet. Kommunikationsverket ska årligen sända samarbetsgruppen en sammanfattande rapport i enlighet med artikel 10.3 i direktivet.

313 §

Behandling av tillsynsärenden vid Kommunikationsverket

— —

Kommunikationsverket kan ställa sina tillsynsuppgifter enligt denna lag i viktighetsordning. Kommunikationsverket får lämna ett ärende utan prövning om

— —

2) ärendet trots en misstanke om fel eller försummelser endast har en ringa betydelse med tanke på kommunikationsmarknadens funktion, kommunikationstjänsternas tillförlitlighet eller tryggandet av störningsfri elektronisk kommunikation och med tanke på deras intressen som använder tjänsterna eller med tanke på riskhanteringen i fråga om de tjänster som avses i 247 a §, eller

— —

318 §

Utlämnande av information från myndigheter

— —

Kommunikationsverket har, trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information, rätt att lämna ut dokument som det fått eller upprättat i samband med sina uppgifter enligt lag samt att röja sekretessbelagd information för Trafiksäkerhetsverket, Energimyndigheten, Finansinspektionen, Tillstånds- och tillsynsverket för social- och hälsovården samt närings-, trafik- och miljöcentralen, om det är nödvändigt för skötseln av deras lagstadgade uppgifter i anslutning till informationssäkerhet.

— —

_____

Denna lag träder i kraft den 20 .

_____

2.

Lag

om ändring av luftfartslagen

I enlighet med riksdagens beslut
fogas till luftfartslagen (864/2014) en ny 128 a och en ny 128 b § som följer:

11 kap.

Luftfartsolyckor, efterspanings- och räddningstjänst för luftfart, tillbud och händelser

128 a §

Skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem

Leverantörer av flygtrafiktjänster samt samhällsviktiga flygplatsoperatörer ska sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som de använder.

Trafiksäkerhetsverket ska bedöma hur den riskhantering som avses i 1 mom. påverkar säkerheten inom luftfarten. Leverantörer av flygtrafiktjänster samt samhällsviktiga flygplatsoperatörer ska lämna Trafiksäkerhetsverket sådana uppgifter som behövs för denna bedömning. Verket får ålägga en leverantör av flygtrafiktjänster eller en samhällsviktig flygplatsoperatör att vidta korrigerande åtgärder för att eliminera en betydande risk för säkerheten inom luftfarten.

Trafiksäkerhetsverket har, trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information, rätt att lämna ut dokument som det fått eller upprättat i samband med sina uppgifter enligt 2 mom. samt att röja sekretessbelagd information för Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter.

Närmare bestämmelser om när en flygplats ska betraktas som samhällsviktig utfärdas genom förordning av statsrådet.

128 b §

Rapportering av informationssäkerhetshändelser

Leverantörer av flygtrafiktjänster samt samhällsviktiga flygplatsoperatörer ska utan dröjsmål lämna Trafiksäkerhetsverket en anmälan om betydande informationssäkerhetsrelaterade händelser som är riktade mot kommunikationsnät eller informationssystem.

Om det ligger i allmänt intresse att en händelse anmäls kan Trafiksäkerhetsverket ålägga den som tillhandahåller tjänsten att informera om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.

Trafiksäkerhetsverket ska bedöma om en sådan händelse som avses i 1 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna.

Trafiksäkerhetsverket får meddela närmare föreskrifter om när en händelse som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in.

_____

Denna lag träder i kraft den 20 .

_____

3.

Lag

om ändring av järnvägslagen

I enlighet med riksdagens beslut
fogas till järnvägslagen (304/2011) en ny 41 a § som följer:

6 kap.

Säkerhet

41 a §

Skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten

Förvaltaren av statens bannät samt den som tillhandahåller trafikledningstjänster ska sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som denne använder.

Förvaltaren av statens bannät samt den som tillhandahåller trafikledningstjänster ska utan dröjsmål lämna Trafiksäkerhetsverket en anmälan om betydande informationssäkerhetsrelaterade störningar som är riktade mot kommunikationsnät eller informationssystem.

Om det ligger i allmänt intresse att en störning anmäls kan Trafiksäkerhetsverket ålägga den som tillhandahåller tjänsten att informera om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.

Trafiksäkerhetsverket ska bedöma om en sådan störning som avses i 2 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna.

Trafiksäkerhetsverket har, trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information, rätt att lämna ut dokument som det fått eller upprättat i samband med sina uppgifter enligt denna paragraf samt att röja sekretessbelagd information för Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter.

Trafiksäkerhetsverket får meddela närmare föreskrifter om när en sådan störning som avses i 2 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in.

———

Denna lag träder i kraft den 20 .

———

4.

Lag

om ändring av lagen om fartygstrafikservice

I enlighet med riksdagens beslut

fogas till 16 § i lagen om fartygstrafikservice (623/2005) ett nytt 5 mom., till lagen en ny 18 a § samt till 28 §, sådan den lyder delvis ändrad i lag (1307/2009), ett nytt 4 mom. som följer:

16 §

Upprätthållande av fartygstrafikservice

— —

VTS-myndigheten ska sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som denne använder.

18 a §

Anmälan om störningar i informationssäkerheten

VTS-myndigheten ska utan dröjsmål lämna Trafiksäkerhetsverket en anmälan om betydande informationssäkerhetsrelaterade störningar som är riktade mot kommunikationsnät eller informationssystem som denne använder.

Om det ligger i allmänt intresse att en störning anmäls kan Trafiksäkerhetsverket ålägga den som tillhandahåller tjänsten att informera om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.

Trafiksäkerhetsverket ska bedöma om en sådan störning som avses i 1 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna.

Trafiksäkerhetsverket får meddela närmare föreskrifter om när en sådan störning som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in.

Trafiksäkerhetsverket har, trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information, rätt att lämna ut dokument som det fått eller upprättat i samband med sina uppgifter enligt denna paragraf samt att röja sekretessbelagd information för Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter.

28 §

Tillsyn

— —

Trafiksäkerhetsverket ska bedöma hur den riskhantering som avses i 16 § 5 mom. påverkar säkerheten inom sjöfarten. Trafiksäkerhetsverket kan ålägga en aktör att vidta korrigerande åtgärder för att eliminera en betydande risk som inverkar på säkerheten inom sjöfarten. Åläggandet kan förenas med vite. Bestämmelser om vite finns i viteslagen (1113/1190).

_____

Denna lag träder i kraft den 20 . _____

5.

Lag

om ändring av lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet

I enlighet med riksdagens beslut

fogas till lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet (485/2004) en ny 7 e och en ny 7 f § som följer:

2 a kap.

Sjöfartsskyddet i hamnar

7 e §

Hamninnehavares skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem

Innehavare av samhällsviktiga hamnar ska sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som de använder.

Trafiksäkerhetsverket ska bedöma hur den riskhantering som avses i 1 mom. påverkar säkerheten inom sjöfarten. Verket kan ålägga en i 1 mom. avsedd hamninnehavare att vidta korrigerande åtgärder för att eliminera en betydande risk som inverkar på säkerheten inom sjöfarten. Åläggandet kan förenas med vite. Bestämmelser om vite finns i viteslagen (1113/1190).

Trafiksäkerhetsverket har, trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information, rätt att lämna ut dokument som det fått eller upprättat i samband med sina uppgifter enligt 2 mom. samt att röja sekretessbelagd information för Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter.

Bestämmelser om när en i 1 mom. avsedd hamn ska betraktas som samhällsviktig utfärdas genom förordning av statsrådet.

7 f §

Anmälan om störningar i informationssäkerheten

Innehavare av samhällsviktiga hamnar ska utan dröjsmål lämna Trafiksäkerhetsverket en anmälan om betydande informationssäkerhetsrelaterade störningar som är riktade mot kommunikationsnät eller informationssystem som de använder.

Om det ligger i allmänt intresse att en störning anmäls kan Trafiksäkerhetsverket ålägga den som tillhandahåller tjänsten att informera om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.

Trafiksäkerhetsverket ska bedöma om en sådan störning som avses i 1 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna.

Trafiksäkerhetsverket får meddela närmare föreskrifter om när en sådan störning som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in.

_____

Denna lag träder i kraft den 20 .

_____

6.

Lag

om ändring av lagen om transportservice

I enlighet med riksdagens beslut
fogas till lagen om transportservice (320/2017) III avd. 2 kap. en ny 7 § som följer:

7 §

Skyldighet för den som tillhandahåller intelligenta trafiksystem att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten

Den som tillhandahåller ett intelligent trafiksystem ska sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som denne använder.

Den som tillhandahåller ett intelligent trafiksystem ska utan dröjsmål lämna Trafiksäkerhetsverket en anmälan om betydande informationssäkerhetsrelaterade störningar, som är riktade mot sådana kommunikationsnät eller informationssystem som denne använder.

Om det ligger i allmänt intresse att en störning anmäls kan Trafiksäkerhetsverket ålägga den som tillhandahåller tjänsten att informera om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.

Trafiksäkerhetsverket ska bedöma om en sådan störning som avses i 2 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna.

Trafiksäkerhetsverket har, trots sekretessbestämmelserna eller andra begränsningar som gäller utlämnande av information, rätt att lämna ut dokument som det fått eller upprättat i samband med sina uppgifter enligt denna paragraf samt att röja sekretessbelagd information för Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter.

Trafiksäkerhetsverket får meddela närmare föreskrifter om när en sådan störning som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in.

———

Denna lag träder i kraft den 20 .

———

7.

Lag

om ändring av elmarknadslagen

I enlighet med riksdagens beslut

ändras i elmarknadslagen (588/2013) 62 § 1 mom., sådant det lyder i lag 590/2017, samt *fogas* till lagen en ny 29 a § som följer:

29 a §

Nätinnehavares skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten

Nätinnehavare ska sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som denne använder.

Nätinnehavare ska utan dröjsmål lämna Energimyndigheten en anmälan om sådana betydande informationssäkerhetsrelaterade störningar som är riktade mot kommunikationsnät eller informationssystem som denne använder och som kan leda till att eldistributionen i eldistributionsnätet avbryts i betydande omfattning.

Om det ligger i allmänt intresse att en störning anmäls kan Energimyndigheten ålägga den som tillhandahåller tjänsten att informera allmänheten om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.

Energimyndigheten ska bedöma om en sådan störning som avses i 2 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna.

Energimyndigheten får meddela närmare föreskrifter om när en sådan störning som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in.

62 §

Specialbestämmelser som gäller slutna distributionsnät

På slutna distributionsnät och deras innehavare tillämpas inte 23 och 26 a §, 27 § 3 mom., 28, 29, 29 a, 50–53, 53 a, 54–57, 57 a, 58 och 59 §.

———————————————————————————————————————

Denna lag träder i kraft den 20 .

8.

Lag

om ändring av naturgasmarknadslagen

I enlighet med riksdagens beslut
fogas till naturgasmarknadslagen (587/2017) en ny 34 a § som följer:

34 a §

Överföringsnätinnehavares skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten

Överföringsnätinnehavaren ska sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som denne använder.

Överföringsnätinnehavaren ska utan dröjsmål lämna Energimyndigheten en anmälan om sådana betydande informationssäkerhetsrelaterade störningar som är riktade mot kommunikationsnät eller informationssystem som denne använder och som kan leda till att naturgasdistributionen i överföringsnätet avbryts i betydande omfattning.

Om det ligger i allmänt intresse att en störning anmäls kan Energimyndigheten ålägga överföringsnätinnehavaren att informera allmänheten om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.

Energimyndigheten ska bedöma om en sådan störning som avses i 2 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna.

Energimyndigheten får meddela närmare föreskrifter om när en sådan störning som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in.

———

Denna lag träder i kraft den 20 .

———

9.

Lag

om ändring av 27 och 28 § i lagen om tillsyn över el- och naturgasmarknaden

I enlighet med riksdagens beslut

ändras i lagen om tillsyn över el- och naturgasmarknaden (590/2013) 27 §, rubriken för 28 §, det inledande stycket i 28 § 1 mom. och 28 § 1 mom. 1 punkten samt 2 och 3 mom. som följer:

27 §

Myndigheternas tillsynssamarbete

I frågor som hör till Energimyndighetens behörighet har verket rätt att utöva tillsynssamarbete med Finansinspektionen, Konkurrens- och konsumentverket, Kommunikationsverket, konsumentombudsmannen, byrån för samarbete mellan energitillsynsmyndigheter, en annan EES-stats tillsynsmyndighet och Europeiska kommissionen samt på begäran ge handräckning då dessa utför tillsyns- eller kontrolluppgifter som hänför sig till ett elföretag eller naturgasföretag.

28 §

Energimyndighetens rätt att lämna ut uppgifter till andra myndigheter

Utöver det som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999) har Energimyndigheten rätt att trots bestämmelserna om sekretess lämna ut uppgifter till

1) Finansinspektionen, Konkurrens- och konsumentverket och konsumentombudsmannen för att de ska kunna sköta sina uppgifter, och till Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter,

— —

Energimyndigheten har rätt att lämna ut endast sådana uppgifter som behövs för att den berörda myndigheten ska kunna utföra sina uppgifter, och om uppgifter lämnas ut till en utländsk myndighet eller ett internationellt organ förutsätts det dessutom att dessa har motsvarande sekretess som Energimyndigheten i fråga om de uppgifter som lämnas ut.

Energimyndigheten får inte lämna ut sekretessbelagda uppgifter som myndigheten fått av en myndighet i en annan stat eller ett internationellt organ, om inte den myndighet som gett uppgifterna har gett sitt uttryckliga samtycke till att uppgifterna lämnas ut. Uppgifterna får endast användas för skötsel av de uppgifter som avses i denna lag eller för de ändamål som samtycket getts för.

———

Denna lag träder i kraft den 20 .

———

10.

Lag

om ändring av lagen om vattentjänster

I enlighet med riksdagens beslut
ändras i lagen om vattentjänster (119/2001) 35 § 2 mom. och
fogas till lagen en ny 15 b § som följer:

15 b §

Anmälan om störningar i vattentjänster

Ett vattentjänstverk som levererar eller tar emot avloppsvatten till en volym om minst 5 000 kubikmeter vatten per dygn ska utan dröjsmål anmäla betydande störningar i vattentjänsterna till närings-, trafik- och miljöcentralen. Närings-, trafik- och miljöcentralen kan efter att ha mottagit anmälan ålägga vattentjänstverket att informera om saken eller, efter att ha hört vattentjänstverket, själv informera om saken.

Bestämmelserna om vattentjänstverk i 1 mom. gäller också anläggningar som levererar vatten till ett vattentjänstverk eller som tar emot avloppsvatten från ett vattentjänstverk.

Närings-, trafik- och miljöcentralen ska vidarebefordra den anmälan som avses i 1 mom. för kännedom till jord- och skogsbruksministeriet. Närings-, trafik- och miljöcentralen ska dessutom bedöma om en sådan störning som avses i 1 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta den behöriga myndigheten i den berörda medlemsstaten.

Närmare bestämmelser om när en sådan störning som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in får utfärdas genom förordning av jord- och skogsbruksministeriet..

35 §

Tystnadsplikt

— —

Utan hinder av tystnadsplikten enligt lagen om offentlighet i myndigheternas verksamhet får uppgifter om enskildas eller sammanslutningars ekonomiska ställning eller affärs- eller yrkeshemligheter eller enskildas personliga förhållanden, som erhållits vid utförande av åligganden enligt denna lag, lämnas ut till

— —

1) tillsynsmyndigheten för utförande av uppgifter som avses i denna lag,
2) åklagar- och polismyndigheter för utredande av brott,
3) Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter.

———

Denna lag träder i kraft den 20 .

———

11.

Lag

om ändring av lagen om Finansinspektionen

I enlighet med riksdagens beslut
fogas till lagen om Finansinspektionen (878/2008) en ny 50 n och en ny 52 a § som följer:

50 n §

Behörig myndighet enligt direktivet om nät- och informationssäkerhet

Finansinspektionen är behörig myndighet enligt artikel 8.1 i Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen, nedan *direktivet om nät- och informationssäkerhet*, när det gäller sektorerna 3 och 4 i bilaga II till direktivet.

52 a §

Samarbete och utbyte av information vid skötseln av uppgifter enligt direktivet om nät- och informationssäkerhet

Finansinspektionen ska samarbeta med Kommunikationsverket och andra behövliga myndigheter vid skötseln av uppgifter enligt direktivet om nät- och informationssäkerhet. Finansinspektionen har rätt att för detta ändamål trots sekretessbestämmelserna utbyta information med Kommunikationsverket och andra behövliga myndigheter.

Denna lag träder i kraft den 20 .

Helsinfors den 19 december 2017

Statsminister

Juha Sipilä

Kommunikationsminister Anne Berner

Parallelltext

1.

Lag

om ändring av informationssamhällsbalken

I enlighet med riksdagens beslut

ändras i informationssamhällsbalken (917/2014) 275 §, 304 § 1 mom. 7 och 10 punkten samt 313 § 2 mom. 2 punkten och

fogas till lagen en ny 247 a §, till 308 §, sådan den lyder delvis ändrad i lag 456/2016 ett nytt 3 mom., samt till 318 §, sådan den lyder delvis ändrad i lag 456/2016, ett nytt 2 mom., varvid det nuvarande 2, 3 och 4 mom. blir 3, 4, och 5 mom., som följer:

Gällande lydelse	Föreslagen lydelse
	247 a §
nya	*Skyldighet för den som tillhandahålle av internetbaserade marknadsplatser, sökmotortjänster och molntjänster att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem*
	Den som tillhandahåller en internetbaserad marknadsplats, en internetbaserad sökmotortjänst eller en molntjänst ska sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som denne använder. Vid riskhanteringen ska hänsyn tas till *1) systems och anläggningars säkerhet,* *2) hantering av hot mot informationssäkerheten och av störningar,* *3) driftskontinuitetshantering,* *4) övervakning, revision och testning,* *5) efterlevnad av internationella standarder.* *Den riskhanteringskyldighet som avses i 1 mom. gäller inte sådana mikroföretag och små företag som avses i artikel 16.11 i Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen, nedan direktivet om nät- och informationssäkerhet.*

275 §

Störningsanmälningar till Kommunikationsverket

Ett teleföretag ska utan dröjsmål göra en anmälan till Kommunikationsverket om dess tjänster utsätts för eller hotas av betydande kränkningar av informationssäkerheten eller av någonting annat som gör att en kommunikationstjänst inte fungerar eller väsentligen stör den. Teleföretaget ska också utan obefogat dröjsmål anmäla hur länge störningen eller hotet beräknas pågå, om vilka verkningar störningen eller hotet har, om avhjälpande åtgärder samt om åtgärder för att förhindra att störningen upprepas. Om det ligger i allmänt intresse att det görs en anmälan om en störning kan Kommunikationsverket ålägga teleföretaget att informera om saken.

Kommunikationsverket får meddela närmare föreskrifter om när en störning som avses i 1 mom. är betydande samt föreskrifter om innehållet i anmälan samt anmälans utformning och hur den lämnas in.

Kommunikationsverket ska årligen sända kommissionen och Europeiska byrån för nät- och kommunikationssäkerhet en sammanfattande informationsrapport om de anmälningar som avses i 1 mom.

275 §

Störningsanmälningar till Kommunikationsverket

Ett teleföretag ska utan dröjsmål göra en anmälan till Kommunikationsverket om dess tjänster utsätts för eller hotas av betydande kränkningar av informationssäkerheten eller av någonting annat som gör att en kommunikationstjänst inte fungerar eller väsentligen stör den. Teleföretaget ska också utan obefogat dröjsmål anmäla hur länge störningen eller hotet beräknas pågå, om vilka verkningar störningen eller hotet har, om avhjälpande åtgärder samt om åtgärder för att förhindra att störningen upprepas. *Kommunikationsverket ska årligen sända kommissionen och Europeiska unionens byrå för nät- och informationssäkerhet en sammanfattande informationsrapport om anmälningarna.*

En i 247 a § avsedd aktör som tillhandahåller en internetbaserad marknadsplats, en internetbasera sökmotortjänst eller en molntjänst ska utan dröjsmål göra en anmälan till Kommunikationsverket om dess tjänster utsätts för en betydande informationssäkerhetsrelaterad störning.

Om det ligger i allmänt intresse att det görs en anmälan om en störning kan Kommunikationsverket ålägga teleföretaget eller den som tillhandahåller tjänsten att informera om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.

Kommunikationsverket får meddela närmare föreskrifter om när en störning som avses i 1 mom. är betydande samt föreskrifter om innehållet i de anmälningar som avses i 1 och 2 mom. samt anmälningarnas utformning och hur de lämnas in.

Kommunikationsverket ska bedöma om en sådan störning som avses i 2 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna.

304 §	304 §
Kommunikationsverkets särskilda uppgifter	*Kommunikationsverkets särskilda uppgifter*
Utöver vad som föreskrivs någon annanstans i denna lag ska Kommunikationsverket	Utöver vad som föreskrivs någon annanstans i denna lag ska Kommunikationsverket
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
7) samla in information om kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster och mervärdestjänster samt om fel och störningar i kommunikationsnät och kommunikationstjänster,	7) samla in information om kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster, mervärdestjänster *och informationssystem* samt om fel och störningar i kommunikationsnät och kommunikationstjänster,
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
10) utreda kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster och mervärdestjänster,	10) utreda kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster, mervärdestjänster och *informationssystem*,
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
	308 §
	Myndighetssamarbete
nya	— — — — — — — — — — — — — — — —
	Kommunikationsverket ska samarbeta med de myndigheter som utövar tillsyn över nät- och informationssäkerheten i övriga medlemsstater i Europeiska unionen, med enheter för hantering av it-säkerhetsincidenter samt med den samarbetsgrupp som avses i artikel 11 i direktivet om nät- och informationssäkerhet. Kommunikationsverket ska årligen sända samarbetsgruppen en sammanfattande rapport i enlighet med artikel 10.3 i direktivet.
313 §	313 §
Behandling av tillsynsärenden vid Kommunikationsverket	*Behandling av tillsynsärenden vid Kommunikationsverket*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Kommunikationsverket kan ställa sina tillsynsuppgifter enligt denna lag i viktighetsordning. Kommunikationsverket får lämna ett ärende utan prövning om	Kommunikationsverket kan ställa sina tillsynsuppgifter enligt denna lag i viktighetsordning. Kommunikationsverket får lämna ett ärende utan prövning om
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
2) ärendet trots en misstanke om fel eller	2) ärendet trots en misstanke om fel eller

försummelser endast har en ringa betydelse med tanke på kommunikationsmarknadens funktion, kommunikationstjänsternas tillförlitlighet eller tryggandet av störningsfri elektronisk kommunikation och med tanke på deras intressen som använder tjänsterna, eller	försummelser endast har en ringa betydelse med tanke på kommunikationsmarknadens funktion, kommunikationstjänsternas tillförlitlighet eller tryggandet av störningsfri elektronisk kommunikation och med tanke på deras intressen som använder tjänsterna *eller med tanke på riskhanteringen* i fråga om *de tjänster som avses i 247 a §*, eller
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
	318 §
	Utlämnande av information från myndigheter
nya	— — — — — — — — — — — — — — — —
	Kommunikationsverket har, trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information, rätt att lämna ut dokument som det fått eller upprättat i samband med sina uppgifter enligt lag samt att röja sekretessbelagd information för Trafiksäkerhetsverket, Energimyndigheten, Finansinspektionen, Tillstånds- och tillsynsverket för social- och hälsovården samt närings-, trafik- och miljöcentralen, om det är nödvändigt för skötseln av deras lagstadgade uppgifter i anslutning till informationssäkerhet.
	— — — — — — — — — — — — — — — —

2.

Lag

om ändring av luftfartslagen

I enlighet med riksdagens beslut
fogas till luftfartslagen (864/2014) en ny 128 a och en ny 128 b § som följer:

Gällande lydelse	Föreslagen lydelse
	11 kap.
	Luftfartsolyckor, efterspanings- och räddningstjänst för luftfart, tillbud och händelser
nya	128 a §
	Skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem
	Leverantörer av flygtrafiktjänster samt samhällsviktiga flygplatsoperatörer ska sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som de använder.
	Trafiksäkerhetsverket ska bedöma hur den riskhantering som avses i 1 mom. påverkar säkerheten inom luftfarten. Leverantörer av flygtrafiktjänster samt samhällsviktiga flygplatsoperatörer ska lämna Trafiksäkerhetsverket sådana uppgifter som behövs för denna bedömning. Verket får ålägga en leverantör av flygtrafiktjänster eller en samhällsviktig flygplatsoperatör att vidta korrigerande åtgärder för att eliminera en betydande risk för säkerheten inom luftfarten.
	Trafiksäkerhetsverket har, trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information, rätt att lämna ut dokument som det fått eller upprättat i samband med sina uppgifter enligt 2 mom. samt att röja sekretessbelagd information för Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter.

Närmare bestämmelser om när en flygplats ska betraktas som samhällsviktig utfärdas genom förordning av statsrådet.

128 b §

Rapportering av informationssäkerhetshändelser

nya

Leverantörer av flygtrafiktjänster samt samhällsviktiga flygplatsoperatörer ska utan dröjsmål lämna Trafiksäkerhetsverket en anmälan om betydande informationssäkerhetsrelaterade händelser som är riktade mot kommunikationsnät eller informationssystem.

Om det ligger i allmänt intresse att en händelse anmäls kan Trafiksäkerhetsverket ålägga den som tillhandahåller tjänsten att informera om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.

Trafiksäkerhetsverket ska bedöma om en sådan händelse som avses i 1 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna.

Trafiksäkerhetsverket får meddela närmare föreskrifter om när en händelse som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in.

3.

Lag

om ändring av järnvägslagen

I enlighet med riksdagens beslut
fogas till järnvägslagen (304/2011) en ny 41 a § som följer:

Gällande lydelse	Föreslag lydelse
	6 kap.
	Säkerhet
nya	41 a §
	Skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten
	Förvaltaren av statens bannät samt den som tillhandahåller trafikledningstjänster ska sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som denne använder.
	Förvaltaren av statens bannät samt den som tillhandahåller trafikledningstjänster ska utan dröjsmål lämna Trafiksäkerhetsverket en anmälan om betydande informationssäkerhetsrelaterade störningar som är riktade mot kommunikationsnät eller informationssystem.
	Om det ligger i allmänt intresse att en störning anmäls kan Trafiksäkerhetsverket ålägga den som tillhandahåller tjänsten att informera om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.
	Trafiksäkerhetsverket ska bedöma om en sådan störning som avses i 2 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna.
	Trafiksäkerhetsverket har, trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information, rätt

att lämna ut dokument som det fått eller upprättat i samband med sina uppgifter enligt denna paragraf samt att röja sekretessbelagd information för Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter.

Trafiksäkerhetsverket får meddela närmare föreskrifter om när en sådan störning som avses i 2 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in.

4.

Lag

om ändring av lagen om fartygstrafikservice

I enlighet med riksdagens beslut

fogas till 16 § i lagen om fartygstrafikservice (623/2005) ett nytt 5 mom., till lagen en ny 18 a § samt till 28 §, sådan den lyder delvis ändrad i lag (1307/2009), ett nytt 4 mom. som följer:

Gällande lydelse	Föreslagen lydelse
	16 §
	Upprätthållande av fartygstrafikservice
	— — — — — — — — — — — — — —
	VTS-myndigheten ska sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som denne använder.
	18 a §
nya	*Anmälan om störningar i informationssäkerheten*
	VTS-myndigheten ska utan dröjsmål lämna Trafiksäkerhetsverket en anmälan om betydande informationssäkerhetsrelaterade störningar som är riktade mot kommunikationsnät eller informationssystem som denne använder.
	Om det ligger i allmänt intresse att en störning anmäls kan Trafiksäkerhetsverket ålägga den som tillhandahåller tjänsten att informera om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.
	Trafiksäkerhetsverket ska bedöma om en sådan störning som avses i 1 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna.
	Trafiksäkerhetsverket får meddela närmare föreskrifter om när en sådan störning som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan

och hur den ska lämnas in.

Trafiksäkerhetsverket har, trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information, rätt att lämna ut dokument som det fått eller upprättat i samband med sina uppgifter enligt denna paragraf samt att röja sekretessbelagd information för Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter.

28 §

Tillsyn

— — — — — — — — — — — — — — —

Trafiksäkerhetsverket ska bedöma hur den riskhantering som avses i 16 § 5 mom. påverkar säkerheten inom sjöfarten. Trafiksäkerhetsverket kan ålägga en aktör att vidta korrigerande åtgärder för att eliminera en betydande risk som inverkar på säkerheten inom sjöfarten. Åläggandet kan förenas med vite. Bestämmelser om vite finns i viteslagen (1113/1190).

5.

Lag

om ändring av lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet

I enlighet med riksdagens beslut

fogas till lagen om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet (485/2004) en ny 7 e och en ny 7 f § som följer:

Gällande lydelse	Föreslagen lydelse
	2 a kap.
	Sjöfartsskyddet i hamnar
nya	7 e §
	Hamninnehavares skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem
	Innehavare av samhällsviktiga hamnar ska sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som de använder.
	Trafiksäkerhetsverket ska bedöma hur den riskhantering som avses i 1 mom. påverkar säkerheten inom sjöfarten. Verket kan ålägga en i 1 mom. avsedd hamninnehavare att vidta korrigerande åtgärder för att eliminera en betydande risk som inverkar på säkerheten inom sjöfarten. Åläggandet kan förenas med vite. Bestämmelser om vite finns i viteslagen (1113/1190).
	Trafiksäkerhetsverket har, trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information, rätt att lämna ut dokument som det fått eller upprättat i samband med sina uppgifter enligt 2 mom. samt att röja sekretessbelagd information för Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter.
	Bestämmelser om när en i 1 mom. avsedd hamn ska betraktas som samhällsviktig ut-

färdas genom förordning av statsrådet.

7 f §

nya

Anmälan om störningar i informationssäkerheten

Innehavare av samhällsviktiga hamnar ska utan dröjsmål lämna Trafiksäkerhetsverket en anmälan om betydande informationssäkerhetsrelaterade störningar som är riktade mot kommunikationsnät eller informationssystem som de använder.

Om det ligger i allmänt intresse att en störning anmäls kan Trafiksäkerhetsverket ålägga den som tillhandahåller tjänsten att informera om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.

Trafiksäkerhetsverket ska bedöma om en sådan störning som avses i 1 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna.

Trafiksäkerhetsverket får meddela närmare föreskrifter om när en sådan störning som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in.

6.

Lag

om ändring av lagen om transportservice

I enlighet med riksdagens beslut
fogas till lagen om transportservice (320/2017) III avd. 2 kap. en ny 7 § som följer:

Gällande lydelse	Föreslagen lydelse
	7 §
nya	*Skyldighet för den som tillhandahåller intelligenta trafiksystem att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten*
	Den som tillhandahåller ett intelligent trafiksystem ska sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som denne använder. *Den som tillhandahåller ett intelligent trafiksystem ska utan dröjsmål lämna Trafiksäkerhetsverket en anmälan om betydande informationssäkerhetsrelaterade störningar, som är riktade mot sådana kommunikationsnät eller informationssystem som denne använder.* *Om det ligger i allmänt intresse att en störning anmäls kan Trafiksäkerhetsverket ålägga den som tillhandahåller tjänsten att informera om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.* *Trafiksäkerhetsverket ska bedöma om en sådan störning som avses i 2 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna.* *Trafiksäkerhetsverket har, trots sekretessbestämmelserna eller andra begränsningar som gäller utlämnande av information, rätt att lämna ut dokument som det fått eller upprättat i samband med sina uppgifter enligt denna paragraf samt att röja sekretessbelagd information för Kommunikationsverket, om*

det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter.

Trafiksäkerhetsverket får meddela närmare föreskrifter om när en sådan störning som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in.

7.

Lag

om ändring av elmarknadslagen

I enlighet med riksdagens beslut
ändras i elmarknadslagen (588/2013) 62 § 1 mom., sådant det lyder i lag 590/2017, samt *fogas* till lagen en ny 29 a § som följer:

Gällande lydelse	Föreslagen lydelse
	29 a §
nya	*Nätinnehavares skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten*
	Nätinnehavare ska sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som denne använder. *Nätinnehavare ska utan dröjsmål lämna Energimyndigheten en anmälan om sådana betydande informationssäkerhetsrelaterade störningar som är riktade mot kommunikationsnät eller informationssystem som denne använder och som kan leda till att eldistributionen i eldistributionsnätet avbryts i betydande omfattning.* *Om det ligger i allmänt intresse att en störning anmäls kan Energimyndigheten ålägga den som tillhandahåller tjänsten att informera allmänheten om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.* *Energimyndigheten ska bedöma om en sådan störning som avses i 2 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna.* *Energimyndigheten får meddela närmare föreskrifter om när en sådan störning som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in.*

62 §	62 §
Specialbestämmelser som gäller slutna distributionsnät	*Specialbestämmelser om slutna distributionsnät*
På slutna distributionsnät och deras innehavare tillämpas inte 23 och 26 a §, 27 § 3 mom., 28, 29, 50–53, 53 a, 54–57, 57 a, 58 och 59 §.	På slutna distributionsnät och deras innehavare tillämpas inte 23 och 26 a §, 27 § 3 mom., 28, 29, *29 a*, 50–53, 53 a, 54–57, 57 a, 58 och 59 §.

8.

Lag

om ändring av naturgasmarknadslagen

I enlighet med riksdagens beslut
fogas till naturgasmarknadslagen (587/2017) en ny 34 a § som följer:

Gällande lydelse	Föreslagen lydelse
	34 a §
nya	*Överföringsnätinnehavares skyldighet att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem samt anmälan om störning i informationssäkerheten*
	Överföringsnätinnehavaren ska sörja för riskhanteringen i fråga om de kommunikationsnät och informationssystem som denne använder.
	Överföringsnätinnehavaren ska utan dröjsmål lämna Energimyndigheten en anmälan om sådana betydande informationssäkerhetsrelaterade störningar som är riktade mot kommunikationsnät eller informationssystem som denne använder och som kan leda till att naturgasdistributionen i överföringsnätet avbryts i betydande omfattning.
	Om det ligger i allmänt intresse att en störning anmäls kan Energimyndigheten ålägga överföringsnätinnehavaren att informera allmänheten om saken eller, efter att ha hört den anmälningspliktiga, själv informera om saken.
	Energimyndigheten ska bedöma om en sådan störning som avses i 2 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta de berörda medlemsstaterna.
	Energimyndigheten får meddela närmare föreskrifter om när en sådan störning som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in.

9.

Lag

om ändring av 27 och 28 § i lagen om tillsyn över el- och naturgasmarknaden

I enlighet med riksdagens beslut

ändras i lagen om tillsyn över el- och naturgasmarknaden (590/2013) 27 §, rubriken för 28 §, det inledande stycket i 28 § 1 mom. och 28 § 1 mom. 1 punkten samt 2 och 3 mom. som följer:

Gällande lydelse	Förslagen lydelse
27 §	27 §
Myndigheternas tillsynssamarbete	*Myndigheternas tillsynssamarbete*
I frågor som hör till Energimarknadsverkets behörighet har verket rätt att utöva tillsynssamarbete med Finansinspektionen, Konkurrens- och konsumentverket, konsumentombudsmannen, byrån för samarbete mellan energitillsynsmyndigheter, en annan EES-stats energitillsynsmyndighet och Europeiska kommissionen samt på begäran ge handräckning då dessa utför tillsyns- eller kontrolluppgifter som hänför sig till ett elföretag eller naturgasföretag.	I frågor som hör till *Energimyndighetens* behörighet har verket rätt att utöva tillsynssamarbete med Finansinspektionen, Konkurrens- och konsumentverket, *Kommunikationsverket*, konsumentombudsmannen, byrån för samarbete mellan energitillsynsmyndigheter, en annan EES-stats tillsynsmyndighet och Europeiska kommissionen samt på begäran ge handräckning då dessa utför tillsyns- eller kontrolluppgifter som hänför sig till ett elföretag eller naturgasföretag.
28 §	28 §
Energimarknadsverkets rätt att lämna ut uppgifter till andra myndigheter	***Energimyndighetens** rätt att lämna ut uppgifter till andra myndigheter*
Utöver det som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999) har Energimarknadsverket rätt att trots bestämmelserna om sekretess lämna ut uppgifter till	Utöver det som föreskrivs i lagen om offentlighet i myndigheternas verksamhet (621/1999) har *Energimyndigheten* rätt att trots bestämmelserna om sekretess lämna ut uppgifter till
1) Finansinspektionen, Konkurrens- och konsumentverket och konsumentombudsmannen för att de ska kunna sköta sina uppgifter,	1) Finansinspektionen, Konkurrens- och konsumentverket och konsumentombudsmannen för att de ska kunna sköta sina uppgifter, *och till Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter*,

Energimarknadsverket har rätt att lämna ut endast sådana uppgifter som behövs för att den berörda myndigheten ska kunna utföra sina uppgifter. Om uppgifter lämnas ut till en utländsk myndighet eller ett internationellt organ förutsätts det dessutom att dessa har motsvarande sekretess som Energimarknadsverket i fråga om de uppgifter som lämnas ut.	*Energimyndigheten* har rätt att lämna ut endast sådana uppgifter som behövs för att den berörda myndigheten ska kunna utföra sina uppgifter, och om uppgifter lämnas ut till en utländsk myndighet eller ett internationellt organ förutsätts det dessutom att dessa har motsvarande sekretess som Energimyndigheten i fråga om de uppgifter som lämnas ut. *Energimyndigheten* får inte lämna ut sekretessbelagda uppgifter som myndigheten fått av en myndighet i en annan stat eller ett internationellt organ, om inte den myndighet som gett uppgifterna har gett sitt uttryckliga samtycke till att uppgifterna lämnas ut. Uppgifterna får endast användas för skötsel av de uppgifter som avses i denna lag eller för de ändamål som samtycket getts för.

10.

Lag

om ändring av lagen om vattentjänster

I enlighet med riksdagens beslut
ändras i lagen om vattentjänster (119/2001) 35 § 2 mom. och
fogas till lagen en ny 15 b § som följer:

Gällande lydelse	Förslagen lydelse
	15 b §
	Rapportering om störningar i vattentjänster
nya	*Ett vattentjänstverk som levererar eller tar emot avloppsvatten till en volym om minst 5 000 kubikmeter vatten per dygn ska utan dröjsmål anmäla betydande störningar i vattentjänsterna till närings-, trafik- och miljöcentralen. Närings-, trafik- och miljöcentralen kan efter att ha mottagit anmälan ålägga vattentjänstverket att informera om saken eller, efter att ha hört vattentjänstverket, själv informera om saken.* *Bestämmelserna om vattentjänstverk i 1 mom. gäller också anläggningar som levererar vatten till ett vattentjänstverk eller som tar emot avloppsvatten från ett vattentjänstverk.* *Närings-, trafik- och miljöcentralen ska vidarebefordra den anmälan som avses i 1 mom. för kännedom till jord- och skogsbruksministeriet. Närings-, trafik- och miljöcentralen ska dessutom bedöma om en sådan störning som avses i 1 mom. berör de övriga medlemsstaterna i Europeiska unionen och vid behov underrätta den behöriga myndigheten i den berörda medlemsstaten.* *Närmare bestämmelser om när en sådan störning som avses i 1 mom. är betydande samt om innehållet i och utformningen av anmälan och hur den ska lämnas in får utfärdas genom förordning av jord- och skogsbruksministeriet.*

35 §	35 §
Tystnadsplikt	*Tystnadsplikt*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Utan hinder av tystnadsplikten enligt lagen om offentlighet i myndigheternas verksamhet får uppgifter om enskildas eller sammanslutningars ekonomiska ställning eller affärs- eller yrkeshemligheter eller enskildas personliga förhållanden, som erhållits vid utförande av åligganden enligt denna lag, lämnas ut till	Utan hinder av tystnadsplikten enligt lagen om offentlighet i myndigheternas verksamhet får uppgifter om enskildas eller sammanslutningars ekonomiska ställning eller affärs- eller yrkeshemligheter eller enskildas personliga förhållanden, som erhållits vid utförande av åligganden enligt denna lag, lämnas ut till
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
1) tillsynsmyndigheten för utförande av uppgifter som avses i denna lag,	1) tillsynsmyndigheten för utförande av uppgifter som avses i denna lag,
2) åklagar- och polismyndigheter för utredande av brott.	2) åklagar- och polismyndigheter för utredande av brott,
	3) Kommunikationsverket, om det är nödvändigt för skötseln av informationssäkerhetsrelaterade uppgifter.

11.

Lag

om ändring av lagen om Finansinspektionen

I enlighet med riksdagens beslut
fogas till lagen om Finansinspektionen (878/2008) en ny 50 n och en ny 52 a § som följer:

Gällande lydelse	Föreslagen lydelse
	50 n §
	Behörig myndighet enligt direktivet om nät- och informationssäkerhet
nya	*Finansinspektionen är behörig myndighet enligt artikel 8.1 i Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen, nedan direktivet om nät- och informationssäkerhet, när det gäller sektorerna 3 och 4 i bilaga II till direktivet.*
	52 a §
nya	*Samarbete och utbyte av information vid skötseln av uppgifter enligt direktivet om nät- och informationssäkerhet*
	Finansinspektionen ska samarbeta med Kommunikationsverket och andra behövliga myndigheter vid skötseln av uppgifter enligt direktivet om nät- och informationssäkerhet. Finansinspektionen har rätt att för detta ändamål trots sekretessbestämmelserna utbyta information med Kommunikationsverket och andra behövliga myndigheter.