RP 85/2026 rd

Regeringens proposition till riksdagen med förslag till lagar om ändring av lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation, lagen om bedömningsorgan för informationssäkerhet och säkerhetsutredningslagen

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation och lagen om bedömningsorgan för informationssäkerhet ändras. Dessutom föreslås det ändringar av teknisk natur i säkerhetsutredningslagen.

Syftet med de ändringar som föreslås i lagen om bedömning av informationssäkerheten i myndigheternas informationssystem är att förtydliga förfarandena för bedömning av myndigheternas informationssystem och datakommunikation och förbättra tillgången till förfarandena genom att möjliggöra flera olika bedömningsförfaranden än för närvarande. Det föreslås att det utöver för bedömningsorgan för informationssäkerhet också ska föreskrivas om en möjlighet för andra företag som konstaterats vara tillförlitliga att åt myndigheterna erbjuda tjänster för bedömning av informationssäkerheten och beredskapen till den del det är fråga om bedömning av hanteringen av information som högst hör till säkerhetsklass IV. I lagen föreslås också en ny skyldighet för statsförvaltningsmyndigheter att utföra bedömningar av sina informationssystem och sin datakommunikation, där minimikravet är att statsförvaltningsmyndigheterna ska göra en självbedömning. Enligt förslaget ska de bedömningar som lagen förutsätter också kunna utföras av andra myndigheter än statsförvaltningsmyndigheter. Alla myndigheter måste dock begära bedömning av en bedömningsmyndighet när det gäller hantering av information som hör till säkerhetsklass I eller II. Dessutom ska alla myndigheter begära bedömning av en bedömningsmyndighet eller skaffa en bedömning av ett bedömningsorgan för informationssäkerhet när det gäller hantering av information som hör till säkerhetsklass III, om inte myndigheten på basis av en riskbedömning beslutar att det är onödigt. De föreslagna ändringarna effektiviserar bedömningarna eftersom riskbedömningar kommer att få större betydelse vid valet av bedömningsförfarande. Genom ändringarna betonas också myndigheternas ansvar för informationssäkerheten i och beredskapen hos deras egna informationssystem och deras egen datakommunikation samt myndigheternas ansvar för beslut om ibruktagning av informationssystem eller datakommunikation.

Genom de ändringar som föreslås i lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation preciseras också Transport- och kommunikationsverkets uppgifter, och det föreslås bestämmelser om en rätt för tillverkare av säkerhetskritiska lösningar att ansöka om bedömning. Till lagen fogas dessutom en bedömningsuppgift för Försvarsmakten, genom vilken man svarar på det ökade behovet av bedömningar till följd av förändringar i säkerhetsmiljön. Genom de föreslagna ändringarna preciseras och effektiviseras bedömningsmyndigheternas samarbete, arbetsfördelning och rätt att få uppgifter samt föreskrivs det om en möjlighet att anlita sakkunniga som bistår bedömningsmyndigheten.

Genom de ändringar som föreslås i lagen om bedömningsorgan för informationssäkerhet främjas förutsättningarna för näringsverksamhet för bedömningsorganen för

informationssäkerhet genom att bestämmelserna om bedömningsorganens tillförlitlighet förenklas och effektiviseras och förfarandet för godkännande av bedömningsorganens kompetenser görs smidigare.

_____

INNEHÅLL

MOTIVERING

1 Bakgrund och beredning

1.1 Bakgrund

Med bedömning av informationssäkerheten och beredskapen utreds hur föreskrivna krav som valts på grundval av riskbedömning uppfylls i informationssystem, datakommunikation och säkerhetskritiska produkter. Den centrala lagstiftningen som gäller bedömning av informationssäkerheten i den offentliga förvaltningens informationssystem och datakommunikation, lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011), nedan *bedömningslagen*, och lagen om bedömningsorgan för informationssäkerhet (1405/2011), nedan *lagen om bedömningsorgan,* har beretts mer än 14 år sedan.

Digitaliseringens utveckling och den nya teknologin förknippad med till exempel molntjänster, artificiell intelligens och kvantberäkning har påverkat såväl den offentliga förvaltningens verksamhetssätt som de förfaranden som används för att genomföra informationssystem inom den offentliga förvaltningen. Nationella författningar som är centrala vid bedömningarna, såsom lagen om informationshantering inom den offentliga förvaltningen (906/2019), nedan *informationshanteringslagen*, och säkerhetsutredningslagen (726/2014), har trätt i kraft efter att bedömningslagen och lagen om bedömningsorgan trätt i kraft. Dessutom har EU-lagstiftningen om bedömning av överensstämmelsen med kraven i fråga om informationssäkerhet ökat under de senaste åren. Utifrån dessa ändringar och tidigare utredningar har det identifierats ett behov av att uppdatera och förbättra lagstiftningen om bedömningen av den offentliga förvaltningens informationssäkerhet och beredskap.

Finlands cybersäkerhetsstrategi för åren 2024–2035 har godkänts som statsrådets principbeslut 10.10.2024. Efter cybersäkerhetsstrategins godkännande har det beretts en genomförandeplan för den, där utvecklingsåtgärder fastställs för att uppnå målen med strategin. Uppdatering av lagstiftningen om bedömning av informationssäkerheten i informationssystem, datakommunikation och säkerhetskritiska produkter hör till genomförandeplanens prioriterade åtgärder. I statsrådets försvarsredogörelse 2024 (Försvarsministeriets publikationer 2024:6) konstateras det att Försvarsmaktens mål är att ha egen kapacitet och verksamhet för bedömning och godkännande av informationssystem och krypteringsprodukter. Detta förutsätter att bedömningslagen ändras på motsvarande sätt. Enligt regeringsprogrammet för statsminister Petteri Orpos regering ska processen för att godkänna krypteringsprodukter snabbas upp så att inhemsk cyberteknik kommer snabbare ut på marknaden. Finland har som mål att skaffa sig status som land med en kvalificerad utvärderingsmyndighet som godkänner informationssäkerhetsprodukter inom EU. För att främja dessa mål är det nödvändigt att göra ändringar i bedömningslagen.

1.2 Beredning

Finansministeriet tillsatte 22.2.2024 en arbetsgrupp för uppdatering och förbättring av överensstämmelsebedömningen av informationssystem för mandatperioden 1.3.2024–31.12.2025 (VN/36127/2023). Arbetsgruppens mål var att bedöma såväl behovet av att uppdatera den nuvarande bedömningslagstiftningen som metoderna att förbättra bedömningarna, med beaktande av de möjligheter som utnyttjandet av självbedömningar erbjuder, kostnadseffektiviteten och förändringarna i verksamhetsmiljön.

Finansministeriet hade arbetsgruppens ordförandeskap och medlemmarna kom från finansministeriet, statsrådets kansli, utrikesministeriet, utrikesministeriets nationella säkerhetsmyndighet (NSA), justitieministeriet, inrikesministeriet, försvarsministeriet, jord- och skogsbruksministeriet, kommunikationsministeriet, cybersäkerhetsdirektörens byrå, social- och hälsovårdsministeriet, arbets- och näringsministeriet, dataombudsmannens byrå, Statens center för informations- och kommunikationsteknik Valtori, Myndigheten för digitalisering och befolkningsdata, Transport- och kommunikationsverket, Försvarsmakten, Välfärdsområdesbolaget Hyvil Ab och Kommunförbundet. Arbetsgruppen sammanträdde 17 gånger. Medlemmarna i expertsekretariatet som stödde arbetsgruppen kom från finansministeriet, försvarsministeriet, kommunikationsministeriet, inrikesministeriet, Försvarsmakten och Transport- och kommunikationsverket samt under 2024 dessutom från Statens center för informations- och kommunikationsteknik Valtori och Myndigheten för digitalisering och befolkningsdata. Sekretariatet sammanträdde totalt 30 gånger.

Arbetsgruppens uppgifter delades in i två faser. I den första fasen beredde arbetsgruppen en rapport om nulägesbedömning och utvecklingsförslag för överensstämmelsebedömningen av informationssystemens informationssäkerhet och beredskap. Rapporten färdigställdes 12.12.2024. Ett intressentmöte om rapporten för den första fasen ordnades för den offentliga förvaltningen och näringslivet 21.11.2024.

Ministerarbetsgruppen för samhällsförnyelse behandlade 7.3.2025 de lagberedningsobjekt som presenterades i arbetsgruppens rapport för den första fasen. Utifrån detta beredde arbetsgruppen ändringsförslag till lagstiftningen i form av regeringens proposition. Arbetsgruppens utkast till regeringens proposition färdigställdes 23.9.2025. Förslag till lagstiftningsändringar som ingår i propositionsutkastet behandlades på intressentmöten som arbetsgruppen ordnade för den offentliga förvaltningen 9.9.2025 och för företagsrepresentanter 11.9.2025. Cirka 220 representanter för den offentliga förvaltningen och 30 representanter för företag deltog i intressentmötena.

Utifrån det utkast till regeringens proposition som bereddes av arbetsgruppen, beredde finansministeriet som tjänsteuppdrag ett delvis modifierat utkast till regeringsproposition, som till sitt sakinnehåll dock följde arbetsgruppens förslag. Detta utkast till regeringsproposition var på remiss 27.11.2025–23.1.2026. Utlåtanden begärdes från ministerier, statsmyndigheter, välfärdsområden, kommuner, domstolar, högskolor, nationella ackrediteringsorgan, bedömningsorgan för informationssäkerhet och aktörer som tillverkar säkerhetskritiska lösningar.

Den fortsatta beredningen av propositionen efter remissbehandlingen har gjorts vid finansministeriet. Under den fortsatta beredningen har samarbete utförts med försvarsministeriet, kommunikationsministeriet, Försvarsmakten och Transport- och kommunikationsverket.

Beredningsunderlaget till propositionen finns offentligt tillgängligt på adressen https://vm.fi/sv/projekt-och-lagberedning, identifieringskod VM167:00/2023.

2 Nuläge och bedömning av nuläget

2.1 Bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation

Bestämmelser om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation finns i bedömningslagen. Bedömningen av myndigheternas informationssystem och datakommunikation gäller i nuläget endast bedömning av informationssäkerheten. I bedömningslagen definieras inte informationssäkerhet, men i förarbetet till lagen (RP 45/2011 rd) hänvisas till internationella skyldigheter, enligt vilka informationssäkerhet kan anses avse allmänt tryggande av informationens tillförlitlighet, integritet och tillgänglighet. Internationellt betonas också betydelsen av informationens ursprung och obestridlighet. I informationshanteringslagen föreskrivs om informationssäkerhetsåtgärder, med vilka avses säkerställande av informationsmaterials tillgänglighet, integritet och tillförlitlighet genom administrativa, funktionella och tekniska åtgärder.

Vid sidan om informationssäkerheten har betydelsen av beredskap ökat på grund av förändringar i säkerhetsmiljön. Beredskap har också lagts till i 13 a § i informationshanteringslagen, enligt vilken en informationshanteringsenhet ska utreda väsentliga risker som hänför sig till behandlingen av informationsmaterial, utnyttjandet av informationssystem och verksamhetens kontinuitet samt förbereda sig för störningssituationer under normala förhållanden och undantagsförhållanden. Bedömning av beredskapen föreskrivs dock inte i bedömningslagen och denna bedömning är inte en etablerad del av bedömningsverksamheten. Beredskap har dock identifierats som ett delområde vars bedömning ska utvecklas och antalet bedömningar av beredskapen ökas.

I gällande lagstiftning föreskrivs inte om någon allmän skyldighet för myndigheterna att bedöma informationssystem och datakommunikation. Enligt 13 § i informationshanteringslagen ansvarar informationshanteringsenheten, det vill säga myndigheten själv, för att säkerställa informationssäkerheten i fråga om informationsmaterial och informationssystem. Enligt 2 mom. i paragrafen ska de med tanke på skötseln av en myndighets uppgifter relevanta informationssystemens feltolerans och funktionella användbarhet regelbundet säkerställas genom tillräcklig testning. Enligt 5 mom. i samma paragraf föreskrivs det särskilt om bedömning av informationssäkerheten i myndigheters informationssystem och datakommunikation. Syftet med bestämmelsen är att skapa en koppling till bedömningslagen och lagen om bedömningsorgan så att planeringen av informationssystemens informationssäkerhet och signeringen av utvärderingen av planeringen ska bilda en tydlig helhet (RP 284/2018 rd, s. 93).

Bedömningsskyldigheter ingår i sektorspecifik lagstiftning. Bedömning av informationssäkerheten i informationssystem och datakommunikation krävs branschspecifikt i lagen om behandling av kunduppgifter inom social- och hälsovården (703/2023), nedan *kunduppgiftslagen*, och lagen om sekundär användning av personuppgifter inom social- och hälsovården (552/2019), nedan *lagen om sekundär användning*, samt i statsrådets förordning om verksamheten i den offentliga förvaltningens säkerhetsnät (1109/2015). Enligt lagen om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster (1226/2013) ska statens gemensamma informations- och kommunikationstekniska tjänster uppfylla behövliga krav på informationssäkerhet och beredskap, och i lagens förarbete (RP 150/2013 rd, s. 32) hänvisas till att bedömning och verifiering kan göras enligt bedömningslagen.

Myndigheternas informationssystem omfattas av bedömningsskyldigheter även på grund av internationella förpliktelser som gäller informationssäkerhet. Lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004) gäller skyddet av EU:s och Natos säkerhetsklassificerade information. I samband med stiftandet av lagen om internationella förpliktelser som gäller informationssäkerhet och ikraftsättandet av avtalet mellan parterna i nordatlantiska fördraget (FördrS 55–56/2023) har Finland nationellt satt i kraft EU:s och Natos säkerhetsregler som gäller skydd av säkerhetsklassificerad information och som innefattar bedömningsskyldigheter.

I den förändrade säkerhetssituationen kan det dock vara motiverat att statsförvaltningsmyndigheter utöver de sektorspecifika och internationella skyldigheterna att bedöma informationssäkerhet även genomför bedömningar av alla sina informationssystem och all sin datakommunikation. Då krävs det också granskning av bedömningsförfarandena, det vill säga vilka aktörer som gör bedömningar samt bedömningens innehåll och genomförandesätt.

I 3 § i bedömningslagen föreskrivs om de bedömningsförfaranden som är tillåtna för statsförvaltningsmyndigheterna. Enligt bestämmelsen får statsförvaltningsmyndigheterna för bedömning av informationssäkerheten i sina informationssystem och sin datakommunikation bara använda sig av Transport- och kommunikationsverket eller ett bedömningsorgan för informationssäkerhet som godkänts i enlighet med lagen om bedömningsorgan. Det föreskrivs inget om förfaranden som är tillåtna för bedömning av informationssäkerheten i andra än statsförvaltningsmyndigheters informationssystem och datakommunikation. Förhållandet mellan självbedömningar av informationssystem och datakommunikation som genomförs av statsförvaltningsmyndigheter och 3 § i bedömningslagen är i viss mån oklart och möjligheten till självbedömningar bör klargöras.

I praktiken bedömer myndigheterna informationssäkerheten i sina informationssystem och sin datakommunikation även med andra förfaranden än de som anges i bedömningslagen. Till bedömning av informationssäkerheten hör till exempel de hanteringsskyldigheter förknippade med informationshanteringsenheternas cybersäkerhet som föreskrivs i 4 a kap. i informationshanteringslagen. Enligt 18 b § i informationshanteringslagen ska en informationshanteringsenhet identifiera, utvärdera och hantera cyberrisker som hänför sig till säkerheten i de kommunikationsnät och informationssystem som den använder i sina funktioner eller för att tillhandahålla sina tjänster samt vidta de åtgärder för hantering av cybersäkerhetsrisker som avses i 18 c § i lagen i fråga. Enligt 18 c § 1 punkten i informationshanteringslagen ska informationshanteringsenheten upprätthålla riktlinjerna för hantering av cybersäkerhetsrisker samt bedömningen av effektiviteten i fråga om åtgärderna för hantering av cybersäkerhetsrisker. Enligt förarbetet till lagen (RP 57/2024 rd, s. 166) kan bedömningen göras exempelvis genom självbedömning eller med hjälp av oberoende tillhandahållare av informationssäkerhetstjänster. Åtgärder som anknyter till bedömning av informationssäkerheten genomförs i enlighet med 9 § i informationshanteringslagen också i utlåtandeförfarande om ändringar i informationshanteringen som gäller statliga ämbetsverk och inrättningar, och som en del av detta bedöms även ändringar i informationssystemens informationssäkerhetskrav och -åtgärder. I samband med beredningen av utlåtandeförfarandet är det möjligt att genomföra en självbedömning av informationssystemets informationssäkerhet.

Av alla dessa skäl är det ändamålsenligt att uppdatera bedömningslagen så att den omfattar fler bedömningsförfaranden.

I bedömningslagen föreskrivs inte på vilka grunder bedömningsförfarandet och den som genomför bedömningen ska väljas. Genomförandet av bedömningarna är inte heller begränsat till bedömning av behandlingen av säkerhetsklassificerad information, utan gäller likaledes alla

informationssystem och all datakommunikation. De bedömningsförfaranden som föreskrivs i bedömningslagen beaktar inte heller riskerna i och skillnaderna mellan databehandlingen i olika informationssystem och datakommunikation. I 8 a § i lagen föreskrivs om bemyndigande att utfärda förordning, genom vilken en statsförvaltningsmyndighet kan förpliktas att skaffa ett intyg i fråga om informationssystem eller datakommunikation där handlingar som hör till säkerhetsklass I eller II behandlas. Förordningen har dock inte utfärdats, vilket innebär att den bedömningsskyldighet som grundar sig på riskbedömning och som möjliggörs i 8 a § har i praktiken inte förverkligats. På grund av de i 13 § i informationshanteringslagen föreskrivna skyldigheterna som grundar sig på riskbedömningen av informationsmaterial och informationssystem och säkerhetsklassificeringens inbyggda riskperspektiv, fastställs bedömningsgrunderna i nuläget i praktiken på grundval av riskbedömningen och i bedömningskriterierna beaktas informationssäkerhetshot vars sannolikhet att förverkligas är stor om tillräckliga informationssäkerhetsåtgärder inte vidtas som skydd mot dessa hot. Av dessa skäl har det identifierats ett behov av att precisera valet av bedömningsförfaranden i den gällande lagstiftningen så att valet grundar sig på säkerhetsklasser och riskbedömning.

Antal bedömningar av informationssäkerhet och deras kostnader

Efterfrågan på och volymen av bedömningar av informationssäkerheten i myndigheternas informationssystem har ökat under de senaste åren. Det ökade behovet av bedömningar har orsakat överbelastning i bedömningsverksamheten. Det ökade bedömningsbehovet beror på förändringar i verksamhetsmiljön, som har ökat behovet av att höja säkerhetsnivån för myndigheternas informationssystem. Dessa förändringar inkluderar teknikens och informationshanteringens roll i den geopolitiska konkurrensen, allt mer avancerade hot, mer sammanlänkade system och mer komplexa logistiska leveranskedjor.

Behovet av bedömningar i anslutning till internationella skyldigheter gällande informationssäkerhet har ökat särskilt i och med Nato-medlemskapet. Antalet informationssystem som är avsedda för behandling av Natos säkerhetsklassificerade information och som granskas och ackrediteras av myndigheter har nästan tiofaldigats mellan april 2022 och april 2024. Antalet informationssystem som används för behandling av internationellt informationsmaterial även inom Försvarsmakten och användningen av dem i internationella övningar har ökat snabbt och avsevärt.

Transport- och kommunikationsverket genomför årligen flera tiotals bedömningar av informationssystem. Systemens omfattning och därmed bedömningarnas tekniska omfattning, arbetsmängd och varaktighet varierar mycket. En del av bedömningarna är ändringsbedömningar eller periodiska bedömningar. Det finns inga offentliga uppgifter om antalet bedömningar som genomförts av bedömningsorgan för informationssäkerhet.

Under bedömningslagens giltighetstid har antalet överensstämmelsebedömningar som Statens center för informations- och kommunikationsteknik Valtori och Suomen Erillisverkot Oy skaffat ökat. Ökningen beror på utvecklingsåtgärder för tjänster, nya tjänster och behovet av att behandla EU- och Nato-information. Statens center för informations- och kommunikationsteknik Valtori har mellan augusti 2021 och år 2024 låtit genomföra sammanlagt 73 bedömningar, varav 40 har riktats mot säkerhetsnätets tjänster och 33 mot statens gemensamma informations- och kommunikationstekniska tjänster. Suomen Erillisverkot Oy har genomfört cirka 20 självbedömningar per år och har låtit bedömningsorgan för informationssäkerhet utföra flera bedömningar per år.

Antalet lagstadgade bedömningar av informationssäkerhet som offentliga och privata organisationer inom social- och hälsovården skaffat från bedömningsorgan för

informationssäkerhet har ökat något från och med 2021. Tillväxten beror på att antalet informationssystem som omfattas av bedömningsskyldigheten har ökat. För närvarande finns det 99 av dessa informationssystem och driftmiljöer registrerade i Tillstånds- och tillsynsverkets (fram till 31.12.2025 Valvira) register. År 2023 antecknades 27 intyg över bedömningar av informationssäkerhet i registret.

Enligt Kommunförbundets uppskattning genomför bedömningsorgan för informationssäkerhet eller Transport- och kommunikationsverket inga bedömningar av informationssäkerheten i stor skala i kommunerna, men det finns ingen heltäckande lägesbild. I de största städerna genomförs självbedömningar av informationssäkerheten i informationssystem som valts utifrån en riskbedömning, ofta med stöd från privata tjänsteleverantörer. I mindre kommuner och samkommuner genomförs självbedömningar av informationssäkerheten i informationssystem från fall till fall.

På grund av den ökade efterfrågan och volymen av bedömningar bör tillgången till bedömningar förbättras.

Ökad användning av informations- och kommunikationstekniska system och säkerhetsbehov har ökat systemens kostnader i förhållande till myndighetsverksamhetens övriga kostnadsstruktur. Information om kostnaderna för bedömningar av informationssäkerheten har samlats in från Suomen Erillisverkot Oy, Statens center för informations- och kommunikationsteknik Valtori och ministerier[1]. De dagsverken som krävs för de cirka 20 självbedömningar som genomförs årligen av Suomen Erillisverkot Oy har varit cirka 300 dagsverken per år och kostnaderna har varit cirka 210 000 euro. Kostnaderna för självbedömningarna har sålunda i genomsnitt varit cirka 10 500 euro/bedömning. Kostnaderna för de bedömningar som Suomen Erillisverkot Oy har låtit bedömningsorgan för informationssäkerhet utföra har varit cirka 57 000 euro/bedömning. Priset för de bedömningar av informationssäkerhet som myndigheterna ansökt om har i genomsnitt varit totalt 60 000–70 000 euro/bedömning, varav andelen extern bedömning som i regel har skaffats från bedömningsorgan för informationssäkerhet i genomsnitt har varit 30 000–40 000 euro. Till exempel har det inom kommunikationsministeriets förvaltningsområde årligen skaffats bedömningstjänster enligt bedömningslagen och lagen om bedömningsorgan för cirka 220–230 dagsverken. Anskaffningskostnaderna för tjänster inom förvaltningsområdet uppskattas uppgå till cirka 300 000 euro per år. Från andra företag som erbjuder informationssäkerhetstjänster har årligen köpts bedömningstjänster för cirka 720–750 dagsverken. Kostnaderna beräknas uppgå till cirka 650 000 euro per år. Inom kommunikationsministeriets förvaltningsområde har bedömningar enligt bedömningslagarna sålunda i dagsverken varit cirka 20 procent och i euro cirka 30 procent av alla bedömningar av informationssäkerheten.[1] Kostnaderna för bedömningarna påverkas av de kriterier som används i bedömningen och av det dagliga pris som bestäms utifrån lagen om grunderna för avgifter till staten eller konkurrensutsättningen av genomförandet av bedömningen.

Transport- och kommunikationsverkets uppgifter

Bestämmelser om Transport- och kommunikationsverkets uppgifter i anknytning till bedömningar och godkännanden av informationssäkerheten i informationssystem finns i lagen om internationella förpliktelser som gäller informationssäkerhet, säkerhetsutredningslagen och bedömningslagen. Enligt 3 § i bedömningslagen är Transport- och kommunikationsverket i

[1] Rapporten Tietojärjestelmien tietoturvallisuuden ja varautumisen vaatimustenmukaisuuden arvioinnin nykytila-arvio ja kehittämisehdotukset 12.12.2024, finansministeriet.

nuläget den enda myndigheten som genomför bedömningar av informationssäkerheten i myndigheternas informationssystem och datakommunikation i enlighet med bedömningslagen. När det gäller Transport- och kommunikationsverkets uppgifter har ett behov av uppdatering identifierats för de uppgifter som behandlas nedan.

Transport- och kommunikationsverket ger råd om bedömning av informationssäkerheten av säkerhetsklassificerad information. Det finns dock inga bestämmelser om rådgivningsuppgiften i bedömningslagen, trots att det är fråga om en mer omfattande uppgift än den avgiftsfria myndighetsrådgivning som föreskrivs i 8 § i förvaltningslagen (434/2003) och rådgivningsuppgiften är kopplad till olika faser av bedömningens planering och genomförande. Bestämmelser om rådgivningens avgifter finns i kommunikationsministeriets förordning om avgifter som tas ut för Transport- och kommunikationsverkets prestationer som gäller elektronisk kommunikation (1338/2025).

Enligt 4 § 3 mom. i bedömningslagen utför Transport- och kommunikationsverket sina uppgifter inom ramen för de resurser som står till buds och med beaktande av uppfyllandet av internationella förpliktelser som gäller informationssäkerhet och de begärda åtgärdernas betydelse för en allmän förbättring av informationssäkerheten i myndigheternas informationssystem och datakommunikation. I nuläget prioriterar Transport- och kommunikationsverket bedömningsbegäranden förknippade med myndigheternas internationella förpliktelser som gäller informationssäkerhet och begäranden enligt säkerhetsutredningslagen från skyddspolisen eller Försvarsmaktens Huvudstab förknippade med säkerhetsutredningar av företag samt vid behov begäranden förknippade med bedömning av informationssystem där uppgifter som hör till den nationella säkerhetsklassen I och II behandlas, för vilka det inte finns bedömningar från ett bedömningsorgan för informationssäkerhet tillgängliga.

Försvarsmaktens uppgifter

Behovet och volymen av bedömningar av Försvarsmaktens informationssäkerhet har ökat under de senaste åren. Trots Försvarsmaktens stora bedömningsbehov har ingen befogenhet att bedöma och godkänna informationssystem eller krypteringsprodukter fastställts separat för försvarsförvaltningen i nuläget. När det gäller nationell säkerhetsklassificerad information grundar sig bedömningsverksamheten på de skyldigheter att säkerställa informationssäkerheten i informationsmaterial och informationssystem som fastställts för informationshanteringsenheter och statsförvaltningsmyndigheter i informationshanteringslagen och statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen. Försvarsmakten har interna förfaranden och förmågor att utvärdera sina egna informationssystem och krypteringsprodukter. Bedömnings- och godkännandeuppgifterna fördelas på olika aktörer inom Försvarsmakten, och bedömningsverksamheten har för närvarande inte ordnats som en oberoende och självständig funktion. Försvarsmaktens nuvarande bedömnings- och godkännanderesurser har dimensionerats utifrån de nationella systemens informationssäkerhetskrav, med fokus på de högsta säkerhetsklasserna. På grund av Nato-medlemskapet och den ökade övningsverksamheten har Huvudstaben kommit överens med Transport- och kommunikationsverket om skötseln av vissa bedömningsuppgifter på grundval av 5 § i lagen om internationella förpliktelser som gäller informationssäkerhet. Av alla dessa skäl har det identifierats behov av att föreskriva en separat myndighetsuppgift för Försvarsmakten att göra bedömningar av dess egna informationssystem och dess egen datakommunikation.

Informationsutbyte, samarbete och bistående uppgifter

I nuläget föreskriver bedömningslagen inte om myndigheternas samarbete. Transport- och kommunikationsverket har vid behov samarbetat med andra myndigheter med stöd av 10 § i förvaltningslagen. När det gäller bedömningar som genomförs i enlighet med säkerhetsutredningslagen och lagen om internationella förpliktelser som gäller informationssäkerhet finns det utöver bestämmelser om Transport- och kommunikationsverkets uppgifter även bestämmelser om skyddspolisens och Huvudstabens uppgifter. I dessa lagar föreskrivs också om de behöriga myndigheternas skyldigheter att utbyta information och samarbeta samt om möjligheten att avtala om skötseln av en viss uppgift som tillhör en annan myndighet. I bedömningsmyndigheternas verksamhet har identifierats behov av att även i bedömningslagen föreskriva om informationsutbyte och samarbetsförpliktelser samt om överenskommelse om uppgifter.

Enligt 6 § i bedömningslagen som gäller rätten att få uppgifter och rätten att få tillträde till lokaler och informationssystem, gäller rättigheterna både verket och sakkunniga som handlar på uppdrag av verket. I bedömningslagen föreskrivs dock inte om Transport- och kommunikationsverkets möjlighet att anlita privata fysiska eller juridiska personer som bistår i bedömningsuppgiften. Verket har inte gett uppdrag till privata aktörer och den gällande bedömningslagen kan inte anses uppfylla förutsättningarna för att ge offentliga förvaltningsuppgifter till andra än myndigheter. I de bedömningar som genomförts av bedömningsmyndigheterna har dock identifierats ett behov av att möjliggöra användning av dagsverken som skaffats på den privata marknaden i en bistående roll, särskilt för att trygga uppgifternas personalresursbehov.

Bedömningsgrunder och -kriterier

I 7 § i bedömningslagen och 10 § i lagen om bedömningsorgan föreskrivs om bedömningsgrunder som Transport- och kommunikationsverket eller bedömningsorgan för informationssäkerhet kan använda som bedömningsgrunder för informationssäkerheten i myndigheternas informationssystem och datakommunikation. Förteckningen över bedömningsgrunder har samma innehåll i båda lagarna och gör det möjligt att i stor utsträckning använda olika författningar, anvisningar och standarder som bedömningsgrund. Förteckningen bör dock uppdateras.

Enligt gällande lag kan bedömningsgrunderna och -kriterierna grunda sig på de anvisningar som den nationella säkerhetsmyndighet (NSA) som avses i lagen om internationella förpliktelser som gäller informationssäkerhet gett om genomförandet av internationella förpliktelser som gäller informationssäkerhet, det vill säga i praktiken på de nationella kriterierna för säkerhetsauditering (Katakri), som i enlighet med den nationella säkerhetsmyndighetens anvisning tillämpas vid skötseln av internationella förpliktelser som gäller informationssäkerhet. Katakri används dessutom i många nationella situationer, såsom i bedömningar av tjänster enligt lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015) och i bedömningar relaterade till säkerhetsutredningar av företag. I fastställandet av bedömningskriterierna utnyttjas också informationshanteringsnämndens rekommendation om kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen (Julkri). Det har inte varit möjligt att utnyttja Julkri i bedömningar av informationssäkerheten i informationssystem enligt lagen om bedömningsorgan, eftersom Julkri-kompetenser inte har ansökts, ackrediterats och beviljats till bedömningsorgan för informationssäkerhet som godkänts enligt lagen om bedömningsorgan, eftersom kompetenskraven för tillämpningen av Julkri ännu inte har fastställts. Som bedömningsgrunder har tidigare också använts statsrådets förordning om informationssäkerheten inom statsförvaltningen (681/2010) och finansministeriets anvisningar om genomförandet av den (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI),

men förordningen är upphävd och anvisningarna är föråldrade. Förordningen har ersatts av informationshanteringslagen och av statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019), nedan *säkerhetsklassificeringsförordningen*, som meddelats på grundval av informationshanteringslagen. I de bedömningar som gjorts med stöd av lagen om bedömningsorgan har den fastställda internationella standarden ISO/IEC 27001 också använts som bedömningsgrund. I bedömningar som förutsätts av kunduppgiftslagen och lagen om sekundär användning ska bedömningsgrunden utgöras av bestämmelser från Institutet för hälsa och välfärd och tillståndsmyndigheten för social- och hälsovårdsdata.

Det finns inga etablerade allmängiltiga grunder för bedömning av beredskapen. Grunderna för Julkri-kriteriernas beredskap och kontinuitetshantering (VAR) är inte så väl etablerade att de skulle ha en omfattande tillämpningspraxis.

I bedömningslagen föreskrivs inte på vilka grunder eller av vem de bedömningsgrunder som används i bedömningen väljs. Enligt 10 § i lagen om bedömningsorgan väljs bedömningsgrunderna av den som bedömningen gäller, men de godkända kompetenser som innehas av bedömningsorganet för informationssäkerhet påverkar vilka bedömningar bedömningsorganet kan göra. I bedömningsverksamheten har identifierats behovet av att vid valet av bedömningsgrunder och definitionen av bedömningsobjektet beakta de krav som ställts på informationssäkerheten i och beredskapen hos informationssystemet och de krav som valts på grundval av riskbedömning. Detta framgår dock inte av den gällande lagstiftningen, så mer exakta föreskrifter om valet av bedömningsgrunder behövs.

Intyg över att kraven uppfylls

Enligt 8 § i bedömningslagen kan Transport- och kommunikationsverket på begäran utfärda intyg över informationssystem eller datakommunikation som uppfyller kraven på informationssäkerhet. Till intyget hör också den i 9 § i bedömningslagen föreskrivna skyldigheten att upprätthålla och följa upp informationssäkerhetsnivån, enligt vilken den som får ett intyg ska förbinda sig till att upprätthålla informationssäkerhetsnivån och underrätta Transport- och kommunikationsverket om ändringar som inverkar på informationssäkerhetsnivån. I 10 § i bedömningslagen föreskrivs det om återkallelse av intyg.

Den möjlighet som föreskrivs i 8 a § i bedömningslagen att genom statsrådets förordning föreskriva skyldighet för statsförvaltningsmyndigheter att skaffa intyg över bedömningar av system där handlingar som hör till säkerhetsklass I eller II behandlas har inte utnyttjats, så det är frivilligt att begära Transport- och kommunikationsverkets bedömning eller intyg vid behandling av nationell säkerhetsklassificerad information. De intyg som begärts enligt 8 § i bedömningslagen och som Transport- och kommunikationsverket har utfärdat har gällt informationssystem där nationella säkerhetsklassificerade uppgifter behandlas. Intyg har begärts och utfärdats mycket sällan.

Ett beslut eller utlåtande av intygskaraktär kan dock ges om system som uppfyller informationssäkerhetskraven i de situationer som avses i lagen om internationella förpliktelser som gäller informationssäkerhet. Godkännandeutlåtandet som förutsätts i säkerhetsreglerna för bedömningar enligt EU:s och Natos förpliktelser som gäller informationssäkerhet är i ljuset av förfarandet i bedömningslagen av intygskaraktär. På begäran av skyddspolisen eller Huvudstaben utfärdar Transport- och kommunikationsverket också intygsliknande utredningar om informationssystem som uppfyller informationssäkerhetskraven i samband med säkerhetsutredningar av företag enligt säkerhetsutredningslagen. Den slutliga

säkerhetsutredningen av företag görs dock av en enligt säkerhetsutredningslagen behörig myndighet.

I praktiken utarbetas alltid en bedömningsrapport om bedömningen av informationssäkerheten, i vilken det beskrivs hur de kriterier som ligger till grund för bedömningen förverkligas i bedömningsobjektet och om avvikelser eller brister har observerats i bedömningen av informationssäkerhetsåtgärderna. Bestämmelser om bedömningsrapporten finns dock inte i den gällande bedömningslagen. De gällande bestämmelserna i bedömningslagen för den rapportering som produceras av bedömningen motsvarar alltså inte den praxis som används i bedömningsverksamheten. Därför har det konstaterats ett behov av att uppdatera rapporteringen och dokumentationen av bedömningsresultatet även på lagnivå.

2.2 Bedömning av krypteringsprodukter och andra säkerhetskritiska lösningar

EU:s och Natos säkerhetsregler omfattar skyldigheter gällande bedömning av krypteringslösningar och skydd mot diffus strålning (TEMPEST) samt skyldigheter att bedöma vissa andra säkerhetskritiska produkter. Överenskommelse om krypteringslösningar för elektroniska dataförbindelser mellan stater är också en central avtalsbestämmelse och -praxis i staternas bilaterala eller multilaterala informationssäkerhetsavtal.

Transport- och kommunikationsverket bedömer och godkänner produkter i enlighet med internationella förpliktelser som gäller informationssäkerhet. Produktbedömningarna gäller krypteringsprodukter eller andra säkerhetskritiska produkter. De grundar sig på Transport- och kommunikationsverkets uppgift enligt 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet att vara den nationella säkerhetsmyndighetens sakkunnig i ärenden som gäller informationssäkerhet i fråga om informationssystem och datakommunikation. Med krypteringsprodukter säkerställs informationens konfidentialitet och integritet med olika krypteringsmekanismer. Krypteringsprodukter är till exempel VPN-produkter och lösningar för kryptering av hårddisk eller massminne. Krypteringsbehoven kan till exempel gälla kryptering av tal och datakommunikation med fasta eller trådlösa förbindelser. Utöver krypteringsprodukter är även andra komponenter som är centrala för informationssystemens säkerhet, såsom gateway-produkter och överskrivningsprodukter som används för att förstöra information, säkerhetskritiska produkter.

I skyddet av nationell säkerhetsklassificerad information föreskrivs ingen bedömnings- eller godkännandeskyldighet för krypteringslösningar eller andra säkerhetskritiska produkter och lösningar, så Transport- och kommunikationsverket gör bedömningar av dem på myndighetens begäran med stöd av bedömningslagen som en del av myndighetens informationssystem eller datakommunikation. Systemspecifika bedömningar som begärts av myndigheterna publiceras inte.

I bedömningslagen föreskrivs inte att Transport- och kommunikationsverket har som uppgift att göra produktbedömningar på begäran av tillverkare av säkerhetskritiska eller andra produkter, och företag eller tillverkare som erbjuder säkerhetskritiska lösningar kan inte självständigt göra bedömningsbegäranden enligt bedömningslagen. I den gällande lagstiftningen föreskrivs således inte om med vilka förutsättningar tillverkaren kan få sina säkerhetskritiska lösningar bedömda av en behörig myndighet eller med vilka förutsättningar företaget kan få myndighetsgodkännande för sin produkt.

För att stödja myndigheternas behov gör Transport- och kommunikationsverket dock en del produktspecifika bedömningar av säkerhetskritiska lösningar för produkter från finländska tillverkare och utarbetar utlåtanden om dessa bedömningar. Bedömningarna görs på

tillverkarens begäran, men det måste finnas ett myndighetsbehov av produkten i bakgrunden. Behandlingen av tillverkarnas bedömningsbegäranden förutsätter att ett avtal ingås mellan Transport- och kommunikationsverket och tillverkaren. Avtalsmodellen grundar sig på Cybersäkerhetscentrets avtalsbefogenhet enligt 3 § i lagen om Transport- och kommunikationsverket (935/2018), enligt vilken Cybersäkerhetscentret kan på avtalsbasis utföra prestationer som baserar sig på uppgifter som föreskrivits för Cybersäkerhetscentret. På avtalsbasis gör Transport- och kommunikationsverket endast bedömningar av produkter som tillverkats i Finland av finländska tillverkare. Syftet med bedömningarna är att säkerställa tillförlitligheten av den säkerhetskritiska lösningen i den utsträckning att Transport- och kommunikationsverket kan publicera information om den bedömda produkten. Förteckningen som upprätthålls på verkets webbplats innehåller för närvarande ett tiotal bedömda krypteringsprodukter och fem andra bedömda produkter. Det pågår vanligen på en och samma gång färre än tio nya bedömningar eller bedömningar av produktuppdateringar.

Myndighetsuppgifterna i anslutning till bedömningen av krypteringsprodukter och andra säkerhetskritiska lösningar ska preciseras och tillverkarna ska ges möjlighet att ansöka om bedömning och godkännande av säkerhetskritiska lösningar och deras tillverkning.

2.3 Bedömningsorgan för informationssäkerhet

I lagen om bedömningsorgan föreskrivs om förutsättningarna och förfarandet för godkännande av bedömningsorgan för informationssäkerhet och deras kompetenser, tillsynen över bedömningsorganens verksamhet och kraven på bedömningsorganens verksamhet. Bedömningsorgan för informationssäkerhet spelar en betydande roll som producenter av tjänster för bedömning av informationssäkerheten. Genom lagen om bedömningsorgan har strävan varit att främja myndigheternas och företagens informationssäkerhet genom att skapa ett arrangemang där Transport- och kommunikationsverket på ansökan godkänner bedömningsorgan för informationssäkerhet och deras kompetensområden samt övervakar deras verksamhet.

I lagen om bedömningsorgan föreskrivs inte om vilka aktörer som kan skaffa bedömningar från bedömningsorgan för informationssäkerhet. Sålunda finns det inget hinder för att en myndighet skaffar en bedömning från ett bedömningsorgan för informationssäkerhet och enligt 3 § i bedömningslagen är en bedömning som utförs av ett bedömningsorgan för informationssäkerhet ett alternativt bedömningsförfarande för en statsförvaltningsmyndighet.

Enligt 3 § i lagen om bedömningsorgan kan ett bedömningsorgan för informationssäkerhet ansöka om godkännande hos Transport- och kommunikationsverket. Bestämmelser om förutsättningarna för godkännande och behandlingen av ansökan finns i 4 och 5 § i lagen. Med stöd av 5 § 2 mom. i lagen ska uppfyllandet av kraven på oberoende och kompetens visas på det sätt som anges i lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (920/2005), det vill säga genom ackreditering som utförs av det nationella ackrediteringsorganet, ackrediteringstjänsten FINAS. Transport- och kommunikationsverkets godkännandebeslut grundar sig till dessa delar på ackrediteringsintyg.

Ackrediteringsförfarandet baserar sig på Europeiska unionens regleringsmodell som tillämpas för att visa kompetensen hos bedömningsorgan för överensstämmelse eller anmälda organ i flera EU-rättsakter. Som ett alternativt förfarande kan de dock även innefatta att den behöriga myndigheten godkänner kompetensen på grundval av en utredning. Till exempel i lagen om anmälda organ för vissa produktgrupper (278/2016) föreskrivs att om bedömningsorganet inte kan lägga fram något ackrediteringsintyg, ska det till den behöriga myndigheten ge in behövliga skriftliga bevis för att myndigheten ska kunna bedöma huruvida sökanden uppfyller de krav

som gäller godkännande som anmält organ och som grundar sig på harmoniserad unionslagstiftning. Ett motsvarande förfarande kan utnyttjas så att bedömningsorganen för informationssäkerhet mer flexibelt kan skaffa tilläggskompetenser för att förbättra tillgången till bedömningar.

Utöver ackrediteringen av kompetensen förutsätter godkännandet av ett bedömningsorgan enligt 5 § 1 mom. 4 och 5 punkten i lagen om bedömningsorgan att tillförlitligheten hos de ansvariga personerna och säkerheten i databehandlingen och lokalerna har säkerställts och att organet har ändamålsenliga anvisningar för sin verksamhet och uppföljningen av den. Transport- och kommunikationsverket utreder säkerheten i databehandlingen genom en inspektion. Dessutom kontrollerar verket att de anvisningar som förutsätts i 5 § 1 mom. 5 punkten är ändamålsenliga. Lokalernas säkerhet säkerställs av antingen skyddspolisen eller Transport- och kommunikationsverket. Enligt 4 § i lagen om bedömningsorgan ska verket innan ett bedömningsorgan för informationssäkerhet godkänns ge skyddspolisen tillfälle att yttra sig om tillförlitligheten hos bedömningsorganets ansvariga personer och om säkerheten i bedömningsorganets lokaler. Skyddspolisen gör en säkerhetsutredning av ansvariga personer på ansökan av Transport- och kommunikationsverket.

Det har upplevts svårt att bli ett bedömningsorgan för informationssäkerhet och få organets behörigheter godkända. Dessutom har processen kunnat ta lång tid. I förfarandena i den gällande lagen om bedömningsorgan utnyttjas förfarandena för säkerhetsutredning av företag enligt säkerhetsutredningslagen endast delvis för att säkerställa företagens tillförlitlighet. Lagen föreskriver inte heller om tillförlitligheten hos personalen vid ett bedömningsorgan för informationssäkerhet. Det är ändamålsenligt att precisera lagstiftningen för dessa omständigheter.

Det finns fyra bedömningsorgan för informationssäkerhet som godkänts av Transport- och kommunikationsverket i enlighet med lagen om bedömningsorgan. Alla bedömningsorgan för informationssäkerhet har godkänd kompetens att utföra bedömningar av ledningssystem för informationssäkerhet enligt standarden ISO/IEC 27001, men efterfrågan på dessa bedömningar har inte varit stor. Tre bedömningsorgan för informationssäkerhet har dessutom s.k. Katakri-kompetens, det vill säga kompetens att göra bedömningar av behandling av information som klassificerats i säkerhetsklass IV och III i enlighet med de nationella kriterierna för säkerhetsauditering (Katakri). Ackrediteringen och godkännandet av det tredje bedömningsorganets Katakri 2020-kompetens genomfördes i början av 2025. På grund av myndigheternas långsiktiga upphandlingsavtal var det ännu inte möjligt att konstatera den tredje anbudsgivarens konsekvenser för bedömningarnas utbud och priser.

Enligt vad de myndigheter som skaffar bedömningar anser och har erfarit har bedömningsorganen för informationssäkerhet haft så stor efterfrågan på bedömningar att de inte har kunnat erbjuda bedömningstjänster i enlighet med efterfrågan. Bedömningarna av Statens center för informations- och kommunikationsteknik Valtoris tjänster och de tillhörande informations- och kommunikationstekniska tjänsterna har krävt stöd av Valtoris personal, varvid även Valtoris tillgängliga personalresurser har påverkat tidtabellerna för genomförandet av bedömningarna. Bedömningsorganen för informationssäkerhet har i sin respons lyft fram att det är utmanande att rekrytera personer för bedömning av informationssäkerheten i behandlingen av den offentliga förvaltningens säkerhetsklassificerade information. Det finns ett begränsat antal personer med tillräcklig teknisk förmåga i Finland. Arbetet kan i regel inte heller utföras på distans, vilket gör det mindre attraktivt. På grund av dessa utmaningar med att genomföra bedömningar av informationssäkerheten finns det behov av att förbättra tillgången till bedömningstjänster.

I den praktiska verksamheten har dessutom identifierats behov av att precisera lagstiftningen om bedömningsorgan för informationssäkerhet till exempel när det gäller förfaranden kopplade till bedömningen, styrning och rätt att få information. I 9 § 2 mom. i lagen om bedömningsorgan föreskrivs om utfärdande av intyg om lokalerna och verksamheten hos den som bedömningen gäller är förenliga med de bedömningsgrunder som legat till grund för utredningen. De grunder för bedömning av informationssäkerheten som använts vid bedömningen och bedömningens omfattning ska specificeras i intyget. Det finns inga särskilda bestämmelser om bedömningsrapporten, men ändamålsenlig dokumentation ingår i bedömningsverksamhetens praxis och i ackrediterad kompetens. I kunduppgiftslagen och lagen om sekundär användning föreskrivs om skyldigheten att för vissa funktioner skaffa ett intyg från ett godkänt bedömningsorgan för informationssäkerhet. I dessa lagar föreskrivs också om intygets giltighet, upprätthållande och återkallelse.

I 13 § i lagen om bedömningsorgan föreskrivs om tillämpningen av bestämmelser om god förvaltning, det vill säga allmänna förvaltningslagar, i verksamheten vid bedömningsorgan för informationssäkerhet. Enligt förarbetet till den gällande lagen ska tillämpningen av de nämnda författningarna för undvikande av tolkningsproblem inte vara bunden till skötsel av en offentlig förvaltningsuppgift, utan författningarna ska tillämpas på skötseln av alla uppgifter som är förenliga med lagen om bedömningsorgan (RP 45/2011 rd s. 10). I praktiken har tolkningen dock varit att alla uppgifter enligt lagen om bedömningsorgan är offentliga förvaltningsuppgifter. I paragrafen föreskrivs trots detta inte om det straffrättsliga tjänsteansvaret för personalen vid bedömningsorgan för informationssäkerhet. För detta har identifierats ett behov av att uppdatera lagen, eftersom delegering av en offentlig förvaltningsuppgift utanför tjänstemannakåren förutsätter enligt grundlagsutskottets praxis en uttrycklig bestämmelse på lagnivå om tjänstebrottsansvar (till exempel GrUU 93/2022 rd, s. 4, GrUU 15/2019 rd, s. 4). I lagen om bedömningsorgan föreskrivs inte heller om ramvillkor för att låta underleverantörer utföra uppgifter som anknyter till bedömningen. Ramvillkoren bör preciseras i lagen.

I lagen om bedömningsorgan, kunduppgiftslagen eller lagen om sekundär användning föreskrivs inte om fördelningen av styrnings- eller tillsynsbefogenheter mellan Transport- och kommunikationsverket och myndigheterna inom social- och hälsovården, Institutet för hälsa och välfärd (THL), Tillstånds- och tillsynsverket (fram till 31.12.2025 Valvira), tillståndsmyndigheten för användning av social- och hälsovårdsdata (Findata) och Folkpensionsanstalten (FPA), när bedömningsorganet för informationssäkerhet utför bedömningen på grundval av bestämmelser från myndigheter inom social- och hälsovården. Myndigheterna samarbetar vid behov i ärendet i enlighet med den allmänna samarbetsbestämmelsen i 10 § i förvaltningslagen. I lagen om bedömningsorgan föreskrivs om Transport- och kommunikationsverkets rätt att från bedömningsorgan för informationssäkerhet få de uppgifter som är nödvändiga för att övervaka att organet uppfyller kraven som gäller dess verksamhet. Rätten att få information gäller inte sekretessbelagda uppgifter eller uppgifter som begärs av andra myndigheter eller av den som bedöms av ett bedömningsorgan för informationssäkerhet, som är nödvändiga för att övervaka att organet uppfyller kraven som gäller dess verksamhet. Tillsynens rätt att få information kräver precisering.

2.4 Unionsrätten

Europeiska unionens lagstiftning om bedömningen av informations- och cybersäkerhetens överensstämmelse med kraven i informations - och kommunikationssystem har ökat under de senaste åren. Europeiska unionens bestämmelser gäller i regel certifiering av tjänster och produkter när de kommer ut på marknaden. Certifiering och certifikat avser i EU-regleringen i allmänhet en bedömning som utförs av vissa föreskrivna bedömningsorgan för vissa produkter,

tjänster eller processer utifrån noggrant definierade krav och certifikat som utfärdas på grundval av bedömningsresultaten i syfte att påvisa produktens, tjänstens eller processens egenskaper på den inre marknaden i Europeiska unionen.

Enligt artikel 1 i cybersäkerhetsakten (Europaparlamentets och rådets förordning (EU) 2019/881 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013) är förordningens syfte att säkerställa en väl fungerande inre marknad och sträva efter en hög nivå i fråga om cybersäkerhet, cyberresiliens och förtroende inom unionen. I detta syfte fastställs i förordningen ett ramverk för inrättandet av ordningar för cybersäkerhetscertifiering för IKT-produkter, IKT-tjänster och IKT-processer och för informationssäkerhetstjänster. Med ramverket undviks en fragmentering av den inre marknaden när det gäller dessa certifieringsordningar. Enligt artikel 1.2 begränsar förordningen inte medlemsstaternas befogenheter i fråga om verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på straffrättens område.

Det första certifieringssystemet är EU:s Common Criteria-schema (EUCC) som nyligen antogs genom kommissionens genomförandeförordning (EU) 2024/482. Schemat lämpar sig till exempel för certifiering av smartkort och maskinvara med säkerhetsboxar, anordningar för skapande av underskrifter, maskinläsbara resehandlingar och färdskrivare. Certifieringsscheman för bland annat molntjänster (EUCS, European Union Cybersecurity Certification Scheme for Cloud Services) och 5G-nät bereds. Möjliga framtida arbetsobjekt är enligt kommissionens arbetsprogram (Work Programme for European cybersecurity certification, SWD (2024) 7.2.2024) en plånboksapplikation för digital identitet, tjänster för hantering av informationssäkerheten och i allmänhet de scheman och automatiseringssystem för industrin som behövs inom ramen för Cyber Resilience Act. Att ansöka om certifiering enligt cybersäkerhetsakten är frivilligt för den som erbjuder en tjänst eller produkt.

Europaparlamentets och rådets förordning (EU) 2024/2847 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828, nedan cyberresiliensförordningen eller CRA, Cyber Resilience Act, antogs 23.10.2024 och dess ikraftträdande är förknippat med övergångsperioder. Förordningen fastställer regler för att göra produkter med digitala element tillgängliga på EU-marknaden för att säkerställa produkternas cybersäkerhet. CRA är en övergripande produktsäkerhetsförordning och genomförandet av dess krav kommer att garanteras i framtiden som en del av CE-märkningen. I fortsättningen kommer det att vara en förutsättning för marknadstillträde i EU att säkerhetskraven enligt förordningen uppfylls. Enligt artikel 2.7 ska förordningen inte tillämpas på produkter med digitala element som utvecklats eller ändrats uteslutande för ändamål som rör nationell säkerhet eller försvarsändamål eller på produkter som utformats specifikt för att behandla säkerhetsskyddsklassificerade uppgifter.

Bestämmelser om system för artificiell intelligens utifrån riskerna de förorsakar finns i Europaparlamentets och rådets förordning (EU) 2024/1689 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens). Förordningen förbjuder mycket skadlig användning av artificiell intelligens och ställer skärpta krav på vissa AI-system som klassificeras som system med hög risk, vilket bland annat inkluderar att säkerställa informationssäkerheten under systemets hela livscykel, inklusive utformning, utveckling, ibruktagande och underhåll. I förordningen fastställs harmoniserade regler för utsläppande på marknaden, ibruktagande och användning av AI-system i unionen.

Förordningen kräver att AI-system med hög risk är föremål för en bedömning av överensstämmelse innan de släpps ut på marknaden eller tas i bruk.

Kraven på hanteringen av cybersäkerhetsrisker för aktörer inom den offentliga förvaltningen har å sin sida harmoniserats med NIS2-direktivet, det vill säga Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, som har genomförts i Finland i fråga om den offentliga förvaltningen i det nya 4 a kap. i informationshanteringslagen. NIS2-direktivet gör det möjligt att förplikta kategorier av väsentliga och viktiga entiteter att använda produkter som är certifierade enligt cybersäkerhetsakten. Denna möjlighet har inte föreskrivits i lag i Finland med utnyttjande av det nationella spelrummet. Enligt direktivet har kommissionen dock befogenhet att anta delegerade akter om skyldigheten för kategorier av väsentliga och viktiga entiteter att använda vissa certifierade produkter. Om sådana delegerade akter antas finns det till denna del inget nationellt spelrum i ärendet.

Europeiska unionens lagstiftning möjliggör lagstiftning om bedömningen av informationssäkerheten i och beredskapen hos medlemsstaternas nationella myndigheters informationssystem och datakommunikation, eftersom den nationella bedömningsverksamheten i Finland riktas på en fallspecifik bedömning av informationssäkerheten i och beredskapen hos informationssystem eller datakommunikation som en myndighet bestämmer över eller planerar att skaffa, och inte på kraven på produkter, tjänster eller processer som erbjuds allmänt på marknaden. Certifierade produkter som finns tillgängliga på EU-marknaden kan dock utnyttjas i myndighetens informationssystem till den del deras säkerhet motsvarar myndighetens behov. I bedömningar enligt bedömningslagen kan det vara möjligt att utnyttja resultaten av certifiering enligt Europeiska unionens bestämmelser till den del som grunderna och kriterierna för certifieringen är tillämpliga.

Behoven av bedömning och godkännande av krypteringsprodukter, säkerhetskritiska produkter och TEMPEST-produkter och -mättjänster är framför allt förknippade med genomförandet av internationella förpliktelser som gäller informationssäkerheten vid elektronisk behandling av informationsmaterial som ska ges särskilt skydd och med skydd av elektronisk behandling av nationell säkerhetsklassificerad information. Grunderna för säkerhetsklassificeringen kan i allmänhet anses vara förknippade med den nationella säkerheten och i vissa fall uttryckligen med till exempel beredskap eller försvar. Sålunda verkar certifieringsbestämmelserna för Europeiska unionens inre marknad inte hindra att krav och bedömningsförfaranden fastställs för dessa syften i enlighet med nationell lagstiftning och internationella förpliktelser som gäller informationssäkerhet.

3 Målsättning

Målet för propositionen är att möjliggöra kostnadseffektiva förfaranden för bedömningen av informationssäkerheten i och beredskapen hos myndigheters informationssystem och datakommunikation. Förslaget svarar på det ökade behovet av bedömning som beror på förändringarna i verksamhetsmiljön och säkerhetshoten. Syftet är att förbättra tillgången till bedömningstjänster, att göra bedömningsförfarandena smidigare, att förtydliga bedömningsgrunderna och att effektivisera myndighetssamarbetet. Målet är att myndigheterna ska få ett bedömningsförfarande som ökar säkerheten och lämpar sig för det aktuella läget och som kan användas vid dimensioneringen av informationssäkerhetsåtgärderna i och beredskapen hos myndigheternas informationssystem och datakommunikation.

Propositionen har dessutom som mål att genom lagstiftningen klargöra principen om att det är myndigheten som ansvarar för informationssäkerheten i och beredskapen hos sina

informationssystem och sin datakommunikation och för de beslut som gäller ibruktagning av dessa. Myndigheten ansvarar för informationssäkerheten i och beredskapen hos sitt informationssystem, och den oberoende aktören som utför bedömningen ansvarar för bedömningens kvalitet.

Syftet med propositionen är att genom bedömningen och godkännandet av de säkerhetskritiska lösningarna förbättra företagens förutsättningar att erbjuda sina lösningar både i Finland och i internationella sammanhang. Målet är också att bedömningen av informationssystemen och datakommunikationen går snabbare när myndigheterna kan välja sådana lösningar för sina informationssystem och sin datakommunikation som redan är bedömda och godkända.

Propositionens mål är att främja förutsättningarna för näringsverksamheten vid bedömningsorgan för informationssäkerhet genom att förenkla och effektivisera lagstiftningen om tillförlitligheten av bedömningsorgan för informationssäkerhet och genom att göra godkännandet av kompetenser mer flexibelt. Målet är att bedömningsorganen har förutsättningar att erbjuda bedömningar som grundar sig på fler bedömningsgrunder och -kriterier än i dag.

4 Förslagen och deras konsekvenser

4.1 De viktigaste förslagen

Bedömningen av myndigheternas informationssystem och datakommunikation utvidgas så att den utöver informationssäkerhet även omfattar beredskap som ett nytt delområde i bedömningen.

En ny uppgift för bedömning av inhemska säkerhetskritiska lösningar föreskrivs för Transport- och kommunikationsverket. Säkerhetskritiska lösningar avser krypteringslösningar, lösningar för skydd mot informationsläckage via diffus strålning och andra informations- och kommunikationstekniska lösningar, det vill säga produkter, implementeringar eller tjänster som skyddar säkerhetsklassificerad information i informationssystem och datakommunikation. Finländska tillverkare ges möjlighet att hos Transport- och kommunikationsverket ansöka om bedömning och godkännande för den offentliga förteckningen över säkerhetskritiska lösningar och deras tillverkning. Dessutom preciseras Transport- och kommunikationsverkets uppgifter i rådgivningen om bedömning av informationssäkerheten och i prioriteringen av uppgifter.

Som bedömningsmyndighet fastställs utöver Transport- och kommunikationsverket även den utsedda säkerhetsmyndigheten vid Huvudstaben. För denna säkerhetsmyndighet föreskrivs uppgiften som en självständig och oberoende bedömningsmyndighet med behörighet att bedöma Försvarsmaktens egna system och tillhörande säkerhetskritiska lösningar.

För statsförvaltningsmyndigheter föreskrivs en skyldighet att genomföra bedömningen av informationssystem och datakommunikation med hjälp av de bedömningsförfaranden som avses i bedömningslagen. Bedömningsförfarandet ska väljas på grundval av en riskbedömning så att statsförvaltningsmyndigheten åtminstone genomför en självbedömning. Även andra myndigheter, såsom myndigheter i kommuner och välfärdsområden, kan använda de bedömningsförfaranden som föreskrivs i bedömningslagen i bedömningen av sina informationssystem och sin datakommunikation. Alla myndigheter ska dock begära bedömning av en bedömningsmyndighet när det gäller hantering av information som hör till säkerhetsklass I eller II. Dessutom ska alla myndigheter begära bedömning av en bedömningsmyndighet eller skaffa en bedömning av ett bedömningsorgan för informationssäkerhet när det gäller hantering

av information som hör till säkerhetsklass III, om inte myndigheten på basis av en riskbedömning beslutar att det är onödigt.

För att smidiggöra bedömningarna och förbättra tillgängligheten samt för att förtydliga lagstiftningen ska bedömningsförfarandena i bedömningslagen även inkludera en självbedömning som utförs av myndigheten och en bedömning som utförs av en tjänsteleverantör som handlar på uppdrag av myndigheten. En tjänsteleverantör som handlar på uppdrag av en myndighet kan bedöma informationssystem där offentlig och sekretessbelagd information som högst hör till säkerhetsklass IV hanteras. Ett bedömningsorgan för informationssäkerhet kan bedöma informationssystem där uppgifter som högst hör till säkerhetsklass III hanteras. De bedömningsgrunder som föreskrivs i bedömningslagen förtydligas och bestämmelserna om dem görs mindre detaljerade.

I bedömningslagen läggs till bestämmelser om bedömningsmyndigheternas samarbete, arbetsfördelning och rätt att få information och tryggas tillräckligheten av resurserna för bedömningsmyndigheternas verksamhet genom att föreskriva om en uppgift som bistår bedömningsmyndigheten.

Det föreslås att intyget om överensstämmelse ersätts med en bedömningsrapport, med undantag för situationer där internationella förpliktelser som gäller informationssäkerhet eller internationellt samarbete eller andra bestämmelser kräver att ett beslut om godkännande eller utlåtande om godkännande utfärdas om bedömningen.

Säkerställandet av tillförlitligheten av ett företag som fungerar som bedömningsorgan för informationssäkerhet förenklas och effektiviseras genom att föreskriva att en säkerhetsutredning av företag ska göras om bedömningsorganet för informationssäkerhet ansöker om behörighet för bedömning av hanteringen av säkerhetsklassificerad information. Skyddspolisens möjlighet att yttra sig om ansvariga personer och lokaler i enlighet med gällande lagstiftning gäller även i fortsättningen de bedömningsorgan för informationssäkerhet som inte ansöker om behörigheter för säkerhetsklassificerad information. Lagen föreskriver också om under vilka förutsättningar ett bedömningsorgan för informationssäkerhet kan anlita en underleverantör för att utföra sina bedömningsuppgifter. Förteckningen över allmänna förvaltningslagar som gäller offentliga förvaltningsuppgifter kompletteras så att den motsvarar nuläget och en bestämmelse om straffrättsligt tjänsteansvar läggs till i lagen.

Förfarandena för att påvisa bedömningskompetens hos ett bedömningsorgan för informationssäkerhet görs mer flexibla. Kompetensområdet anknyter alltid till kännedom om den bedömningsgrund som föreskrivs i 10 § i lagen om bedömningsorgan, såsom en författning, anvisning eller standard. Det föreslås att förutom att kompetens kan påvisas genom FINAS ackreditering och att varje godkänt bedömningsorgan för informationssäkerhet har någon ackreditering som påvisar kompetens och oberoende, föreskrivs det att Transport- och kommunikationsverket har behörighet att besluta om godkännande av nya kompetensområden efter att ha hört de myndigheter som är centrala för godkännandet av kompetensen.

Dessutom görs det tekniska ändringar i lagen om bedömningsorgan, så att bedömningslagen och lagen om bedömningsorgan även i fortsättningen bildar en samverkande helhet.

4.2 De huvudsakliga konsekvenserna

4.2.1 De ekonomiska konsekvenserna

4.2.1.1 Företag

Bedömningsorgan för informationssäkerhet

De föreslagna ändringarna i lagen om bedömningsorgan effektiviserar säkerställandet av tillförlitligheten hos bedömningsorgan för informationssäkerhet och gör godkännandet av kompetenser mer flexibelt, vilket ökar utbudet av bedömningstjänster. En uppdatering av vissa delar av lagen om bedömningsorgan i enlighet med de föreslagna ändringarna i bedömningslagen bevarar de gemensamma egenskaperna hos bedömningar som utförs av bedömningsmyndigheter och bedömningsorgan för informationssäkerhet tydliga för den som begär bedömning och den som skaffar bedömning.

Den nya möjlighet som föreslås i bedömningslagen för tjänsteleverantörer att på uppdrag av en myndighet genomföra bedömning av informationssystem och datakommunikation där det behandlas uppgifter som är offentliga eller sekretessbelagda eller hör till säkerhetsklass IV påverkar verksamheten vid de nuvarande bedömningsorganen för informationssäkerhet och kan minska deras beställningsvolymer.

Vid bedömningar av informationssystem och datakommunikation där uppgifter som hör till säkerhetsklass IV behandlas kan konkurrensförutsättningarna för bedömningsorgan för informationssäkerhet påverkas av att de krav på bedömningskompetens och -förfarande som föreskrivs i lagen om bedömningsorgan, ansökan om säkerhetsutredning av företag eller skyddspolisens bedömning inte gäller andra tjänsteleverantörer. Bedömningsorgan för informationssäkerhet förutsätts också vara oberoende, vilket begränsar deras möjlighet att konsultera planeringen av genomförandet. Detta påverkar möjligheten för bedömningsorgan för informationssäkerhet att konkurrera med andra tjänsteleverantörer genom prissättning och kan därmed skapa tryck att överföra verksamheten vid bedömningsorgan för informationssäkerhet till tjänster som erbjuds utanför den övervakade kompetensen.

År 2023 uppgick omsättningen för två bedömningsorgan för informationssäkerhet till totalt cirka 6 miljoner euro medan rörelsevinsten var totalt cirka 1,8 miljoner euro. Enligt den skriftliga respons som erhölls från representanter för bedömningsorgan för informationssäkerhet i samband med intressentmötet hösten 2024 baserar sig endast en del av omsättningen på tjänster för bedömning av informationssäkerheten som den offentliga förvaltningen skaffat. Marknaden för tjänster för bedömning av informationssäkerheten i behandlingen av säkerhetsklassificerad information som beställts av myndigheter och företag uppskattades vara cirka två miljoner euro år 2023. Detta värde i euro kan anses vara den maximala effekten av propositionen för bedömningsorgan för informationssäkerhet. [2]

I den skriftliga responsen från bedömningsorgan för informationssäkerhet som gavs hösten 2024 betonas att bedömningsmarknaden är liten. Statens center för informations- och kommunikationsteknik Valtori använder på grundval av statsrådets förordning om verksamheten i den offentliga förvaltningens säkerhetsnät och finansministeriets föreskrift och anvisningar bedömningar genomförda av bedömningsorgan för informationssäkerhet för

[2] Rapporten Tietojärjestelmien tietoturvallisuuden ja varautumisen vaatimustenmukaisuuden arvioinnin nykytila-arvio ja kehittämisehdotukset 12.12.2024, finansministeriet.

bedömning av informationssystem och datakommunikation där det behandlas information som hör till säkerhetsklass IV och III. Försvarsmakten har vid behov skaffat bedömningar av informationssystem där det behandlas information som hör till säkerhetsklasserna III och IV som köptjänster. Representanter för bedömningsorgan för informationssäkerhet har uttryckt oro för att affärsmöjligheterna försämras om den bedömningsmyndighetsuppgift som planerats för Försvarsmakten förverkligas och det blir möjligt att låta andra tjänsteleverantörer bedöma system där uppgifter som hör till säkerhetsklass IV behandlas. Bedömningsorganen för informationssäkerhet har konstaterat att om Försvarsmaktens beställningar hos bedömningsorgan för informationssäkerhet upphör, är bedömningsverksamheten inte längre attraktiv affärsverksamhet. Syftet med Försvarsmaktens egen förmåga är dock att i första hand bedöma informationssystem där information i säkerhetsklass I och II behandlas, varvid Försvarsmaktens bedömningsmyndighetsuppgift inte har någon avgörande betydelse för marknaden för köptjänster för bedömning av informationssystem där information i säkerhetsklass III och IV behandlas.

Efterfrågan på bedömningsverksamhet och -tjänster förväntas i allmänhet fortsätta att öka i framtiden på grund av förändringar i verksamhetsmiljön och EU-lagstiftningen. Certifieringsverksamhet i enlighet med EU-bestämmelserna öppnar också upp möjligheter för finländska företag att erbjuda certifieringstjänster i hela EU. Detta förutsätter utveckling av kompetens och förfaranden inom de delområden som omfattas av EU:s certifieringsregler och förvärv av status som bedömningsorgan för överensstämmelse eller anmäld organ enligt EU-bestämmelserna.

Bedömningsorganens möjligheter till näringsverksamhet påverkas också av annan lagstiftning som gäller bedömningarna som organen genomför. Detta inkluderar kraven i kunduppgiftslagen och lagen om sekundär användning om att skaffa ett intyg från ett godkänt bedömningsorgan för informationssäkerhet för vissa funktioner, finansministeriets föreskrifter om bedömning av säkerhetsnätet och i genomförandet av NIS2-direktivet de möjligheter som föreskrivs i cybersäkerhetslagen (124/2025) och i 4 a kap. i informationshanteringslagen om att använda godkända bedömningsorgan i en uppgift som bistår tillsynsmyndigheten.

Företag som tillhandahåller bedömningstjänster

På marknaden finns utöver bedömningsorgan för informationssäkerhet även företag som erbjuder experttjänster för informationssäkerhet och beredskap, såsom certifierings-, gransknings- och verifieringstjänster eller tjänster för utveckling av informationssäkerhet och beredskap som anknyter till planering och utveckling av informationssystem. Propositionen gör det möjligt för företag som tillhandahåller motsvarande tjänster och som konstaterats vara tillförlitliga att till myndigheterna erbjuda tjänster för bedömning av informationssäkerhet i och beredskap hos informationssystem och datakommunikation där det behandlas offentlig och sekretessbelagd information samt information som hör till säkerhetsklass IV enligt bedömningslagen. Antalet företag som erbjuder bedömningstjänster och utbudet av bedömningstjänster förväntas öka. Företagen förväntas i allt större utsträckning främja produktifieringen av bedömningstjänster och förbättra kvaliteten.

Propositionen ökar andelen andra marknadsaktörer än bedömningsorgan för informationssäkerhet i den helhet som bedömningsverksamheten utgör, eftersom det är möjligt att använda tjänster från företag som erbjuder bedömningstjänster både på uppdrag av myndigheter och i uppgifter som bistår bedömningsmyndigheten. Omsättningen för företag som erbjuder bedömningstjänster kan öka mer än vad som omsättningen för verksamheten vid bedömningsorgan för informationssäkerhet har uppskattats vara, eftersom en ökning av utbudet av bedömningstjänster också kan synliggöra en uppdämd efterfrågan på bedömningstjänster.

Tillverkare av säkerhetskritiska lösningar

Den föreslagna lagstiftningen som gäller bedömningen av säkerhetskritiska lösningar förbättrar möjligheterna för de finländska tillverkarnas affärsverksamhet genom bedömnings- och godkännandeprocessen för produkter och tjänster. Lagstiftningen ökar förutsägbarheten av vilka förutsättningar bedömningarna kräver, vilket uppskattas minska företagens administrativa börda. Att för Transport- och kommunikationsverket föreskriva uppgiften att bedöma en inhemsk tillverkares lösning som siktar på en plats i den offentliga förteckningen över godkända lösningar förtydligar ur tillverkarens synvinkel ansökan om bedömning med principen om ett enda serviceställe. Å andra sidan möjliggör den föreslagna lagstiftningen om bedömningsmyndigheternas samarbete, informationsutbyte och ömsesidiga överenskommelser om uppgifter en ändamålsenlig arbetsfördelning för bedömningsmyndigheterna, vilket uppskattas göra bedömningarna smidigare och stödja tillverkarnas möjligheter att snabbare få lösningar ut på marknaden. Utöver samarbetet och överenskommelserna om uppgifter främjar den för bedömningslagen föreslagna samordningen av tillämpningspraxis att bedömningsgrunderna för säkerhetskritiska lösningar är enhetliga, även om lösningen bedöms av den utsedda säkerhetsmyndigheten vid Huvudstaben för Försvarsmaktens behov och tillverkaren senare ansöker om ett mer omfattande godkännande från Transport- och kommunikationsverket.

Möjligheten för inhemska tillverkare av säkerhetskritiska lösningar att ansöka om bedömning och godkännande främjar för sin del dessa företags möjligheter att också erbjuda lösningar som är nödvändiga för att skydda EU:s och Natos säkerhetsklassificerade information.

4.2.2 Andra konsekvenser för enskilda och för samhället

4.2.2.1 Myndigheter

Verksamheten hos myndigheter som skaffar bedömningar och produktionen av tjänster

Genomförandet av de bedömningar enligt bedömningsskyldigheterna som föreslås i bedömningslagen för statsförvaltningsmyndigheter uppskattas medföra vissa kostnader för dem som omfattas av ramen för de befintliga anslagen. Den administrativa bördan ökar i de statsförvaltningsmyndigheter som inte har utfört en omfattande bedömning av huruvida överensstämmelse realiseras i informationssäkerheten i och beredskapen hos informationssystem och datakommunikation. Å andra sidan uppskattas genomförandet av bedömningar minska den administrativa bördan när det gäller hanteringen av störningar och avvikande situationer i informationssäkerheten och därmed även informationssystemens livscykelkostnader. För en sådan aktör inom den offentliga förvaltningen som upprätthåller informationssystem som utnyttjas av flera myndigheter eller som används i stor utsträckning är den administrativa bördan och kostnaderna som propositionen medför större än i den övriga offentliga förvaltningen. För att begränsa kostnaderna för genomförandet av bedömningarna kan myndigheterna om möjligt skaffa bedömningar tillsammans.

Möjligheten att i större utsträckning utnyttja självbedömningar och bedömningar som genomförts på uppdrag samt den förväntade ökningen av antalet företag som erbjuder bedömningstjänster enligt bedömningslagen uppskattas underlätta tillgången till bedömningar och dämpa ökningen av kostnaderna för bedömningar. Enligt en beräkning som gjorts i Statens center för informations- och kommunikationsteknik Valtori sparar till exempel rekrytering av två personer för att göra självbedömningar av informationssystem cirka 458 000 euro per år jämfört med att motsvarande bedömningstjänster köps från externa bedömningsorgan.

Varje ansökan hos bedömningsmyndigheterna om bedömning av myndigheternas informationssystem och datakommunikation där uppgifter som hör till säkerhetsklass I och II behandlas medför kostnader som är en nödvändig del av systemens bygg- och livscykelkostnader. Ansökningar från bedömningsorgan för informationssäkerhet om bedömningar av informationssystem och datakommunikation där information som hör till säkerhetsklass III behandlas medför i nuläget sådana kostnader som det utifrån en riskbedömning är möjligt att minska genom att genomföra bedömningen som självbedömning. Å andra sidan kan den försämring av informationssäkerheten i eller beredskapsnivån hos informationssystem eller datakommunikation som detta eventuellt medför orsaka risker, inklusive risker för den nationella säkerheten och kostnader vid störningar eller kriser.

Även om bedömningar av informationssäkerhet och beredskap som är mer omfattande än självbedömningar medför högre kostnader för myndigheterna än i dag, är det möjligt att med hjälp av bedömningarna uppnå en högre nivå av informationssäkerhet och därmed en bättre beredskaps- och reaktionsförmåga på informationssäkerhets- och personuppgiftsincidenter. På så sätt är det möjligt att förebygga personuppgiftsincidenter och deras skadliga konsekvenser, som kan orsaka kostnader både för myndigheterna och i samhället överlag för de aktörer som använder myndigheternas tjänster. Om till exempel tilltron till en myndighet eller tjänstens säkerhet förloras till följd av dataläckage, kan kostnaderna vara betydligt högre än kostnaderna för bedömningarna.

Kostnaderna för informationssäkerhetsincidenter kan grovt uppskattas utifrån vad de redan inträffade informationssäkerhetsincidenterna har kostat organisationer. Kostnaderna för störningssituationer påverkas av många olika faktorer, såsom störningens kvalitet, omfattning och konsekvenser för aktörens och verksamhetens kontinuitet samt hur snabbt aktören återhämtar sig från störningen. Störningssituationer kan orsaka både direkta utrednings- och reparationskostnader och indirekta kostnader till exempel på grund av avbrott i verksamheten eller skada på anseendet. Till exempel uppgick de direkta kostnaderna för cyberattacken mot Lahtis stad år 2019 till 685 670 euro[3]. På grund av den exponentiella ökningen av informationssäkerhetsincidenter har kostnaderna som orsakas av dem också ökat i sin helhet.

Förtydligandet av bedömningsförfarandena och förbättringen av tillgängligheten förväntas utvidga bedömningarnas omfattning och öka deras genomförandeintervall samt förbättra bedömningarnas aktualitet, vilket ökar nivån på informationssäkerheten i och beredskapen hos myndigheternas informationssystem och datakommunikation. De nya bedömningsförfaranden som läggs till i bedömningslagen förväntas öka utnyttjandet av bedömningar som informationssäkerhetsåtgärder enligt informationshanteringslagen. Det är också möjligt att kombinera bedömningen av informationssäkerheten med andra processer som föreskrivs i informationshanteringslagen, såsom den uppdatering av riktlinjerna för hantering av cybersäkerhetsrisker samt bedömningen av effektiviteten i fråga om åtgärderna för hantering av cybersäkerhetsrisker som föreskrivs i 18 c § samt utlåtandeförfarandet för ändringar i informationshanteringen enligt 9 §, vilket underlättar genomförandet av bedömningar av informationssäkerheten.

Myndigheten kan i sin egen riskbedömning anse det nödvändigt att begära en bedömning av bedömningsmyndigheten även i en situation där den föreslagna lagstiftningen inte förpliktar till det. Enligt den redan gällande bedömningslagen prioriterar Transport- och kommunikationsverket de bedömningar som begärs av den. Förslagets 4 § 3 mom. gör det dock

[3] YLE (2019) Kyberhyökkäys on maksanut Lahden kaupungille lähes 690 000 euroa https://yle.fi/a/3-10914550

också möjligt för Transport- och kommunikationsverket att genom sitt beslut avstå från att göra en bedömning som begärts av det. Mot bakgrund av de grunder som föreslås i lagen beaktar Transport- och kommunikationsverket vid prioriteringen av bedömningsbegäranden den allmänna betydelsen av de begärda åtgärderna för den allmänna förbättringen av informationssäkerheten i myndigheternas informationssystem och datakommunikation eller för skyddet av samhällets livsviktiga funktioner. I sig kan ingen myndighets begäran anses vara utan samhällelig betydelse, men Transport- och kommunikationsverket kan bli tvunget att konstatera att det inte kan utföra den begärda bedömningen på grund av brist på resurser. Transport- och kommunikationsverket kan då ge myndigheten som begärt bedömning stöd i form av rådgivning. Att göra eller underlåta att göra en bedömning påverkar inte det faktum att informationshanteringsenheten ansvarar för informationssäkerheten i och beredskapen hos informationssystem och datakommunikation.

Genomförandet av bedömningar blir dock nödvändigtvis inte vanligare och bedömningarnas positiva konsekvenser uppnås nödvändigtvis inte på alla förvaltningsnivåer, eftersom en annan myndighet än statsförvaltningsmyndighet kan besluta att inte göra ens en självbedömning av informationssäkerheten och beredskapen. Å andra sidan bedöms förslaget vara möjliggörande för kommunerna och beakta kommunernas särdrag, så det kan anses stödja kommunernas arbete med informationssäkerhet och höja nivån på informationssäkerheten i kommunerna på ett kostnadseffektivt sätt.

Utvidgningen av bedömningslagens tillämpningsområde så att det utöver bedömningen av informationssäkerheten även omfattar beredskap stöder den skyldighet att vidta förberedelser för att säkerställa att myndigheterna sköter sina uppgifter även under undantagsförhållanden som föreskrivs i 12 § i beredskapslagen. Genomförandet av bedömningar av beredskapen kan öka myndigheternas administrativa börda, eftersom bedömning av beredskapen hos informationssystem och datakommunikation inte är en etablerad praxis och de föreslagna skyldigheterna som gäller denna bedömning är nya för myndigheterna. Samtidigt förbättras dock kontinuiteten av bedömningsobjektens verksamhet, vilket minskar den administrativa bördan och kostnaderna vid störningar och undantagsförhållanden.

Förslagen om bedömning av säkerhetskritiska lösningar ökar myndigheternas möjligheter att skaffa säkra och tillförlitliga lösningar. Att välja godkända lösningar för skydd av säkerhetsklassificerad information i informationssystem och datakommunikation minskar behovet av fallspecifika produktbedömningar och påskyndar för sin del bedömningen av informationssystemet och datakommunikationen, vilket i regel uppskattas minska myndigheternas bedömningskostnader.

Bedömningsmyndigheternas verksamhet och produktion av tjänster

I propositionen föreslås inga resurstillägg för bedömningsmyndigheterna.

Transport- och kommunikationsverkets föreslagna uppgifter har inga väsentliga resurs- eller kostnadseffekter till den del som uppgifterna gäller bedömningar av informationssystem och datakommunikation eller säkerhetskritiska lösningar som hör till dem, rådgivning och samordning mellan bedömningsmyndigheter. Dessa uppgifter kan skötas med befintliga resurser som verket kan allokera i enlighet med bestämmelserna om prioritering av bedömningsuppgifter. Verkets bedömnings- och rådgivningsuppgifter är avgiftsbelagda.

Den föreslagna rätten för finländska tillverkare av säkerhetskritiska lösningar att ansöka om bedömning och godkännande hos Transport- och kommunikationsverket förutsätter inga tilläggsresurser för verket. De resurser som står till förfogande vid bedömningen av

säkerhetskritiska lösningar påverkar dock hur snabbt och effektivt Transport- och kommunikationsverket kan stödja finländska tillverkare med bedömningar och godkännanden och i hur stor utsträckning det kan svara på myndigheternas begäranden om bedömningen av olika produkter och lösningar. Möjligheten för TEMPEST-företag som erbjuder lösningar förknippade med diffus strålning att ansöka om godkännande är en ny typ av godkännande-, styrnings- och övervakningsuppgift som kan ha måttliga konsekvenser för allokeringen av resurser som helhet. Produktionen av säkerhetskritiska lösningar är en specialiserad bransch som kräver djup teknisk kompetens och investeringar, vilket innebär att antalet företag är litet, vilket i sin tur minskar den eventuella inverkan på resurser.

Den bedömningsuppgift som föreslås för Försvarsmakten är ny, och därmed är även dess resurseffekter mer betydande. Vid bildandet av uppgifterna för Försvarsmaktens bedömningsmyndighet kan det till viss del utnyttjas Försvarsmaktens nuvarande resurser, som har använts för Försvarsmaktens förpliktelser att sköta om informationssäkerheten i och de nationella kraven på informationsmaterial och informationssystem. Utöver den egentliga bedömningsverksamheten behövs det dock tilläggsresurser för stödjande funktioner, såsom ledning, juridisk kompetens och administrativ informationssäkerhet. Försvarsmakten genomför allokeringen av tilläggsresurser inom gränserna för ramar och de anslag som i övrigt ges till Försvarsmakten. När Försvarsmakten får uppbyggt bedömningsförmåga i bedömningsmyndighetens uppgift skapar ändringen också beredskap för de bedömningar som krävs enligt internationella förpliktelser som gäller informationssäkerhet. Detta kan med tiden frigöra resurser från Transport- och kommunikationsverket för andra som söker bedömning och i enlighet med målen i propositionen även förbättra tillgången till bedömningsmyndighetens bedömningar. Utvidgningen av Försvarsmaktens uppgiftsfält till bedömning av internationella system kräver ytterligare personal och kompetensutveckling.

Bedömningen av skyddet mot diffus strålning i myndigheternas informationssystem och i informationssystemen för företag som producerar tjänster för myndigheterna är en del av bedömningen av informationssäkerheten i informationssystem och kan basera sig antingen på zoner eller på lokalernas eller utrustningens förmåga att förhindra oavsiktlig diffus strålning. Bedömningen av lösningar för skydd mot diffus strålning som en del av systemen görs redan i nuläget i samband med bedömningar av system där de högsta säkerhetsklasserna behandlas. Sålunda har den föreslagna lagstiftningen om Transport- och kommunikationsverkets bedömningsuppgifter eller bedömningsuppgifterna för den utsedda säkerhetsmyndigheten vid Huvudstaben ingen omedelbar inverkan på resursbehoven. Uppgifterna sköts i praktiken genom samarbete mellan flera myndigheter och enligt dessa myndigheters bedömning kräver zon- och lokalmätningarna en liten ökning av personalresurserna för att tillgodose de kommande operativa behoven. Krypteringsprodukt- och TEMPEST-uppgifterna är också förknippade med ett behov av laboratoriekapacitet, vars resurseffekter beror på de genomförandemodeller som väljs.

De föreslagna uppgifterna som bistår bedömningsmyndigheten anses inte ha betydande kostnadseffekter. Kostnadseffekter anses inte heller uppstå genom den föreslagna lagstiftningen om bedömningsmyndigheternas samarbete eller genom möjligheten att avtala om skötseln av uppgiften eller en del av den för en annan bedömningsmyndighets räkning.

Bedömning av beredskapen hos informationssystem och datakommunikation är till sitt innehåll ett nytt delområde. Bedömningsmyndigheternas resurser påverkar i vilken utsträckning det är möjligt att utveckla beredskapskompetensen och konsekventa metoder för val, tolkning och verifiering av kriterier.

Andra myndigheters verksamhet och produktion av tjänster

Skyddspolisens arbetsbörda kan i viss mån öka genom att säkerhetsutredning av företag görs om tillverkare av säkerhetskritiska lösningar och bedömningsorgan för informationssäkerhet som ansöker om kompetens för bedömning av behandlingen av säkerhetsklassificerad information. Antalet bedömningsorgan för informationssäkerhet och företag som tillverkar och erbjuder säkerhetskritiska lösningar är dock inte stort, så inverkan på skyddspolisens uppgifter är liten. När det gäller bedömningsorgan för informationssäkerhet gör skyddspolisen även för närvarande säkerhetsutredningar av ansvariga personer och kan yttra sig om lokaler, men uppgiften utvidgas till andra delområden inom säkerhetsutredning av företag, såsom administrativ säkerhet, utredning av företagets bakgrund och uppföljning.

FINAS uppgifter kan i liten utsträckning påverkas av att ansökan om och beviljande av tilläggskompetens för ett bedömningsorgan för informationssäkerhet skulle bli möjligt enligt lagen om bedömningsorgan utan ackreditering från FINAS. Möjligheten gäller endast tilläggskompetenser och godkännande av ett bedömningsorgan för informationssäkerhet förutsätter även i fortsättningen någon lämplig FINAS-ackrediterad kompetens, såsom kompetens för certifiering av ledningssystem för informationssäkerhet enligt standarden ISO/IEC 27001. Godkännande av tilläggskompetenser genom Transport- och kommunikationsverkets beslut utan FINAS-ackreditering påverkar inte FINAS uppgifter eller ansvar, eftersom Transport- och kommunikationsverkets styrnings- och övervakningsverksamhet ansvarar för all uppföljning av dessa tilläggskompetenser. Den ackreditering som eventuellt ska ingå i det godkännande av TEMPEST-företag som föreslås i bedömningslagen medför endast små tilläggsuppgifter för FINAS med beaktande av det ringa antalet TEMPEST-företag.

Den skyldighet som föreslås i lagen om bedömningsorgan om att Transport- och kommunikationsverket ska begära ett utlåtande från myndigheter som är centrala för godkännandet av kompetensen gäller i synnerhet de myndigheter som ansvarar för att informationssystemen inom social- och hälsovården uppfyller kraven, men påverkar inte direkt dessa myndigheters uppgifter, utan tydliggör förhållandet mellan lagen om bedömningsorgan, kunduppgiftslagen och lagen om sekundär användning. På samma sätt tydliggörs myndigheternas förhållande och det samarbete som myndigheterna redan gör av förslaget att Transport- och kommunikationsverket har rätt att få uppgifter som är nödvändiga i övervakningen av uppfyllandet av kraven för bedömningsorgan för informationssäkerhet från de myndigheter som ansvarar för överensstämmelsen med kraven i social- och hälsovårdens informationssystem.

Förändringar i informationshanteringen

Genom de föreslagna ändringarna i bedömningslagen förtydligas informationshanteringsenhetens ansvar för informationsmaterialens och informationssystemens säkerhet. Dessutom stärker propositionen den allmänna nivån på informationssäkerheten och kriståligheten hos myndigheternas tjänster. Störningssituationer i informationssystem och datakommunikation kan ha betydande och omfattande negativa konsekvenser som propositionen strävar efter att hindra från att bli verklighet. God informationssäkerhet och resiliens minimerar dataläckage samt förluster av materiella och immateriella tillgångar och skador som orsakas av avbrott i användningen av informationssystemet. I och med att bedömningen av informationssäkerheten i och beredskapen hos informationssystem förbättras blir det svårare och dyrare att orsaka skadliga konsekvenser för tjänster som är centrala för myndigheternas verksamhet.

4.2.2.2 Den nationella säkerheten

Här granskas den nationella säkerheten med tanke på informationssäkerheten i och beredskapen hos myndigheternas informationssystem och datakommunikation i allmänhet och särskilt med tanke på skyddet av säkerhetsklassificerad information.

Bedömning av informationssäkerheten och beredskapen förbättrar i allmänhet informationssäkerheten i informationssystem och datakommunikation och kontinuiteten av deras verksamhet, vilket också har en positiv inverkan på den nationella säkerheten. Skyldigheten att från bedömningsmyndighet skaffa en bedömning av informationssystem och datakommunikation där uppgifter som hör till säkerhetsklass I och II behandlas förbättrar för sin del den nationella säkerheten. För informationssystem och datakommunikation där information som hör till säkerhetsklass III behandlas beror bedömningarnas positiva effekt på den nationella säkerheten delvis på vilka bedömningsförfaranden myndigheterna väljer utifrån riskbedömningen.

Försvarsförvaltningens bedömningsuppgift uppskattas ha en positiv inverkan på utvecklingen av den nationella säkerheten, eftersom tillgången till tjänster för bedömning av Försvarsmaktens informationssystem och datakommunikation ökar och beaktandet av det militära försvarets särdrag förbättras i bedömningarna, vilket i sin tur förbättrar systemens informationssäkerhet och beredskap samt snabbar upp ibruktagningen av systemen.

Säkerhetsutredningarna av bedömningsorgan för informationssäkerhet och kraven på säkerhetsutredningar av tillverkare av säkerhetskritiska produkter främjar för sin del den nationella säkerheten, eftersom detta säkerställer tillförlitligheten och säkerheten av bedömningsorgan för informationssäkerhet och tillverkare.

Med tanke på den nationella säkerheten kan behandlingen av uppgifter som gäller informationssäkerhetsarrangemang i synnerhet för behandling av uppgifter som hör till säkerhetsklass IV och arrangemang för beredskap hos myndighetens informationssystem och datakommunikation i företag som tillhandahåller bedömningstjänster medföra risk för att konfidentialiteten av uppgifter som hör till säkerhetsklass IV äventyras eller för att dessa uppgifter hamnar hos illvilliga aktörer. Riskerna kan till exempel gälla informationssäkerheten i databehandling, ansamlingen av säkerhetsklassificerad information hos tjänsteleverantören, tjänsteleverantörernas personal, leveranskedjor eller utländska möjligheter att påverka. De kan minska myndigheternas tilltro till varandras system. En bedömning som genomförs på uppdrag förutsätter sålunda noggrann bedömning av nationella risker utifrån bedömningsobjektet samt säkerställande av tjänsteleverantörens tillförlitlighet och ett ändamålsenligt skydd av myndigheternas uppgifter. På så sätt kan de positiva konsekvenserna av de i avsnitten 4.2.1 och 4.2.2.1 beskrivna bedömningarna som tjänsteleverantörer genomför på uppdrag uppnås utan att risker för den nationella säkerheten realiseras.

Propositionen bedöms ha indirekta positiva konsekvenser för medborgarnas säkerhet i och med att den främjar störningsfri verksamhet för myndigheter. Genom att främja myndighetsverksamhetens och -tjänsternas förmåga att tåla informationssäkerhetsincidenter förbättras medborgarnas säkerhet indirekt, särskilt när det i branschen eller tjänsten är fråga om faktorer som påverkar medborgarnas säkerhet. Målet med propositionen är att minska antalet informationssäkerhetsincidenter. Om synliga informationssäkerhetsincidenter blir vanligare kan det påverka medborgarnas tilltro till myndigheterna och medborgarnas upplevelse av säkerhet.

4.2.2.3 Informationssamhälle

Propositionen har positiva konsekvenser för utvecklingen av informationssamhället, eftersom den främjar införandet av informationssäkra tjänster och informationssäker praxis samt förbättrar informationssäkerheten i informationssystem och datakommunikation under hela livscykeln och höjer den allmänna nivån på informationssäkerheten. Detta skapar efterfrågan på marknaden för yrkespersoner inom informationssäkerhet och för informationssäkra produkter och tjänster. En förbättrad informationssäkerhetsnivå minskar antalet störningar i användningen av offentliga tjänster och främjar det allmänna förtroendet för digitala tjänster.

4.2.2.4 Dataskydd

Den föreslagna lagstiftningen gäller bedömning av informationssäkerheten i och beredskapen hos myndigheternas informationssystem och datakommunikation. I de system som är föremål för bedömningar behandlas vanligtvis personuppgifter och bedömningsverksamheten kan i praktiken också förutsätta behandling av personuppgifter. Därför är det nödvändigt att bedöma de föreslagna bestämmelsernas konsekvenser även i förhållande till skyddet av personuppgifter.

Den föreslagna lagstiftningen kan bedömas ha positiva konsekvenser för skyddet av personuppgifter till den del som den stärker den riskbaserade bedömningen av informationssäkerheten i och beredskapen hos statsförvaltningsmyndigheternas informationssystem och datakommunikation under hela livscykeln samt förbättrar det systematiska genomförandet och underhållet av tekniska och organisatoriska skyddsåtgärder. Detta kan minska såväl informationssäkerhetsriskerna för personuppgifter som sannolikheten för och konsekvenserna av personuppgiftsincidenter, särskilt i system där det behandlas information som behöver mer skydd och där incidenternas konsekvenser kan vara betydande även för den registrerade. När det gäller andra myndigheter än statsförvaltningsmyndigheterna riktas de positiva konsekvenserna särskilt till skyddet av personuppgifter som behandlas i informationssystem och datakommunikation där uppgifter som hör till säkerhetsklass I–III behandlas.

Enligt ansvarsskyldigheten i enlighet med artikel 5.2 i dataskyddsförordningen (EU) 2016/679 ska den personuppgiftsansvarige kunna visa att principerna för behandling av personuppgifter följs vid behandlingen av personuppgifter. Enligt artikel 24 i dataskyddsförordningen ska den personuppgiftsansvarige riskbaserat genomföra tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. Dessutom förutsätter artikel 32 i dataskyddsförordningen att den personuppgiftsansvarige ska säkerställa säkerheten i behandlingen av personuppgifter med beaktande av riskerna. De föreslagna bedömningsskyldigheterna och bedömningsförfarandena är i princip förenliga med dataskyddsförordningens riskbaserade tillvägagångssätt och kan i praktiken stödja personuppgiftsansvariga i uppfyllandet av dessa skyldigheter, särskilt när det gäller kraven på behandlingens säkerhet. Den föreslagna lagstiftningen ersätter dock inte den personuppgiftsansvariges skyldighet att göra en riskbedömning av behandlingen av personuppgifter eller genomföra åtgärder enligt dataskyddsförordningen som helhet, utan kompletterar och stöder dem med tanke på bedömningen av informationssäkerhet och beredskap.

Bedömningsförfarandena kan öka behandlingen av personuppgifter i samband med bedömningar, eftersom bedömning kan kräva åtkomst till systemen och deras tekniska data. Behandlingen av personuppgifter i samband med bedömningsverksamheten är till sin karaktär huvudsakligen verifiering av informationssäkerhet och beredskap samt bedömning av kontroller, och syftet med bedömningarna är inte att bedöma sakinnehåll som gäller de

registrerade eller att dra slutsatser som riktas till de registrerade. Riskerna för skyddet av personuppgifter ökar av att bedömningarna kan innefatta tekniska bedömningsåtgärder och tillgång till informationssystem samt av att en utomstående expert, en tjänsteleverantör eller ett godkänt bedömningsorgan för informationssäkerhet och dess underleverantörer kan vid sidan om bedömningsmyndigheten delta i genomförandet av bedömningarna.

Hanteringen av risker för skyddet av personuppgifter baserar sig på principerna i dataskyddsförordningen och den personuppgiftsansvariges skyldigheter. Den personuppgiftsansvarige ska säkerställa att personuppgifter i samband med bedömningsverksamheten endast behandlas i den omfattning som är nödvändig för att genomföra bedömningen och att testdata eller anonymiserat/pseudonymiserat material alltid föredras när det är möjligt med tanke på bedömningssyftet. Dessutom ska den personuppgiftsansvarige säkerställa att rollerna och ansvaret i behandlingen av personuppgifter bland de aktörer som deltar i bedömningsverksamheten samt en eventuell underleverantörskedja är tydliga och ändamålsenligt ordnade och att åtkomsträttigheterna och skyddsåtgärderna som gäller bedömningsmaterialet motsvarar risknivån.

5 Alternativa handlingsvägar

5.1 Handlingsalternativen och deras konsekvenser

Under beredningen av propositionen utvärderades en modell där en självständig och oberoende bedömnings- och godkännandemyndighet inrättas i samband med Statens center för informations- och kommunikationsteknik Valtori. Myndighetens uppgift skulle vara att bedöma överensstämmelsen med kraven på informationssäkerhet i och beredskap hos Valtoris tjänster och tillhörande informationssystem och datakommunikation. I modellen skulle Valtoris bedömningsverksamhet inom ramen för tillgängliga resurser kunna utnyttjas i större utsträckning för att bedöma informationssäkerheten i eller beredskapen hos kundernas informationssystem som ansluts till gemensamma informations- och kommunikationstekniska tjänster. Valtori skulle ha en avgiftsbelagd bedömningstjänst som skulle fungera parallellt med bedömningsverksamheten vid bedömningsorganen för informationssäkerhet. Modellen för ordnande av statens gemensamma informations- och kommunikationstekniska tjänster och Valtoris verksamhet grundar sig dock på separat lagstiftning, med andra ord på lagen om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster och lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015), och det är av processekonomiska skäl inte möjligt att inom ramen för denna proposition bedöma särskilda frågor som gäller bedömningen av överensstämmelse med kraven i statens gemensamma informations- och kommunikationstekniska tjänster. Det är mer ändamålsenligt att granska Valtoris roll som bedömningsaktör i samband med verksamheten i statens gemensamma branschoberoende och säkerhetsnät och uppdateringen av tillhörande lagstiftning, med beaktande av principerna i bedömningslagen som grundar sig på riskhantering

I samband med beredningen av propositionen utvärderades också en modell där de bedömningsskyldigheter som föreslås för bedömningslagen och som gäller statsförvaltningsmyndigheter föreskrivs att även gälla andra myndigheter än statsförvaltningsmyndigheter. Detta skulle stödja propositionens mål enligt vilket myndigheterna vid dimensioneringen av informationssäkerhetsåtgärderna och beredskapen hos samtliga av sina informationssystem och sin datakommunikation ska använda sig av en bedömning som lämpar sig för situationen på grund av den allt större betydelsen av informationssäkerhet i informationssystem.

Bedömningsskyldigheten är dock en ny lagstadgad uppgift för regionförvaltningen, välfärdsområdena och kommunerna, och medför kostnader för dem. Enligt statsminister Petteri Orpos regeringsprogram fortsätter regeringen att avveckla normer inom kommunernas nuvarande verksamhetsfält. Författningsändringar som medför tilläggskostnader för kommunerna kan inte anses överensstämma med regeringens mål. Kommunernas förhållanden, ekonomi och näringsstruktur varierar avsevärt runt om i landet, vilket gör att även deras förutsättningar för att bedöma informationssystem varierar mycket. Således kan det inte anses ändamålsenligt att förplikta kommunerna att bedöma informationssystem. Det ansågs inte heller motiverat att införa nya skyldigheter som eventuellt ökar kostnaderna för den regionförvaltning som är föremål för strukturreform eller för välfärdsområden som precis har inlett sin verksamhet.

I samband med arbetet med att uppdatera bedömningsverksamheten övervägdes också en modell där metoderna för att bedöma informationssäkerheten i och beredskapen hos myndigheternas informationssystem och datakommunikation skulle vara enbart självbedömning och för hantering av säkerhetsklassificerad information en bedömning som genomförs av bedömningsorgan för informationssäkerhet. Bedömningsorganen för informationssäkerhet har investerat avsevärt i utvecklingen av personalens kompetens och i utvecklingen av de lokaler, den utrustning och de processer som behövs för bedömning av informationssäkerheten. I bedömningsorganens kompetens betonas bedömningen av att säkerhetsklassificerad information hanteras med konfidentialitet och integritet. Bedömningsmyndigheterna har dock en mer gedigen kompetens än bedömningsorganen för informationssäkerhet när det gäller de funktionella kraven, verksamhetsmiljön och säkerhetsarrangemangen för informationssystem och datakommunikation där säkerhetsklasserna I och II behandlas. Vid bedömningen av informationssäkerheten i och beredskapen hos informationssystem och datakommunikation där uppgifter som hör till säkerhetsklass IV behandlas är kostnaderna för bedömningarna och säkerställandet av tillgängligheten samt bedömningen av tryggandet av tillgängligheten av informationen betydande vid sidan om bedömningen av konfidentialitet och integritet. Således kan det inte anses motiverat att bedömningarna av behandlingen av säkerhetsklassificerad information helt och hållet centraliseras till bedömningsorgan för informationssäkerhet.

Under granskningen av bedömningsskyldigheten som gäller alla myndigheter övervägdes också ett alternativ där det genom statsrådets förordning föreskrivs om en myndighets skyldighet att ansöka om bedömning från en bedömningsmyndighet eller ett bedömningsorgan för informationssäkerhet för i förordningen nämnda informationssystem eller datakommunikation som är betydande med tanke på samhällets säkerhet och beredskap. Syftet med bestämmelsen skulle ha varit att säkerställa att en bedömningsmyndighet eller ett bedömningsorgan för informationssäkerhet genomför bedömningarna av informationssäkerheten i och beredskapen hos informationssystem och datakommunikation som är av betydelse för samhällets säkerhet och beredskap, även om uppgifter som hör till säkerhetsklasserna I, II eller III inte behandlas i det system som bedöms. Det skulle till exempel ha kunnat vara fråga om ett system som är av betydelse med tanke på samhällets, statsförvaltningens, regionförvaltningens eller lokalförvaltningens funktion eller integritetsskydd, till exempel befolkningsdatasystem, fastighetsdatasystem, valsystem eller ett system för region- eller lokalförvaltning som används i säkerhets- eller beredskapsarrangemang. Alternativet genomfördes dock inte, eftersom det inte fanns grunder för att föreskriva om andra bedömningsskyldigheter på lagnivå och om denna skyldighet genom förordning. Det ansågs inte heller möjligt att på lagnivå tydligt identifiera närmare kriterier utifrån vilka bedömningsskyldigheten skulle ha krävt föreskrift genom förordning. De föreslagna ändringarna i bedömningslagen utesluter dock inte möjligheten att en innehavare av ett system som är av betydelse för samhällets beredskap och säkerhet väljer att

ansöka om bedömning av sitt system hos en bedömningsmyndighet, om det är ändamålsenligt utifrån en riskbedömning.

I samband med beredningen utreddes möjligheten att föreskriva om rätten för bedömningsorgan för informationssäkerhet att ansöka om säkerhetsutredning av person i enlighet med säkerhetsutredningslagen för att säkerställa tillförlitligheten av egen personal eller underleverantörens personal, och skyddspolisen skulle kunna utfärda intyg över säkerhetsutredning av person för personer som utför bedömningar för att förhindra utarbetandet av onödiga säkerhetsutredningar. Förslaget utreddes på grundval av att organen i samband med bedömningarna ansamlar information om genomförandet av myndigheternas informationssystem, deras säkerhetsarrangemang och brister och sårbarheter förknippade med dessa system. Förslaget ansågs också göra det möjligt att undvika flera överlappande utredningar som ansöks av myndighetskunder hos bedömningsorgan för informationssäkerhet. Bedömningsorganen för informationssäkerhet anser för närvarande att utmaningarna förknippade med säkerhetsutredningar av personer är ett problem som avsevärt påverkar bedömningsuppdragens smidighet. Beredningen av förslaget slopades dock, eftersom utgångspunkten för den rådande tillämpningspraxisen för säkerhetsutredningslagen är att utredning kan ansökas av den vars intresse ska skyddas. Även om bedömningsorganen för informationssäkerhet till skillnad från tillämpningspraxisen skulle ges rätt att ansöka om säkerhetsutredningar, är myndigheterna eventuellt ändå tvungna att även själva ansöka om utredningen. Det är ändamålsenligt att granska ärendet i samband med uppdateringen av säkerhetsutredningslagen

Ändringsbehov kopplade till smidigare bedömningsförfaranden har behandlats i större utsträckning i beredningen av propositionen än vad som ingår i de föreslagna ändringarna. De övervägda preciseringarna av lagstiftningen gällde bland annat finansministeriets styrning och anvisningar om bedömningar som begärs och skaffas av myndigheter, verifierings- eller inspektionsmetoder som används i bedömningen, bedömningskriterier, bedömningarnas giltighetstider, myndigheternas skyldigheter att upptäcka avvikelser i informationssystem och reagera på dem samt myndigheternas skyldighet att informera den offentliga förvaltningen om genomförda bedömningar. När det gäller dessa preciseringar konstaterades att finansministeriets allmänna befogenhet är tillräcklig för att tillhandahålla styrningen och anvisningarna i fråga. För de övriga synpunkterna konstaterades att för att undvika detaljerade bestämmelser som snabbt ändras lämpar synpunkterna sig bättre att genomföras med hjälp av styrning och anvisningar än som tillägg i lagstiftningen.

5.2 Lagstiftning och andra handlingsmodeller i utlandet

Vid granskning av andra staters lagstiftning och praxis är det nödvändigt att skilja kraven på skydd av behandlingen av säkerhetsklassificerad information från andra bedömningskrav på informationssystem och datakommunikation. Av kraven och praxisen för skydd av säkerhetsklassificerad information kan EU:s och Natos säkerhetsregler för skydd av säkerhetsklassificerad information anses vara de mest omfattande jämförelsepunkterna. I flera stater tillämpas Nato-bestämmelsernas verksamhetsmodeller också på skydd av nationell säkerhetsklassificerad information. Sålunda är Nato-bestämmelserna den viktigaste bedömningslagstiftningen kopplad till behandlingen av internationella och nationella säkerhetsklassificerade uppgifter. EU-bestämmelserna om bedömningen av behandlingen av säkerhetsklassificerad information överensstämmer i regel med Nato-bestämmelserna. I Finland strävar bestämmelserna om skyddet av säkerhetsklassificerad information, det vill säga säkerhetsklassificeringsförordningen, efter att beakta tillräcklig kompatibilitet med EU:s säkerhetsregler.

De mest betydelsefulla av EU:s och Natos säkerhetsregler med tanke på propositionen är skyldigheterna att bedöma och godkänna alla informationssystem och all datakommunikation där säkerhetsklassificerad information behandlas. Miniminivån för informationssäkerhetskraven har fastställts i säkerhetsreglerna och tillhörande anvisningar, men den centrala skyldigheten är att granska hot och risker systemspecifikt och fastställa säkerhetsåtgärder i enlighet med dem. Det slutliga ansvaret för informationssäkerheten ligger hos systeminnehavaren, men dess marginal i riskbedömningen begränsas av att vissa element måste godkännas av den behöriga aktör som ansvarar för bedömningen. Dessutom ska ett godkännandeutlåtande som visar den kvarstående risken utarbetas av den behöriga bedömningsaktören för informationssystemet och datakommunikationen i sin helhet. Förfarandena i EU:s och Natos säkerhetsregler, särskilt direktiven som preciserar Natos säkerhetsregler, styr också bedömaren och systeminnehavaren till samarbete från och med planeringen av informationssystemet, varvid det är möjligt att reagera på avvikelser redan under planerings- och genomförandefasen.

När det gäller skyddet av EU:s och Natos säkerhetsklassificerade information gäller bedömnings- och godkännandeskyldigheterna uttryckligen även krypteringslösningar och vissa andra IT-lösningar, såsom nätslussar, när skyddet av informationen är beroende av dessa lösningar. Krypteringslösningarna är också förknippade med krav på en andra bedömning, så kallad second party evaluation, från säkerhetsklass EU SECRET och NATO SECRET samt om krypteringslösningen ska ingå i EU:s gemensamma förteckning över godkända krypteringslösningar (LAPC, List of Approved Products). Utöver den behöriga myndigheten i Finland, det vill säga Transport- och kommunikationsverket, görs den andra bedömningen i EU av den behöriga myndigheten i AQUA-staten och i Nato av SECAN-byrån.

Detaljerna i Natos och EU:s säkerhetsregler för säkerhetskritiska produkter och lösningar skiljer sig åt något och de är också förknippade med förändringar som redan är i sikte. Vidare gäller bedömnings- och godkännandeskyldigheten i vissa säkerhetsklasser skydd av information mot konsekvenserna av oavsiktlig diffus strålning (TEMPEST). I handlingar på anvisningsnivå som kompletterar säkerhetsreglerna definieras många detaljer och förfaranden som är förknippade med tillverkningen av produkter och lösningar och med kraven på informationssäkerhet. Med hjälp av handlingar på anvisningsnivå skapas också ett förfarande för godkännande (ackreditering) av TEMPEST-företag och kontinuerlig styrning och övervakning. Syftet med förfarandet är att utse företag som har visat sin förmåga och kompetens att på ett tillförlitligt och högkvalitativt sätt producera vissa produkter eller funktioner som anknyter till skydd mot diffus strålning på ett sådant sätt att en förhandsbedömning från den behöriga TEMPEST-myndigheten inte är nödvändig. Säkerhetsreglerna förutsätter strikt styrning och övervakning, men tar inte ställning till hur ärendet genomförs rättsligt i ett land. Utnämningen av TEMPEST-företag kan således grunda sig på nationell lagstiftning eller ett nationellt förvaltningsavtal. I Finland ska även förvaltningsavtalet grunda sig på lag.

Skyddet av Estlands nationella säkerhetsklassificerade information omfattas av ett liknande ackrediteringsförfarande som till exempel EU:s och Natos säkerhetsklassificerade information. Även i Estland genomgås ackrediteringsprocessen alltså endast av informationssystem där nationell säkerhetsklassificerad information behandlas. I skyddet av informationssystem där nationell säkerhetsklassificerad information behandlas utnyttjas motsvarande krav och förfaranden som till exempel i skyddet av Natos säkerhetsklassificerade information.

I Nederländerna används ramverket General Security Requirements for Central Government (ABRO) för att bedöma skyddet av säkerhetsklassificerad information. Ramverket överensstämmer väl med till exempel Katakri i Finland. I Nederländerna har ABRO använts inom försvarsförvaltningen, men under de senaste åren har användningen av ABRO utökats

även till andra delar av den nederländska statsförvaltningen och dess intressentgrupper i bedömningar av skyddet av säkerhetsklassificerad information.

Regelbunden inspektion av informationssäkerheten hos statens ämbetsverk och aktörer inom kritisk infrastruktur rekommenderas i Danmark, Sverige, Estland, Tyskland och Nederländerna, men genomförandepraxis för inspektionerna varierar och genomförandet av NIS2-direktivet kan ha påverkat praxis. Regelbunden bedömning förutsätts med jämna mellanrum i Estland och Tyskland, medan periodiska bedömningar inte krävs i Danmark, Sverige och Nederländerna. I Estland är ministerier, ämbetsverk och statens personuppgiftsansvariga som är förknippade med informationssäkerhet skyldiga att genomföra en bedömning vartannat, vart tredje eller vart fjärde år i enlighet med skyddsklassificeringen. I Tyskland föreskrivs det att aktörer inom kritisk infrastruktur vartannat år ska visa att deras tjänster uppfyller kraven i informationssäkerhetsförordningen (IT-SiG) med hjälp av auditeringar, undersökningar eller certifikat. Även i Singapore kräver cybersäkerhetslagen att aktörer inom kritisk infrastruktur utför en informationssäkerhetsauditering minst en gång om året.

I Danmark, Sverige, Estland, Tyskland och Nederländerna erkänns och godkänns allmänt taget internationella standarder för informationssäkerhet. ISO/IEC 27001 är en erkänd standard för implementering av ledningssystem för informationssäkerhet och ISO/IEC 17021-1 ställer krav på ackrediteringsprocessen i bedömningsorgan för informationssäkerhet. I Danmark har det särskilt föreskrivits att alla statsmyndigheter ska från och med år 2014 följa ISO/IEC 27001-standarden. I Tyskland har BSI IT-Grundschutz utvecklats som ett ledningssystem för informationssäkerhet och omfattar tekniska och organisatoriska aspekter samt infrastruktur- och personalaspekter. Estland har tagit efter Tysklands IT-Grundschutz och skapat sin egen E-ITS-standard.

I Estland förutsätter förordningen om ordnande av säkerhetsåtgärder för informationssystem att auditören ska ha giltiga certifikat vid auditeringen av genomförandet av statens ledningssystem för säkerhet. Auditören ska därför ha ett CISA-certifikat (Certified Information Systems Auditor) från det lokala ISACA och ett ISO/IEC 27001-certifikat från Förenade kungarikets nationella standardiseringsorgan (British Standards Institution, BSI) eller ett ISO/IEC 27001 IT-certifikat från Tysklands cybersäkerhetsmyndighet (Bundesamt für Sicherheit in der Informationstechnik, BSI).

Endast i en del av jämförelsestaterna hittades information om bedömningsorgan för den offentliga förvaltningens informationssäkerhet eller om lagstiftning som gäller dem. Till exempel i Tyskland stöds bedömningen av myndigheternas informationssäkerhet av leverantörer av informationssäkerhetstjänster som certifierats av cybersäkerhetsmyndigheten (BSI). I Danmark, Sverige, Estland, Tyskland och Nederländerna är granskning av statsmyndigheternas informationssäkerhetssystem en del av statens revisionsverks allmänna uppgift.

6 Remissvar

6.1 Remissbehandling

Propositionen var på remiss den 27.11.2025–23.1.2026. Det kom in sammanlagt 55 utlåtanden i vilka man yttrade sig om propositionen. Det har gjorts ett sammandrag av remissvaren, där den viktigaste responsen och de mest betydande synpunkterna beskrivs. Remissvaren och sammandraget finns att tillgå i statsrådets tjänst för projektinformation med projektbeteckningen VM167:00/2023 på https://vm.fi/sv/projekt?tunnus=VM167:00/2023.

6.2 Det allmänna intrycket av utlåtandena

Det allmänna intrycket av utlåtandena är att propositionen får understöd. Förslagen bedömdes vara aktuella och motiverade och ansågs svara på förändringarna i säkerhetsmiljön.

Som förväntat framhölls i responsen från statsförvaltningsmyndigheterna farhågor om att bedömningsskyldigheterna leder till ökade resursbehov. Remissvaren bekräftar den möjlighet som förs fram i propositionens konsekvensbedömning, nämligen att de föreslagna bedömningsskyldigheterna medför kostnader för statsförvaltningsmyndigheterna. Bedömningar i enlighet med de föreslagna bedömningsskyldigheterna görs dock även i nuläget, så det är inte frågan om helt nya kostnader. Redan i nuläget utgör bedömningskostnaderna för statsförvaltningsmyndigheternas informationssystem, och i synnerhet de system som behandlar uppgifter i säkerhetsklass I-II, en väsentlig del av systemens konstruktions- och livscykelkostnader och de påverkas av faktorer som tekniska val, upphandlingsmodeller och önskad säkerhetsnivå. Myndigheterna kan dock täcka bedömningskostnaderna enligt miniminivån med sina befintliga anslag. Dessutom framhölls det framför allt i utlåtandet från kommunikationsministeriet att de resurser som står till bedömningsmyndigheternas förfogande påverkar bedömningarnas effektivitet, verkningsfullhet och tidsscheman.

I flera svar framhölls den större flexibilitet som självbedömningar möjliggör, men det påpekades också att självbedömningar kräver mer detaljerade anvisningar, till exempel avseende omfattning och noggrannhet. Utöver självbedömningar efterfrågades i remissvaren instruktioner, särskilt när det gäller bedömningen av beredskap, upphandling av bedömningstjänster från tjänsteleverantörer och användningen av kriterier. I samband med att lagändringarna verkställs är det meningen att utarbeta anvisningar om de helheter som tagits upp i remissvaren. Detta medför inga behov av ändringar i denna proposition.

Kommunförbundet konstaterar i sitt yttrande att propositionens konsekvenser för kommunerna är små, eftersom det är mycket lite information klassificerad i säkerhetsklass I–III som statsförvaltningsmyndigheterna sänder till kommunerna för behandling. När det gäller välfärdsområdena var Södra Karelens välfärdsområde av den åsikten att tillämpningsområdet inte bör utvidgas till att omfatta kommuner och välfärdsområden, eftersom det leder till ökade kostnader.

6.3 Närmare om remissvaren och de huvudsakliga ändringarna i den fortsatta beredningen

I yttrandena från riksdagens justitieombudsman, Justitiekanslersämbetet och Norra Karelens tingsrätt framhölls det att propositionen bör ta hänsyn till de högsta laglighetsövervakarnas, riksdagens ämbetsverks och domstolarnas konstitutionella särställning. Till följd av dessa yttranden uteslöts verksamhet som bedrivs av riksdagens justitieombudsman och justitiekanslern i statsrådet samt domstolarna och nämnder som inrättats för att handlägga besvärsärenden, republikens presidents kansli och riksdagens ämbetsverk från tillämpningsområdet för de föreslagna bedömningsskyldigheterna. Under den fortsatta beredningen fördes diskussioner med justitieministeriet om tillämpningen av bedömningsskyldigheter på domstolar. I fråga om tillämpningsområdet fogades ett nytt stycke om det organisatoriska tillämpningsområdet till avsnitt 10 i propositionen.

Skyddspolisen gjorde i sitt yttrande anspråk på status som bedömningsmyndighet med motiveringen att dess informationssystem innehåller mycket sensitivt och känsligt innehåll. Under den fortsatta beredningen diskuterades frågan med skyddspolisen. Utifrån yttrandet och samtalen stannade man för att den skyldighet att välja ett bedömningsförfarande på basis av

riskbedömning och säkerhetsklass som föreslås i bedömningslagen inte ska tillämpas på skyddspolisen.

Utifrån justitieministeriets yttrande fogades en konsekvensbedömning av skyddet av personuppgifter till propositionens avsnitt 4.2.2.4 och en bedömning av användningen av det nationella handlingsutrymme som dataskyddsförordningen medger till avsnitt 10.

I remissvaren framfördes också mer detaljerade preciseringsbehov till följd av vilka propositionens motiveringar kompletterades. Justitieministeriet framförde i sitt yttrande preciseringar av 3 d, 4, 4 b, 6 och 7 a § i bedömningslagen och 5, 7 och 13 § i lagen om bedömningsorgan som har beaktats antingen genom att förtydliga specialmotiveringen eller ändra paragrafformuleringen. Myndighetshörandets omfattning och roll enligt 5 § i lagen om bedömningsorgan preciserades i motiveringarna på grundval av vad Institutet för hälsa och välfärd hade framfört. Dessutom framförde Transport- och kommunikationsverket och kommunikationsministeriet i sina yttranden preciseringar som har beaktats i den fortsatta beredningen. Mest betydande bland dem är utvidgningen av den inspektionsrätt som anges i 6 § i bedömningslagen till att omfatta den utsedda säkerhetsmyndigheten vid Huvudstaben när den sköter en uppgift i enlighet med föreslagna 4 b § 2 mom. Dessutom har motiveringarna för lagstiftningsordningen i propositionens avsnitt 10 förtydligats i den fortsatta beredningen. I den fortsatta beredningen gjordes också enskilda preciseringar i propositionen i samarbete med Transport- och kommunikationsverket, kommunikationsministeriet, Försvarsmakten och försvarsministeriet. I samarbete med kommunikationsministeriet utvärderades framför allt det krav på etablering i Finland som föreslagits i 2 § 1 mom. i lagen om bedömningsorgan, bland annat med tanke på Europeiska unionens regler för den inre marknaden. På grundval av utvärderingen beslutade man att avstå från det föreslagna etableringskravet, eftersom det inte ansågs obligatoriskt att lägga till det på lagnivå.

I sitt yttrande begärde Fintraffic ett klargörande av om en aktör som sköter en offentlig förvaltningsuppgift har rätt eller skyldighet att utföra de bedömningsförfaranden som avses i lagen. Bedömningslagen tillämpas endast på aktörer som omfattas av dess definition av myndigheter, vilket innebär att lagen och där föreskrivna skyldigheter eller rättigheter inte tillämpas på sådana aktörers verksamhet som sköter offentliga förvaltningsuppgifter. Inga ändringar gjordes i propositionen till följd av detta utlåtande.

I remissvaren ställdes också några nya förslag som rörde till exempel tydligheten i föreslagna 3–3 c § i bedömningslagen, inlämnandet av bedömningsrapporter, offentligheten för förteckningen enligt föreslagna 8 a § i bedömningslagen samt bindning av riskbedömningen i bedömningar också till andra kriterier än säkerhetsklass. I den fortsatta beredningen ansågs dessa förslag dock inte vara ändamålsenliga eller genomförbara inom ramen för propositionen. De behov av preciseringar som ackrediteringstjänsten FINAS föreslog avseende den föreslagna motiveringen till 7 och 5 § i lagen om bedömningsorgan ansågs inte kunna beaktas i den fortsatta beredningen, eftersom förslagen bygger på Europeiska unionens säkerhetsregler, sedvanligt skydd av konfidentiell information i enlighet med offentlighetslagen vid sådant utbyte av information mellan myndigheter som är nödvändigt för att de ska kunna utföra sina uppgifter, och hörande av en annan myndighet i frågor som hör till dess uppgifter och expertis inom det normala samarbetet mellan myndigheter.

7 Specialmotivering

7.1 Lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation

1 § *Lagens tillämpningsområde*. Lagens tillämpningsområde utvidgas så att det till *1 mom.* i paragrafen fogas bedömning av beredskapen och bedömning av säkerhetskritiska lösningar och informationssäkerheten för tillverkningen av sådana.

Lagen innehåller framöver bestämmelser om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation och dessutom om bedömning av beredskapen hos myndigheternas informationssystem och datakommunikation. Därmed tillämpas bedömningsförfarandena, bedömningsgrunderna och övriga bestämmelser i bedömningslagen även på bedömning av beredskapen. En utvidgning av tillämpningsområdet främjar ett konsekvent beaktande av faktorer som påverkar kontinuitetshanteringen och beredskapsplaneringen för informationssystem och datakommunikation vid myndigheterna.

Dessutom innehåller lagen bestämmelser om bedömning av informationssäkerheten i säkerhetskritiska lösningar och vid tillverkningen av dem. Säkerhetskritiska lösningar behöver bedömas både som en del av myndigheternas informationssystem och datakommunikation och i situationer där tillverkaren självständigt skaffar godkännande för säkerhetskritiska lösningar för skydd av myndigheters säkerhetsklassificerade uppgifter. Bestämmelser om säkerhetskritiska lösningar utfärdas eftersom de utgör produkter och tjänster vars tillförlitlighet har en betydande roll vid skyddet av säkerhetsklassificerade uppgifter och vilka tillverkarna har möjlighet att tillhandahålla som en del av informationssystem och datakommunikation.

Till paragrafen fogas ett nytt *2 mom.* med bestämmelser om att bestämmelserna i bedömningslagen tillämpas på bedömningsmyndigheternas förfarande även i säkerhetsmyndigheternas uppgifter som hänför sig till informationssäkerheten i sådana informationssystem och sådan datakommunikation som avses i de internationella förpliktelserna som gäller informationssäkerhet, såvida inget annat föreskrivs i lagen om internationella förpliktelser som gäller informationssäkerhet eller följer av de internationella förpliktelserna som gäller informationssäkerhet. Lagen om internationella förpliktelser som gäller informationssäkerhet innehåller bestämmelser om bland annat uppgiftsfördelningen mellan de utsedda säkerhetsmyndigheterna. Internationella förpliktelser som gäller informationssäkerhet finns även i EU:s eller Natos säkerhetsbestämmelser och bilaterala informationssäkerhetsavtal. De internationella förpliktelserna som gäller informationssäkerhet och som hänför sig till informationssäkerheten i informationssystem och datakommunikation innefattar uppgifter för bedömning och godkännande av krypteringslösningar och andra säkerhetskritiska lösningar samt skydd mot informationsläckage via diffus strålning, det vill säga TEMPEST. Även vid bedömningar för att uppfylla de internationella förpliktelserna som gäller informationssäkerhet tillämpas de bestämmelser i bedömningslagen som hänför sig till förfarandet för anhängiggörande av ansökningar, fastställande av bedömningsgrunder, utfärdande av bedömningsrapporter, utlåtanden eller beslut och ändringssökande till den del som inget annat föreskrivs i rättsakterna om de internationella förpliktelserna som gäller informationssäkerhet.

Paragrafens *3 mom.* överensstämmer med det gällande 2 mom. med vissa ändringar. Namnet på den behöriga myndigheten ändras till Transport- och kommunikationsverket. Ändringen är av teknisk karaktär. I och med ämbetsverksreformen inom Transport- och kommunikationsverkets förvaltningsområde upphörde Kommunikationsverket att existera den 1 januari 2019, och den nya kommunikationsförvaltningsmyndigheten är Transport- och kommunikationsverket.

Momentet överensstämmer med det gällande momentet till den delen att det, när det gäller Transport- och kommunikationsverkets uppgifter, hänvisas till säkerhetsutredningslagen vid uppgörandet av säkerhetsutredningar av företag. Till momentet fogas en hänvisning till Transport- och kommunikationsverkets uppgifter som föreskrivs i lagen om internationella förpliktelser som gäller informationssäkerhet. Enligt 4 § i ovan nämnda lag verkar verket som en utsedd säkerhetsmyndighet i ärenden som gäller informationssäkerheten hos informationssystem och datakommunikation. En säkerhetsmyndighets uppgifter som föreskrivs i bedömningslagen påverkar inte de uppgifter för bedömning och godkännande som hänför sig till de internationella förpliktelserna som gäller informationssäkerhet.

2 § *Definitioner*. Paragrafen innehåller bestämmelser om de definitioner som används i lagen. Paragrafen ändras så att definitionerna i dess 2 och 3 punkt ändras och nya 5–10 punkten fogas till paragrafen.

Paragrafens *1 punkt* överensstämmer med 1 punkten i den gällande lagen, det vill säga att man med informationssystem avser ett helhetsarrangemang som består av databehandlingsutrustning, programvara och annan databehandling.

Paragrafens *2 punkt* ändras så att definitionen av datakommunikation preciseras. Definitionen av datakommunikation överensstämmer med den gällande definitionen med den skillnaden att ett helhetsarrangemang som består av dataöverföringsnät, dataöverföringsutrustning, programvara och annan databehandling samt förfarandena i anslutning till dem fogas till definitionen. Ändringen preciserar det faktum att system för databehandling kan omfatta såväl dataöverföringsnät, dataöverföringsutrustning, programvara och annan databehandling som sådana administrativa, funktionella och tekniska förfaranden som direkt hänför sig till dem som beskrivs i exempelvis organisationens principer, bestämmelser och anvisningar för informationssäkerhet.

Informationssystem och datakommunikation kan omfatta säkerhetskritiska lösningar. Databehandling i enlighet med definitionerna hänvisar till behandling av elektroniska data.

I paragrafens *3 punkt* utvidgas definitionen av myndighet så att de myndigheter som avses i lagen utgörs av alla myndigheter som avses i 4 § 1 mom. i lagen om offentlighet i myndigheternas verksamhet (621/1999), nedan *offentlighetslagen*. Därmed omfattar definitionen av myndighet såväl definitionen i den gällande lagen som de arbetsgrupper och motsvarande samt välfärdsområdens, välfärdssammanslutningars, kommuners och samkommuners revisorer samt andra därmed jämförbara organ som har tillsatts för att självständigt utföra en uppgift i enlighet med 4 § 1 mom. 8 punkten i offentlighetslagen. Informationshanteringslagen gäller också dessa aktörer och de kan behandla uppgifter som tillhör de högsta säkerhetsklasserna i informationssystem och datakommunikation, varvid de också ska iaktta de skyldigheter i bedömningslagen som hänför sig till bedömning av system.

Paragrafens *4 punkt* överensstämmer med den gällande lagen, det vill säga att man med statsförvaltningsmyndighet avser statliga förvaltningsmyndigheter och andra statliga ämbetsverk och inrättningar samt domstolar och andra rättskipningsmyndigheter.

Till paragrafen fogas en ny *5 punkt* med en definition av informationssäkerhet. Med informationssäkerhet avses skyddande av uppgifternas tillgänglighet, integritet och konfidentialitet genom administrativa, funktionella och tekniska åtgärder. De administrativa, tekniska eller övriga åtgärderna som definitionen avser kan exempelvis vara sådana informationssäkerhetsåtgärder som avses i informationshanteringslagen.

Med informationssäkerhet avses allmänt förfaranden som bidrar till att trygga uppgifternas konfidentialitet vid behandling av uppgifter, det vill säga skydd av uppgiftsinnehållet från oberättigad användning, uppgifternas integritet, det vill säga oföränderlighet, och uppgifternas tillgänglighet med beaktande av eventuella begränsningar av tillgängligheten på grund av uppgifternas konfidentialitet. Med behandling av uppgifter avses åtgärder som gäller mottagning, upprättande, registrering, läsning, ändring, utlämnade, kopiering, överföring, förmedling, förstöring, förvaring och arkivering av uppgifter eller ett dokument samt andra åtgärder som hänför sig till uppgifter eller ett dokument. De förfaranden som används för att genomföra informationssäkerhet kan vara administrativa, funktionella, fysiska och tekniska. Sådana är exempelvis administrativa informationssäkerhetsprinciper, krav på administrativa tillvägagångssätt som hänför sig till behandling av uppgifter, utredning av säkerheten för företag och personer, säkerhetsavtal, lokalsäkerhet, informationstekniska implementeringar, säkerhetskontroller och säkerhetskritiska lösningar.

Till paragrafen fogas en ny *6 punkt* med en definition av beredskap. Med beredskap avses åtgärder för att sörja för att utnyttjandet av informationssystem och datakommunikation samt den verksamhet som baserar sig på dem fortsätter så störningsfritt som möjligt vid störningar under normala förhållanden samt under sådana undantagsförhållanden som avses i beredskapslagen. Kontinuitet och beredskap för verksamhet kan omfatta många slags åtgärder, såsom identifiering av viktiga funktioner och informationssystem, bedömning och förvaltning av risker exempelvis genom att dubblera komponenter samt granskning och förvaltning av funktioner och leveranskedjor och reservsystem för verksamheten.

I 13 a § 3 mom. i informationshanteringslagen finns bestämmelser om informationshanteringsenhetens beredskapsskyldigheter, enligt vilka informationshanteringsenheten utifrån riskbedömningen genom beredskapsplaner och förberedelser för verksamhet i störningssituationer samt genom andra åtgärder ska se till att behandlingen av uppgiftsmaterial, utnyttjandet av informationssystem och verksamheten fortsätter så störningsfritt som möjligt i störningssituationer under normala förhållanden samt under sådana undantagsförhållanden som avses i beredskapslagen. I 3 kap. i beredskapslagen finns bestämmelser om myndigheternas beredskapsskyldigheter under undantagsförhållanden.

Till paragrafen fogas en ny *7 punkt* med en definition av bedömningsorgan för informationssäkerhet. Med bedömningsorgan för informationssäkerhet avses sådana företag, sammanslutningar och myndigheter som avses i bedömningslagen och som Transport- och kommunikationsverket har godkänt i enlighet med lagen om bedömningsorgan. Definitionen överensstämmer med hänvisningen i 3 § i den gällande lagen till bedömningsorgan och lagen om bedömningsorgan.

Till paragrafen fogas en ny *8 punkt* med en definition av säkerhetsklass. Med säkerhetsklass avses en sådan säkerhetsklass som avses i 18 § 1 mom. i informationshanteringslagen och i den statsrådsförordning som utfärdats med stöd av 4 mom. i den paragrafen. Enligt 3 § i den gällande förordningen om säkerhetsklassificering finns säkerhetsklasserna I, II, III och IV.

Till paragrafen fogas en ny *9 punkt* med en definition av säkerhetskritiska lösningar. Med säkerhetskritiska lösningar avses krypteringslösningar, lösningar för skydd mot informationsläckage via diffus strålning och andra informations- och kommunikationstekniska lösningar som skyddar säkerhetsklassificerade uppgifter i informationssystem och datakommunikation. Med lösning avses produkter, tjänster eller implementeringar som används för skydd av uppgifter som behandlas i informationssystem och datakommunikation, inklusive lagring och överföring av uppgifter mellan informationssystem eller datakommunikation genom dataanslutning. Definitionen är oberoende av teknik. En krypteringslösning kan vara till

exempel krypteringsutrustning eller krypteringsprogramvara. Skydd mot informationsläckage via diffus strålning kan genomföras genom exempelvis lokallösningar och skydd för utrustning. Säkerhetskritiska lösningar är också till exempel nätslussar.

Till paragrafen fogas en ny *10 punkt* med en ny definition av tillverkare av en säkerhetskritisk lösning. Med tillverkare av en säkerhetskritisk lösning avses ett företag som ansvarar för en säkerhetskritisk lösning under hela dess livscykel, från utveckling till underhåll. Med andra ord ansvarar företaget för de åtgärder som har betydelse för lösningens tillförlitlighet vid skyddet av säkerhetsklassificerade uppgifter. En säkerhetskritisk lösning kan bestå av flera olika element eller komponenter och det typiska är att tillverkaren skaffar element, komponenter eller funktioner för lösningen av flera olika aktörer. Företaget ansvarar för tillförlitligheten för hela leveranskedjan, inklusive tillförlitligheten för delar som skaffas av underleverantörer.

Med företag avses en fysisk person eller en annan enhet som bedriver näringsverksamhet och som, enligt 3 § 1 mom. 1–3 punkten i företags- och organisationsdatalagen (244/2001) , ska registreras i företags- och organisationsdatasystemet. Det kan alltså vara fråga om 1) fysiska personer eller dödsbon som bedriver näringsverksamhet, 2) öppna bolag, kommanditbolag, aktiebolag, andelslag, föreningar, stiftelser och andra privaträttsliga juridiska personer eller 3) staten och statliga inrättningar, kommuner, samkommuner, församlingar och andra religionssamfund samt andra offentligrättsliga juridiska personer. Däremot blir sådana utländska organisationers eller stiftelsers filialer i Finland eller europabolag, europaandelslag eller europeiska ekonomiska intressegrupperingar som avses i 3 § 4–5 punkten i lagen i praktiken inte aktuella till följd av det krav på inhemskhet som avses i föreslagna 4 § 2 mom. 1 punkten och en eventuell uteslutning av utländsk påverkan i en sådan säkerhetsutredning för företag som ska sökas enligt föreslagna 7 a §.

3 § *Förfaranden för bedömning av informationssäkerhet och beredskap*. Paragrafens rubrik ändras från anlitande av tjänster för bedömning av informationssäkerheten till förfaranden för bedömning av informationssäkerhet och beredskap. Den ändrade paragrafen innehåller bestämmelser om bedömningsförfaranden och begränsningar av användningen av dem.

Paragrafens *1 mom*. ändras så att det innehåller bestämmelser om bedömningsförfaranden som är tillgängliga för myndigheter. Det föreslås att det till de nuvarande bedömningsförfarandena fogas att självbedömning som en myndighet genomför och bedömningar som en tjänsteleverantör utför på uppdrag av en myndighet är bedömningsförfaranden utöver bedömningar som utförs av ett bedömningsorgan för informationssäkerhet och bedömningar som utförs av en bedömningsmyndighet enligt den gällande lagen.

Momentets *1 punkt* innehåller bestämmelser om självbedömning som en myndighet genomför som ett av de bedömningsförfaranden som är tillgängliga för myndigheter. Med självbedömning avses bedömning som en myndighet genomför självständigt av sådana informationssystem eller datakommunikation som omfattas av myndighetens beslutanderätt eller som det finns planer på att skaffa. Självbedömning kan också utgöras av bedömning som genomförts av flera myndigheter tillsammans eller kollegial bedömning. En myndighet som genomför självbedömning ska se till att den har den kunskap inom genomförande av informationssäkerhet och beredskap som behövs vid självbedömning. En statsförvaltningsmyndighet kan genomföra självbedömning i enlighet med förslaget till exempel i samband med det utlåtandeförfarande för sådana förändringar i informationshanteringen som avses i 9 § i informationshanteringslagen. En myndighet som genomför självbedömning kan också använda sig av en sådan informationssäkerhetsrapport om informationssystem eller datakommunikation som ska bedömas och som den fått av Statens center för informations- och kommunikationsteknik Valtori.

Momentets *2 punkt* innehåller bestämmelser om bedömningar som en tjänsteleverantör utför på uppdrag av en myndighet som ett av bedömningsförfarandena. Myndigheter har inte nödvändigtvis den kunskap och de resurser som behövs för en utförlig bedömning av i synnerhet informationssäkerheten i och beredskapen hos informationssystem och datakommunikation med hög risk. Då är det motiverat att möjliggöra bedömningar av informationssäkerhet och beredskap på uppdrag av myndigheten. Med bedömningar som en tjänsteleverantör utför på uppdrag av en myndighet avses bedömningar som utförs av någon annan än ett bedömningsorgan för informationssäkerhet eller en annan myndighet än en bedömningsmyndighet som avses i föreslagna 3 d §.

I *3 och 4 punkten* i momentet föreskrivs att bedömningar som utförs av ett bedömningsorgan för informationssäkerhet och bedömningar som utförs av sådana bedömningsmyndigheter som avsis i föreslagna 3 d § är bedömningsförfaranden. Dessa bedömningsförfaranden motsvarar de tillåtna bedömningsförfaranden som föreskrivs i 3 § i den gällande lagen.

Till paragrafen fogas ett nytt *2 mom*. med bestämmelser om att en myndighet i form av uppdrag kan anlita tjänsteleverantörer för att utföra en bedömning av sådana informationssystem eller sådan datakommunikation som behandlar uppgifter som är offentliga eller sekretessbelagda eller som högst hör till säkerhetsklass IV. Bedömning av informationssystem och datakommunikation som behandlar de högsta säkerhetsklasserna kräver omfattande kunskap och särskilda lokaler och verktyg. Om en tjänsteleverantör vill specialisera sig på bedömning av informationssystem och datakommunikation som behandlar uppgifter i säkerhetsklass III, kan den ansöka om att bli ett bedömningsorgan.

I 2 mom. i paragrafen föreskrivs också att en myndighet, när den använder sig av sådana bedömningstjänster som avses i 1 mom. 2 punkten, ska försäkra sig om tjänsteleverantörens tillförlitlighet i den omfattning som uppdraget förutsätter. Syftet med bestämmelsen är att säkerställa att endast tillförlitliga utomstående aktörer kan bedöma myndigheters informationssystem och datakommunikation.

Bedömningsuppdragen, de informationssystem och den datakommunikation som ska bedömas och de myndighetsuppgifter som en tjänsteleverantör fått i samband med ett uppdrag kan variera avsevärt, så metoderna för tillräckligt säkerställande av tillförlitligheten kan vara olika. Myndigheterna kan fastslå krav på skydd av uppgifter och leverantörernas lämplighet på det sätt som möjliggörs av upphandlingslagstiftningen. Dessutom kan myndigheterna försäkra sig om tjänsteleverantörernas tillförlitlighet genom att utreda tillgängliga uppgifter om tjänsteleverantörerna, deras ansvariga personal och deras ägare genom att använda sig av offentliga registeruppgifter, myndigheters registeruppgifter och tjänster för kredit- och företagsuppgifter.

Det är särskilt viktigt att försäkra sig om tjänsteleverantörernas tillförlitlighet vid uppdrag som innebär att tjänsteleverantörerna behandlar sekretessbelagda uppgifter, i synnerhet om uppgifterna som behandlas tillhör säkerhetsklass IV, vilken är den högsta möjliga klassen vid bedömning som utförs av tjänsteleverantörer. Därmed ska risker som hänför sig till den nationella säkerheten beaktas noggrant vid upphandling av bedömningstjänster och i avtal som gäller tjänsterna. Om villkoren uppfylls ska myndigheterna vid behov låta göra säkerhetsutredningar av de företag och personer som utför bedömningsuppgifter och som getts tillgång till myndigheternas säkerhetsklassificerade uppgifter under uppdraget. Bestämmelser om villkoren för utarbetande av säkerhetsutredningar av företag och personer finns i säkerhetsutredningslagen.

Myndigheterna ska också försäkra sig om skyddet för uppgifterna. I 26 § 3 mom. i offentlighetslagen finns bestämmelser om skyldigheten för en myndighet att på förhand försäkra sig om att uppgifterna kommer att hemlighållas och skyddas på behörigt sätt. Enligt 6 § 1 mom. i statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen ska en statsförvaltningsmyndighet på förhand säkerställa att en säkerhetsklassificerad handling skyddas på behörigt sätt om myndigheten lämnar ut den till någon annan än en statsförvaltningsmyndighet. De informationssystem och lokaler i vilka tjänsteproducenten behandlar myndighetens sekretessbelagda eller säkerhetsklassificerade uppgifter ska särskilt uppmärksammas.

Dessutom ska myndigheten beakta sådana informationssäkerhetsavtal med andra stater som är baserade på ömsesidigt skydd. I Finland kan en annan stats uppgifter som är ”RESTRICTED” i regel behandlas i sådana nationella system som uppfyller kraven för säkerhetsklass IV och övriga krav för internationella uppgifter med särskilt skydd. Behandling av EU:s och Natos säkerhetsklassificerade uppgifter är däremot tillåten endast i informationssystem och datakommunikation som ackrediterats enligt EU:s eller Natos säkerhetsbestämmelser.

Vid utarbetandet av ett upphandlingsavtal med tjänsteleverantören kan myndigheten använda sig av rekommendationer, anvisningar, bestämmelser och verktyg för fastställande av informationssäkerhetskrav för upphandlingar samt system för gemensamma upphandlingar. Systemen för gemensamma upphandlingar kan omfatta säkerhetskrav för tjänsteleverantörer och säkerhetsavtal. I sådana situationer som avses i lagen om offentlig försvars- och säkerhetsupphandling (1531/2011) kan myndigheten genomföra bedömningstjänsten i form av en försvars- och säkerhetsupphandling.

Till paragrafen fogas ett nytt *3 mom*. med bestämmelser om en ny begränsning jämfört med den gällande lagen. Enligt begränsningen kan en myndighet anlita ett bedömningsorgan för informationssäkerhet för att utföra en bedömning av informationssystem eller datakommunikation som behandlar offentliga eller sekretessbelagda uppgifter eller uppgifter i säkerhetsklass IV eller III. Bestämmelser om bedömningsorgan för informationssäkerhet och deras oberoende, tillförlitlighet och kompetens finns i lagen om bedömningsorgan. Bedömningsorgan för informationssäkerhet bedöms som säkra och kompetenta att bedöma informationssystem och datakommunikation som behandlar uppgifter i säkerhetsklass III.

3 a § *Bedömningsskyldigheter för statsförvaltningsmyndigheter* Till lagen fogas en ny 3 a § som innehåller bestämmelser om statsförvaltningsmyndigheters bedömningsskyldigheter. Paragrafen innehåller dessutom bestämmelser om vissa begränsningar av tillämpningsområdet för bedömningsskyldigheterna.

Paragrafens *1 mom*. innehåller bestämmelser om statsförvaltningsmyndigheters skyldighet att bedöma informationssäkerheten i och beredskapen hos sina informationssystem och sin datakommunikation med hjälp av de förfaranden som avses i 3 §, med andra ord självbedömning, bedömning utförd av en tjänsteleverantör, bedömning utförd av ett bedömningsorgan för informationssäkerhet eller bedömning utförd av en bedömningsmyndighet

I *2 mom*. i paragrafen finns bestämmelser om valet av bedömningsförfarande. Statsförvaltningsmyndigheter ska, på basis av en riskbedömning av informationssäkerheten i och beredskapen hos informationssystemet eller datakommunikationen, välja vem som utför bedömningen, vilka krav och kriterier som ska användas vid bedömningen och hur bedömningar ska sörjas för under informationssystemets och datakommunikationens livscykel. Olika bedömningsförfaranden kan väljas för olika delar eller delområden av informationssystemet

eller datakommunikationen. Vid valet av bedömningsförfarande kan faktorer som ett ekonomiskt och effektivt genomförande av bedömningen, krav på tillförlitlighet, integritet, tillgänglighet och kontinuitetshantering för de uppgifter som behandlas i det informationssystem eller den datakommunikation som bedöms, sekretesskrav och säkerhetsklasser, krav på och teknisk omfattning för en lämplig metod för produktion av det system som ska bedömas, metoden för genomförande, anslutning till andra system och behovet av utomstående specialkunskap i förhållande till myndighetens tillgängliga resurser. Valet av bedömningsförfarande begränsas dock av de föreslagna begränsningarna i föreslagna 3 § 2 och 3 mom. och av de föreslagna bedömningsskyldigheterna i 1 och 2 punkten i momentet.

I momentets *1 punkt* föreskrivs att statsförvaltningsmyndigheter är skyldiga att begära att en bedömningsmyndighet bedömer sådana informationssystem och sådan datakommunikation där uppgifter som hör till säkerhetsklass I eller II behandlas. Skyldigheten är motiverad eftersom bedömning av informationssystem och datakommunikation som behandlar uppgifter som tillhör de högsta säkerhetsklasserna kräver viss specialkunskap om de funktionella kraven, villkoren och säkerhetsarrangemangen för de högsta säkerhetsklasserna, inom vilket bedömningsmyndigheterna har gedigen kunskap.

I momentets *2 punkt* finns bestämmelser om statsförvaltningsmyndigheters skyldighet att av en bedömningsmyndighet eller ett bedömningsorgan för informationssäkerhet begära eller skaffa en bedömning av informationssäkerheten i och beredskapen hos informationssystem eller datakommunikation där uppgifter som hör till säkerhetsklass III behandlas, om inte statsförvaltningsmyndigheten på basis av en riskbedömning beslutar att det är onödigt. I riskbedömningen ska samma faktorer beaktas som i riskbedömningar i enlighet med momentets inledningsstycke. Den tekniska omfattningen för systemet som ska bedömas kan variera och myndigheten kan själv ha de resurser som behövs för exempelvis bedömning av arbetsstationer eller bedömning av ändringar på användningsställen. Även för bedömning av åtgärder för beredskap kan myndigheten själv ha goda förutsättningar och den bästa sakkunskapen när det gäller betydelsen av beredskap hos de system som hänför sig till myndighetens verksamhet. Om en statsförvaltningsmyndighet utifrån en riskbedömning beslutar att inte begära en bedömning av en bedömningsmyndighet eller att inte skaffa en bedömning av ett bedömningsorgan för informationssäkerhet, ska beslutet fattas i enlighet med myndighetens interna beslutanderätt, vilket ofta förutsätter ledningens godkännande.

Momentets *3 punkt* i innehåller bestämmelser om miniminivån för statsförvaltningsmyndigheters bedömningsskyldighet, det vill säga att statsförvaltningsmyndigheter alltid åtminstone ska utföra en självbedömning av informationssäkerheten i och beredskapen hos sina informationssystem och sin datakommunikation.

Enligt 13 § i informationshanteringslagen ska en informationshanteringsenhet följa upp informationsmaterialens och informationssystemens informationssäkerhet under hela deras livscykel samt identifiera relevanta risker som är förenade med informationsbehandlingen och dimensionera informationssäkerhetsåtgärderna utifrån riskbedömningen. Det är därmed inte nödvändigt att binda de föreslagna bedömningsskyldigheterna till endast användningen av informationssystem och datakommunikation, utan det är lämpligt att utföra bedömningar regelbundet under informationssystemens och datakommunikationens livscykel. Det är lämpligt att, baserat på en riskbedömning, överväga en förnyad bedömning av sådana informationssystem och sådan datakommunikation som behandlar uppgifter som tillhör säkerhetsklass I, II och III till exempel i samband med ändringar.

I *3 mom*. i paragrafen finns bestämmelser om avgränsning av de skyldigheter som gäller val av bedömningsförfarande så att de inte omfattar vissa myndigheter.

För det första föreskrivs i momentet att de skyldigheter som gäller val av bedömningsförfarande i enlighet med föreslagna 2 mom. inte tillämpas på skyddspolisens verksamhet. Förslaget är motiverat eftersom skyddspolisens informationssystem innehåller mycket känsligt innehåll. Redan risken för att innehållet hamnar hos tredje part kan äventyra skyddspolisens inhämtande av information och därmed äventyra den nationella säkerheten. Enligt skyddspolisens bedömning innebär det konsekvenser som försämrar den nationella säkerheten om bedömningar utförs av ett organ som inte tillhör skyddspolisen.

Dessutom föreskrivs i momentet att de skyldigheter som gäller val av bedömningsförfarande i enlighet med föreslagna 2 mom. i paragrafen inte tillämpas på verksamhet som bedrivs av riksdagens justitieombudsman eller justitiekanslern i statsrådet eller på domstolar, nämnder som inrättats för att handlägga besvärsärenden, republikens presidents kansli eller riksdagens ämbetsverk. De föreslagna begränsningarna av tillämpningsområdet beror huvudsakligen på den ställning som organisationerna inom den offentliga sektorn enligt grundlagen har, baserat på vilken styrningsbehörigheten för myndigheter som tillhör statens centralförvaltning inte kan utvidgas till att omfatta styrning av den interna förvaltningen av dessa organisationer.

De myndigheter som inte omfattas av de föreslagna bedömningsskyldigheterna i 2 mom. väljer sina bedömningsförfaranden av de förfaranden som föreskrivs i 3 § baserat på egen prövning. Detta innebär att de också kan begära en bedömning av informationssäkerheten av Transport- och kommunikationsverket eller skaffa en bedömning av ett bedömningsorgan för informationssäkerhet. De myndigheter som inte omfattas av skyldigheterna i 2 mom. i paragrafen ansvarar själva för informationssäkerhetsåtgärderna för de informationssystem som de använder. Därmed beslutar de ovan nämnda myndigheterna även själva i vilken mån de beaktar en bedömningsrapport av Transport- och kommunikationsverket eller ett bedömningsorgan för informationssäkerhet när de fattar beslut om deras informationssystem.

3 b § *Bedömningsskyldigheter för andra myndigheter än statsförvaltningsmyndigheter.* Till lagen fogas en ny 3 b § med bestämmelser om bedömningsskyldigheter för andra myndigheter än statsförvaltningsmyndigheter, alltså bedömningsskyldigheter för andra myndigheter än de som avses i föreslagna 3 a §. Bedömningsskyldigheterna gäller bedömning av informationssäkerheten i och beredskapen för sådana informationssystem och sådan datakommunikation som behandlar säkerhetsklassificerade uppgifter.

I *1 mom*. i paragrafen finns bestämmelser om en skyldighet för andra myndigheter än statsförvaltningsmyndigheter som motsvarar den som föreslås i 3 a § 2 mom. 1 punkten att av en bedömningsmyndighet begära bedömning av informationssäkerheten i och beredskapen hos deras informationssystem och datakommunikation som behandlar uppgifter som tillhör säkerhetsklass I eller II.

I *2 mom*. i paragrafen föreskrivs för andra myndigheter än statsförvaltningsmyndigheter en skyldighet som motsvarar den som föreslås i 3 a § 2 mom. 2 punkten att av en bedömningsmyndighet begära eller av ett bedömningsorgan för informationssäkerhet skaffa en bedömning av informationssäkerheten i och beredskapen hos sådana informationssystem eller sådan datakommunikation som behandlar uppgifter som tillhör säkerhetsklass III, om inte myndigheten på basis av en riskbedömning beslutar att det är onödigt. Utarbetandet av en riskbedömning motsvarar också den riskbedömning som föreslås i 3 a §.

Trots att den skyldighet att säkerhetsklassificera dokument vilken föreskrivs i informationshanteringslagen och förordningen om säkerhetsklassificering inte gäller andra myndigheter än statliga myndigheter, är det möjligt att även andra myndigheter behandlar säkerhetsklassificerade uppgifter i sina informationssystem eller i sin datakommunikation, varvid bedömningsskyldigheterna i den föreslagna paragrafen tillämpas. Med behandling av uppgifter avses, i enlighet med vad som skrivits i motiveringen till 2 § 5 punkten, även lagring och arkivering av uppgifter, så skyldigheten gäller även myndigheter som lagrar eller arkiverar uppgifter som tillhör säkerhetsklass I, II eller III i informationssystem eller datakommunikation.

Utöver de föreslagna bedömningsskyldigheterna som gäller andra myndigheter än statliga myndigheter kan dessa myndigheter, exempelvis kommuner, även mer omfattande använda sig av sådana bedömningsförfaranden för informationssäkerheten i och beredskapen hos informationssystem och datakommunikation som avses i bedömningslagen som en del av det identifierande av risker som är förenade med informationsbehandlingen och det dimensionerande av informationssäkerhetsåtgärderna som avses i 13 § i informationshanteringslagen. Genomförande eller skaffande av bedömningar av informationssäkerheten och beredskapen stöder riskhanteringen som hänför sig till myndigheternas informationsbehandling. Vid genomförandet av bedömningar enligt bedömningslagen gäller även begränsningarna vid användning av bedömningsförfaranden i föreslagna 3 a § 2 och 3 mom. andra myndigheter än statliga myndigheter.

3 c § *Påvisande av att kraven uppfylls.* Till lagen fogas en ny 3 c § med bestämmelser om myndigheters möjlighet att begära godkännande av en bedömningsmyndighet för sitt informationssystem eller sin datakommunikation för att visa att kraven på informationssäkerhet uppfylls i de situationer som avses i paragrafen. Behovet av godkännande och rätten att ansöka om godkännande gäller den skyldighet som följer av internationella informationssäkerhetsvillkor eller internationellt samarbete eller som föreskrivs i lag att genom ett oberoende bedömningsorgan visa för tredje part att kraven på informationssäkerhet uppfylls. En bedömning med godkännande som mål innebär att bedömningsprocessen fortsätter tills de avvikelser som observerats vid bedömningen har korrigerats, varvid bedömningsmyndigheten utarbetar ett beslut eller utlåtande om godkännande i enlighet med föreslagna 8 § 2 mom. om att de krav som använts som bedömningsgrund uppfylls. Med det att kraven uppfylls och påvisande av att kraven uppfylls avses att en bedömningsmyndighet baserat på bedömningsprocessen har konstaterat att de avvikelser som observerats vid bedömningen har korrigerats så att den myndighet som begärt bedömningen har förutsättningar att besluta om hur den kvarstående risken ska hanteras utan att detta äventyrar en tredje parts förtroendebaserade system.

De internationella förpliktelser som gäller informationssäkerhet i enlighet med lagen om internationella förpliktelser som gäller informationssäkerhet som avses i *1 punkten* i paragrafen kan till exempel vara baserade på EU:s eller Natos säkerhetsregler eller avtalsbestämmelserna i Finlands informationssäkerhetsavtal. Enligt 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet är ärenden som gäller informationssäkerheten i informationssystem och datakommunikation uppgifter som tillfaller Transport- och kommunikationsverkets uppgifter i egenskap av den utsedda säkerhetsmyndigheten.

En sådan övrig slags situation av internationellt samarbete som avses i *2 punkten* i paragrafen kan uppstå exempelvis om inga informationssäkerhetsavtal har ingåtts med den andra staten, varvid det inte uppstår några sådana internationella förpliktelser som gäller informationssäkerhet som avses i lagen om internationella förpliktelser som gäller informationssäkerhet och som är baserade på det statsavtal som avses i 1 punkten, men en oberoende bedömning och ett konstaterande att kraven på informationssäkerhet uppfylls är i

praktiken nödvändigt för att det internationella samarbetet ska kunna genomföras. Därmed kan den utsedda säkerhetsmyndigheten vid Huvudstaben på begäran av Försvarsmakten och Transport- och kommunikationsverket på begäran av en annan myndighet vid behov utarbeta ett sådant godkännande som förutsätts vid internationellt samarbete.

De förutsättningar för en bedömningsmyndighets godkännande av att kraven uppfylls som avses i *3 punkten* i paragrafen finns inte i den gällande lagstiftningen.

3 d § *Bedömningsmyndigheter*. Till lagen fogas en ny 3 d § med bestämmelser om bedömningsmyndigheter.

I *1 mom*. i paragrafen finns bestämmelser om bedömningsmyndigheterna, som utgörs av Transport- och kommunikationsverket och den utsedda säkerhetsmyndigheten vid Huvudstaben (DSA Designated Security Authority) och som avses i 4 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet. Transport- och kommunikationsverket utför bedömningsuppgifter redan med stöd av den gällande lagen, men för den utsedda säkerhetsmyndigheten vid Huvudstaben är uppgiften ny. Försvarsmaktens bedömningsuppgift behöver föreskrivas uttryckligen till den utsedda säkerhetsmyndigheten vid Huvudstaben för att säkerställa att verksamheten är oberoende. I övrigt finns bestämmelser om uppgifterna för den utsedda säkerhetsmyndigheten vid Huvudstaben i lagen om internationella förpliktelser som gäller informationssäkerhet.

Utförandet av bedömningar omfattas i huvudsak av Transport- och kommunikationsverkets behörighet.–Behörigheten för den utsedda säkerhetsmyndigheten vid Huvudstaben omfattar sådana bedömningar som gäller Försvarsmaktens egna system. Det är lämpligt att avgränsa behörigheten och uppgifterna för bedömnings- och godkännandemyndigheten för den utsedda säkerhetsmyndigheten vid Huvudstaben till Försvarsmaktens egna informationssystem, så att uppgiftsfördelningen mellan Transport- och kommunikationsverket och myndigheten förblir tydlig och så att överlappningar undviks. Den utsedda säkerhetsmyndigheten vid Huvudstaben utför bedömningar av informationssäkerheten i och beredskapen hos Försvarsmaktens egna informationssystem och egen datakommunikation som behandlar offentliga eller sekretessbelagda uppgifter eller uppgifter som tillhör någon säkerhetsklass samt bedömningar av de säkerhetskritiska lösningar som Försvarsmakten behöver i sin verksamhet.

I *2 mom*. i paragrafen föreskrivs att de bedömningsuppgifter som hör till den utsedda säkerhetsmyndigheten vid Huvudstaben också kan skötas av en person som hör till Försvarsmaktens avlönade personal och som har utsetts till uppgiften av säkerhetsmyndigheten. Vid utförandet av sina uppgifter agerar de utsedda personerna under styrning och övervakning av den utsedda säkerhetsmyndigheten vid Huvudstaben. Syftet med bestämmelsen är att säkerställa att verksamheten är oberoende.

I *3 mom*. i paragrafen föreskrivs att bedömningsmyndigheterna till sin organisation och sitt beslutsfattande ska vara oberoende vid skötseln av bedömningsuppgifterna. Bedömningsmyndigheterna ska kunna ta fram objektiv information om föremålen för bedömning baserat på utredningar de fått vid bedömningen eller information som de på annat sätt fått vid bedömningen. Bedömningsmyndigheterna ska därför i sina uppgifter vara oberoende av de beslut som föremålet för bedömningen fattar och föremålet för bedömningen ska inte kunna påverka bedömningsmyndigheternas observationer eller slutsatser. Oberoende kan säkerställas till exempel genom myndighetens arbetsordning.

Villkoret på oberoende gäller även en person som hör till Försvarsmaktens avlönade personal och som har utsetts till uppgiften av den utsedda säkerhetsmyndigheten vid Huvudstaben.

Bedömningsuppgifterna för informationssäkerhet och beredskap kan därmed inte skötas av exempelvis samma personer som leder eller genomför planeringen, byggandet eller underhållet av de informationssystem eller den datakommunikation som ska bedömas.

I 3 mom. föreskrivs dessutom att bedömningsmyndigheterna ska säkerställa att dess anställda eller personer som agerar för dess räkning har tillräcklig utbildning och erfarenhet med tanke på bedömningsuppgiftens art och omfattning. Med personer som agerar för dess räkning avses en person som hör till Försvarsmaktens avlönade personal och som har utsetts till uppgiften av den utsedda säkerhetsmyndigheten vid Huvudstaben. Bedömningsmyndigheterna ska säkerställa att den som utför en bedömning har de kunskaper som krävs för att utföra uppgifterna och att granskningen utförs objektivt. Som en del av säkerställandet av tillräcklig utbildning och erfarenhet ska bedömningsmyndigheterna följa upp den tekniska utvecklingen och upprätthålla och utveckla sin kompetens fortlöpande på det sätt som krävs för föremålen för bedömning.

4 § *Bedömningsmyndigheternas uppgifter*. Paragrafen och dess rubrik ändras så att paragrafen innehåller bestämmelser om bedömningsmyndigheternas uppgifter i stället för Kommunikationsverkets uppgifter.

Paragrafens *1 mom*. ändras så att det innehåller bestämmelser om den uppgift som innebär att bedömningsmyndigheterna, det vill säga Transport- och kommunikationsverket och den utsedda säkerhetsmyndigheten vid Huvudstaben, på begäran av en myndighet ska bedöma informationssäkerheten i och beredskapen hos informationssystemet eller datakommunikationen eller tillhörande säkerhetskritiska lösningar. Momentet överensstämmer med gällande 1 mom. 1 punkten med den skillnaden att bedömning av informationssäkerheten i säkerhetskritiska lösningar som en del av bedömningen av informationssystem och datakommunikation samt bedömning av beredskapen tillfogas som en ny bedömningsuppgift. Uppgiften omfattar även det godkännande på ansökan av en myndighet som avses i föreslagna 3 c § och det utfärdande av bedömningsrapporter samt beslut och utlåtanden om godkännande som avses i föreslagna 8 §.

Paragrafens *2 mom*. ändras så att den innehåller bestämmelser om de uppgifter som endast tilldelas Transport- och kommunikationsverket. Enligt *1 punkten* i momentet har myndigheten till uppgift att handlägga sådana begäranden om bedömning av överensstämmelse med kraven på informationssäkerhet för en säkerhetskritisk lösning och för dess tillverkning som lämnats in av tillverkare som är etablerade i Finland. Detta är en ny uppgift för Transport- och kommunikationsverket, och dess syfte är att göra det möjligt för tillverkare att begära godkännande för säkerhetskritiska lösningar och främja tillhandahållandet av och tillgången till finländska produkter för skydd av säkerhetsklassificerade uppgifter.

Syftet med en bedömning som utförts av Transport- och kommunikationsverket är att få Transport- och kommunikationsverkets godkännande om att den lösning som bedömts uppfyller kraven. Godkännandet offentliggörs i en förteckning i enlighet med föreslagna 8 c §. En bedömning av en säkerhetskritisk lösning ska omfatta en bedömning av alla sådana underleverantörer vars delar är avgörande vid bedömningen av lösningens tillförlitlighet. Vid handläggningen av en tillverkares ansökan med ett offentligt godkännande som mål är det viktigt att bedöma tillverkarens och dess underleverantörers ursprung, produktutveckling och beredskap samt själva lösningen. Bedömningen av tillverkaren och beredskapen är en viktig del av bedömningen av lösningen. Vid godkännande av en tillverkare av lösningar för skydd mot informationsläckage via diffus strålning, det vill säga TEMPEST-lösningar, är den en avgörande del av innehållet i godkännandet. En bedömning och ett godkännande av en tillverkare av lösningar för skydd mot informationsläckage via diffus strålning innebär att företaget har en konstaterad förmåga att upprätthålla kvaliteten på och förfarandena för

tillverkningen utan att en bedömningsmyndighet bedömer varenda produkt, utrustning eller annan lösning.

Med etablerad i Finland avses företag som är etablerade i Finland, vars tillverkning sker i Finland och vilka inte omfattar en risk för utländsk påverkan. Syftet med att avgränsa handläggningen av ansökningar till lösningar som tillverkas i Finland av tillverkare som är etablerade i Finland är att avgränsa Transport- och kommunikationsverkets bedömningar med ett offentligt godkännande som mål till sådan inhemsk tillverkning som verket de facto kan bedöma och följa upp. Syftet med regleringen är att bidra till att främja en praxis i Finland vilken iakttas inom de internationella förpliktelserna som gäller informationssäkerhet och enligt vilken vardera staten ansvarar för att bedöma sådan tillverkning som sker inom området för dess behörighet. I synnerhet när det gäller krypteringslösningar utgörs grunden för praxisen av ett behov av att försäkra sig om att tillverkningen inte innebär eventuella risker orsakade av oönskad utländsk påverkan. Bedömningarna av andra lösningar än inhemska säkerhetskritiska lösningar är en del av bedömningarna av informationssystem och datakommunikation enligt vad som föreskrivs i 1 mom.

I *2 punkten* i mom. finns bestämmelser om Transport- och kommunikationsverkets rådgivningsuppgift. Transport- och kommunikationsverket ska ge rådgivning om informationssäkerhetsåtgärder och bedömning av informationssäkerheten i fråga om informationssystem, datakommunikation och säkerhetskritiska lösningar. Det är fråga om en rådgivningsuppgift som är mer omfattande än sådan allmän myndighetsrådgivning som föreskrivs i 8 § i förvaltningslagen, vilken kräver djupt gående sakkunskap inom informationssäkerhet och hänför sig till identifierande av informationssäkerhetshot samt åtgärder, krav och praxis för informationssäkerhet och tillämpning av dem allmänt eller från fall till fall. Uppgiften stöder exempelvis utvecklingsprocesser för informationssystem, datakommunikation och säkerhetskritiska lösningar. Transport- och kommunikationsverket deltar i dessa processer från och med planeringsstadiet. Beräkningen och planeringen av en bedömning innebär dialog mellan den som ansökt om bedömningen och bedömningsmyndigheten. Genom dialogen utreds säkerhetsmålen för och de uppgifter som hänför sig till det tekniska genomförandet av föremålet för bedömningen samt den planerade tidsplanen för genomförandet av föremålet för bedömningen.

Transport- och kommunikationsverkets rådgivningsuppgift stöder även utnyttjandet av bedömningsorgan för informationssäkerhet vid bedömning av myndigheters informationssystem eller datakommunikation. Transport- och kommunikationsverket kan ge rådgivning i planeringsskedet för en bedömning av informationssystem eller datakommunikation, vid inriktningen av bedömningen och vid valet av bedömningsgrunder, varvid bedömningsuppgiften för bedömningsorganet för informationssäkerhet effektivt kan riktas till testning och bevisning.

Momentets *3 punkt* innehåller bestämmelser om Transport- och kommunikationsverkets nya uppgift att styra och övervaka verksamheten hos tillverkare av säkerhetskritiska lösningar som tillverkar lösningar för skydd mot informationsläckage via diffus strålning och som har fått ett beslut om godkännande som avses i 8 § 3 mom. samt att vid behov meddela beslut om krav på tillverkningen eller lösningen. Syftet är att främja förutsättningarna för verksamheten för godkända TEMPEST-företag. Styrningsmodellen är förenlig med EU:s och Natos säkerhetsbestämmelser. Enligt dem krävs ständig övervakning och styrning av TEMPEST-företag som godkänts av en behörig myndighet. Styrningen och övervakningen skapar förutsättningar för företag att ge kunderna förtroende för deras verksamhet nationellt och internationellt. De allmänna villkoren för verksamheten ska utfärdas i ett beslut om godkännande om tillverkaren av skydd mot informationsläckage via diffus strålning i enlighet

med det som föreskrivs i föreslagna 8 § 3 mom. Styrning av tolkningen av olika åtgärder och krav kan huvudsakligen ske genom rådgivning, men vid behov ska Transport- och kommunikationsverket meddela ett beslut. Åtgärderna kan gälla exempelvis stickprov för funktionskontroll som krävs vid tillverkningen av en viss produkttyp.

Paragrafens *3 mom*. ändras så att lagen även omfattar faktorer som Transport- och kommunikationsverket ska beakta när det placerar sina uppgifter i viktighetsordning med beaktande av de tillgängliga resurserna, och när det fattar beslut om huruvida verket tar på sig att utföra en begärd bedömning. Verket kan också ta på sig att utföra en begärd bedömning endast delvis. Övriga bestämmelser om det tekniska fastställandet av föremålet för bedömningen finns i 7 §.

Enligt *1 punkten* i momentet ska Transport- och kommunikationsverket även framöver i första hand sörja för de bedömningar som krävs enligt de internationella förpliktelserna som gäller informationssäkerhet. Enligt *2 punkten* i momentet ska verket också beakta myndigheternas bedömningsskyldigheter enligt föreslagna 3 a och 3 b §, enligt *3 punkten* informationens säkerhetsklass och enligt *4 punkten* tillgången till annan oberoende bedömning. I praktiken ska Transport- och kommunikationsverket med andra ord åta sig att utföra bedömningar av system som behandlar uppgifter som tillhör säkerhetsklass I och II, såvida inte behörigheten för dem tillhör den utsedda säkerhetsmyndigheten vid Huvudstaben. Dessutom ska verket prioritera bedömningar av informationssystem och datakommunikation som behandlar säkerhetsklassificerade uppgifter med beaktande av huruvida andra oberoende bedömningsorgan är tillgängliga för att utföra bedömningsuppgiften, exempelvis sådana bedömningsorgan för informationssäkerhet som har kompetens att utföra bedömningar av informationssäkerheten i och beredskapen hos informationssystem och datakommunikation som behandlar uppgifter i säkerhetsklass III och IV.

Dessutom ska Transport- och kommunikationsverket enligt *5 punkten* beakta främjande av utbudet av finländska säkerhetskritiska lösningar och enligt *6 punkten* beakta likabehandling av dem som begär och ansöker om bedömning. Momentets *7 punkt* överensstämmer med bestämmelserna i det gällande momentet om beaktande av vilken allmän betydelse de begärda åtgärderna har när det gäller allmänt förbättrande av informationssäkerheten i myndigheternas informationssystem och datakommunikation, med tillägget att även skydd för samhällets vitala funktioner ska beaktas.

Till paragrafen fogas ett nytt 4 mom. som motsvarar 2 mom. i den gällande paragrafen. Momentet innehåller därmed bestämmelser om att en sådan begäran till Transport- och kommunikationsverket som avses i 1 mom. på uppdrag av en myndighet också får framställas av den som för myndighetens räkning sköter anskaffningar eller tillhandahåller databehandlings- eller datakommunikationstjänster eller sköter serviceuppgifter med anknytning till ordnandet av dem. Enligt förarbetet till den gällande lagen har man velat säkerställa att de som anlitar databehandlings- och datakommunikationstjänster kan förvissa sig om att de tjänster som de tillhandahåller olika statsförvaltningsmyndigheter uppfyller kraven på informationssäkerhet inom statsförvaltningen (RP 45/2011 rd s. 12).

4 a § *Uppgifter för att bistå bedömningsmyndigheterna.* Till lagen fogas en ny 4 a § med bestämmelser om uppgifter för att bistå bedömningsmyndigheterna.

Som en ny möjlighet i förhållande till den nuvarande lagen föreskrivs i *1 mom*. i paragrafen att bedömningsmyndigheterna kan anlita fysiska eller juridiska personer, det vill säga företag eller sammanslutningar, som hjälp vid myndighetsbedömningar. Bedömningsmyndigheterna kan dock inte överföra bedömningsuppgiften i sin helhet till en utomstående fysisk eller juridisk

person. För att säkerställa resurser för myndighetsbedömningarna ska personalresurser kunna anlitas på den privata marknaden. Det kan vara svårt för bedömningsmyndigheterna att rekrytera tillräckligt med personal för bedömningsuppgifterna eftersom mängden kompetent personal är liten. För de kostnader som uppstår av bedömningarna ansvarar samma organ som vid bedömningar som utförs av bedömningsmyndigheter. Därmed ska bedömningsmyndigheterna avtala om användningen av utomstående sakkunniga tillsammans med det organ som ansvarar för kostnaderna för bedömningarna.

De utomstående sakkunniga som deltar i bedömningarna ska ha tillräcklig utbildning och erfarenhet med tanke på bedömningsuppgiftens art och omfattning. Vid ett uppdrag som tilldelats en utomstående sakkunnig kan bedömningsmyndigheten bestämma vilken kompetens som förutsätts av den sakkunniga och vilka bedömningskriterierna den sakkunniga ska använda. När utredningsvillkoren uppfylls och vid behov om det krävs för den nationella säkerheten eller säkerhetsklassificeringen för de uppgifter som behandlas i föremålet för bedömningen eller ett annat skäl som hänför sig till den samhälleliga säkerheten, ska det övervägas huruvida en sådan säkerhetsutredning av företag eller person som avses i säkerhetsutredningslagen behöver göras för den som utför en bedömning eller deltar i den. Bestämmelser om villkoren för utarbetande av säkerhetsutredningar av företag och personer finns i säkerhetsutredningslagen.

När utomstående sakkunniga anlitas är det fråga om överförande av en offentlig förvaltningsuppgift till privata aktörer och på de sakkunniga som utför en uppgift tillämpas bestämmelserna om straffrättsligt tjänsteansvar. Till slutet av 1 mom. fogas dessutom en informativ bestämmelse om att bestämmelser om skadeståndsansvar finns i skadeståndslagen (412/1974).

I *2 mom*. i paragrafen finns bestämmelser om att Teknologiska forskningscentralen VTT Ab (nedan Teknologiska forskningscentralen) har till uppgift att på uppdrag av en bedömningsmyndighet bedöma säkerhetskritiska lösningar. Uppgiften hänför sig till målen för cybersäkerheten, vilka har tagits upp i regeringsprogrammet för Petteri Orpos regering, statsrådets försvarsredogörelse 2024 och strategin för cybersäkerheten för åren 2024–2035. Enligt strategin för cybersäkerheten strävar Finland efter att vara självförsörjande i fråga om kritisk krypteringsteknik. Detta förutsätter att nationellt kritisk krypteringsteknik, såsom kvantsäkra krypteringslösningar, utvecklas i Finland och att den övergripande krypteringstekniska förmågan stärks bland annat inom delområdena produktion, forskning, kalkylering, dekompilering och organisering. I genomförandeplanen för strategin för cybersäkerhet av den 3 december 2024 presenteras byggande av ett nationellt krypteringstekniskt laboratorium som ett mål för att utveckla den nationella krypteringstekniska kompetensen. Samtidigt konstateras i statsrådets försvarsredogörelse att ett nationellt krypteringstekniskt laboratorium inrättas för att stödja forskning, kompetensutveckling, inhemsk produktionsförmåga och olika myndigheters uppgifter som hänför sig till krypteringsteknisk kompetens.

Den biträdande uppgift som föreslås för Teknologiska forskningscentralen och som innebär bedömande av säkerhetskritiska lösningar är motiverad eftersom det ovan nämnda krypteringstekniska laboratoriet kommer att byggas i anslutning till Teknologiska forskningscentralen.

Teknologiska forskningscentralens biträdande bedömningsuppgift möjliggör långsiktigt samarbete med bedömningsmyndigheterna. Teknologiska forskningscentralen utför inte bedömningar självständigt, utan på uppdrag och under ledning av en bedömningsmyndighet. För den uppgift som föreslås för Teknologiska forskningscentralen i momentet är det också fråga om en offentlig förvaltningsuppgift och på anställda vid Teknologiska forskningscentralen

tillämpas det krav på utbildning och erfarenhet som föreskrivs om utomstående sakkunniga i 1 mom. samt bestämmelserna om straffrättsligt tjänsteansvar.

4 b § *Informationsutbyte och samarbete mellan bedömningsmyndigheterna.* Till lagen fogas en ny 4 b § med bestämmelser om informationsutbyte, samarbete och smidig användning av resurser mellan bedömningsmyndigheterna. Förslaget behövs för att säkerställa att bedömningsmyndigheternas verksamhet är effektiv och ändamålsenlig.

I *1 mom*. i paragrafen finns bestämmelser om bedömningsmyndigheternas samarbete och rätt att få uppgifter för att sköta sina uppgifter. Bedömningsmyndigheterna ska lämna ut sådana uppgifter åt varandra som är nödvändiga för skötseln av uppgifterna trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter. Utbyte av informationen är en avgörande del av samarbetet. Syftet med samarbetet och utbytet av information är att förebygga överlappande arbete, främja en gemensam lägesbild av bedömningsbehoven för den offentliga förvaltningen och delad kunskap samt beaktande av den tekniska utvecklingen och informationssäkerhetshot och en enhetlig tolkning av kraven vid bedömningsverksamhet.

Paragrafens *2 mom*. innehåller bestämmelser om att bedömningsmyndigheterna, trots de befogenheter som föreskrivs i 3 d § 1 mom. och bedömningsmyndigheternas uppgifter som föreskrivs i 4 § 1 och 2 mom., kan avtala om att sköta enskilda uppgifter eller en del av uppgifterna för en annan bedömningsmyndighets räkning, om arrangemanget behövs för att uppgifterna ska kunna skötas på ett ändamålsenligt, ekonomiskt och snabbt sätt. Detta främjar en smidig användning av bedömningsresurser enligt den prioritering som avtalats gemensamt.

Bedömningsmyndigheterna kan avtala om att sköta uppgifter för en annan bedömningsmyndighets räkning till den del som det inte är fråga om ett ärende som ska avgöras med förvaltningsbeslut, såsom en uppgift för godkännande eller övervakning. När det gäller ärenden som ska avgöras med förvaltningsbeslut kan bedömningsmyndigheterna avtala om att för en annan bedömningsmyndighets räkning endast sköta sådana uppgifter som hänför sig till utredande av ärendet. Därmed är syftet med det föreslagna samarbetet inte att överföra en bedömningsmyndighets beslutanderätt och befogenheter till en annan bedömningsmyndighet, utan det är snarare fråga om en biträdande uppgift.

I *3 mom*. i paragrafen åläggs Transport- och kommunikationsverket att styra och samordna samarbetet mellan bedömningsmyndigheterna med syfte att skapa en enhetlig tillämpningspraxis. Syftet är att säkerställa att samarbetet och informationsutbytet mellan bedömningsmyndigheterna sker smidigt. När det gäller bedömning av säkerhetskritiska lösningar är ett viktigt mål med samordnandet av samarbetet och tillämpningspraxisen när det gäller tillverkarnas och de olika myndighetsanvändarnas behov att de informationssäkerhetskrav som tillämpas på lösningarna och tillämpningen av dem hos olika bedömningsmyndigheter inte skiljer sig från varandra. Samordningen ska sörja för att tillverkarna blir medvetna om Försvarsmaktens funktionella krav.

5 § *Utredningar på uppdrag av finansministeriet.* Paragrafen ändras så att namnet på den behöriga myndigheten ändras till Transport- och kommunikationsverket i form av en teknisk ändring.

Paragrafens *1 mom*. ändras så att det i enlighet med det utökade tillämpningsområdet för lagen omfattar såväl utredningar om nivån på informationssäkerheten och beredskapen som sådana objekt för eventuella utredningar som finansministeriet begär av Transport- och kommunikationsverket. I form av en teknisk ändring uppdateras momentet så att

finansministeriet kan begära utredningar av Transport- och kommunikationsverket i stället för termen utredning som används inom den gällande enheten.

I *2 mom*. i paragrafen uppdateras formuleringen av den rätt att få uppgifter oberoende av sekretessbestämmelserna som föreskrivs i den gällande lagen så att den gäller oberoende av sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter. I stället för en bedömning som lämnats av Transport- och kommunikationsverket gäller bestämmelserna en utredning som lämnats av Transport- och kommunikationsverket. Det är fråga om en teknisk ändring för att terminologin ska överensstämma med de ändringar som föreslås i 1 mom.

6 § *Bedömningsmyndigheternas rätt att få uppgifter, inspektionsrätt och rätt att få tillträde till lokaler och informationssystem.* Paragrafens rubrik ändras så att Kommunikationsverket byts ut mot bedömningsmyndigheterna och inspektionsrätt tillfogas.

Paragrafens *1 mom*. ändras så att rätten att få uppgifter och tillträde utvidgas till att även omfatta bedömningsmyndigheter, det vill säga både Transport- och kommunikationsverket och den utsedda säkerhetsmyndigheten vid Huvudstaben. Sakkunniga som handlar på uppdrag av bedömningsmyndigheter ersätts med sakkunniga som bistår bedömningsmyndigheterna i biträdande uppgifter i enlighet med det som föreskrivs i föreslagna 4 a §.

Rätten att få uppgifter binds till nödvändighet i stället för behövlighet, vilket föreskrivs i den gällande paragrafen. Bedömning av huruvida uppgifter är nödvändiga är bedömningsmyndigheternas uppgift, varvid de ska kunna motivera att uppgifterna är nödvändiga när de begär dem av myndigheter och företag för att utföra bedömningar, utredningar eller övervakning. Dessutom uppdateras formuleringen av den rätt att få uppgifter oberoende av bestämmelserna om sekretessbelagda uppgifter som föreskrivs i den gällande lagen så att den gäller trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter. Andra begränsningar som gäller utlämnande av uppgifter kan vara exempelvis företags affärs- eller yrkeshemligheter.

Paragrafens 1 mom. ändras också så att rätten att få uppgifter gäller de uppgifter som föreskrivs i denna lag i stället för uppgifterna om de informationssystem och den datakommunikation som ska bedömas eller som är föremål för utredning. Ändringen är motiverad eftersom de föreslagna nya uppgifterna för bedömningsmyndigheterna omfattar såväl bedömning av informationssystem och datakommunikation som exempelvis bedömning, styrning och övervakning av säkerhetskritiska lösningar och tillverkningen av dem.

Bedömningsmyndigheternas rätt att få tillträde till lokaler och informationssystem, vilken föreskrivs i 1 mom. i paragrafen, preciseras så att rätten till tillträde även omfattar datakommunikation. Dessutom fogas handlingar, utrustning och program till objekten för rätten att få information. Vid bedömning av säkerhetskritiska lösningar kan exempelvis program och källkoder behöva bedömas och utrustning behöva testas. För tydlighetens skull fogas till momentet ett omnämnande om rätten att utföra administrativa och tekniska bedömningsåtgärder. Sådana är olika tekniska kontrollåtgärder, såsom sårbarhetsscanningar av och tester för informationssystem och datakommunikation. Teknisk testning är ett nödvändigt förfarande vid bedömningar av informationssäkerheten i både informationssystem och säkerhetskritiska lösningar. Genom teknisk testning kan utredningar baserade på dokument och intervjuer bestyrkas och förmågan för informationssystem eller säkerhetskritiska lösningar observeras vid pågående skydd från olika informationssäkerhetshot. Teknisk testning kan kräva tillträde till lokaler med utrustning som används för informationssystem eller datakommunikation.

Till paragrafen fogas ett nytt *2 mom*. med bestämmelser om rätten för Transport- och kommunikationsverket och den utsedda säkerhetsmyndigheten vid Huvudstaben när den i enlighet med 4 b § 2 mom. i bedömningslagen sköter en uppgift för Transport- och kommunikationsverkets räkning att utföra inspektioner inom sådan tillsyn av tillverkare av lösningar för skydd mot informationsläckage via diffus strålning som avses i föreslagna 4 § 2 mom. 3 punkten. Vid inspektionerna kan Transport- och kommunikationsverket och den utsedda säkerhetsmyndigheten vid Huvudstaben biträdas av sådana biträdande sakkunniga som avses i 4 a §. Syftet med inspektionerna är att utreda om tillverkaren iakttar de beslut som fattats med stöd av denna lag. Med beslut som fattats med stöd av denna lag hänvisas det till sådana beslut om godkännande som avses i föreslagna 8 § 3 mom. och sådant beslutsfattande som avses i 4 § 2 mom. 3 punkten. Till skillnad från vid sådana bedömningar och utredningar som avses i 1 mom. är det vid inspektioner som hänför sig till tillsynen av bedömningsåtgärder för lösningar för skydd mot informationsläckage via diffus strålning fråga om sådana inspektioner som avses i 39 § i förvaltningslagen. Rätten att få information och tillträdet vid inspektioner överensstämmer med det som föreskrivs i 1 mom.

Till paragrafen fogas ett nytt *3 mom*. som överensstämmer med 2 mom. i den gällande lagen, med den skillnaden att tryggandet av hemfriden utvidgas till att även omfatta de inspektioner som avses i föreslagna 2 mom.

7 § *Bedömningsgrunder för informationssäkerhet och beredskap*. Paragrafens rubrik ändras så att den beaktar det utvidgade tillämpningsområde som föreslås för lagen, varvid paragrafen innehåller bestämmelser om både bedömningsgrunderna för informationssäkerhet och bedömningsgrunderna för beredskap.

Inledningsstycket i paragrafens *1 mom*. kompletteras så att paragrafens bedömningsgrunder tillämpas på såväl informationssäkerheten i myndigheters informationssystem och datakommunikation som beredskapen hos informationssystemen och datakommunikationen samt bedömning av informationssäkerheten i säkerhetskritiska lösningar och vid tillverkningen av dem.

Syftet med listningen av bedömningsgrunder i 1 mom. i paragrafen är att möjliggöra omfattande användning av olika bedömningsgrunder. Till *1 punkten* i momentet fogas krav på cybersäkerhet och beredskap utöver kraven på informationssäkerhet. Vid sidan om kraven på informationssäkerhet för myndigheternas verksamhet utfärdas även krav på cybersäkerhet, vilka det är lämpligt att beakta som en del av bedömningar av informationssystem och datakommunikation.

I stället för att nämna anvisningar för särskilda myndigheter, såsom finansministeriet och den nationella säkerhetsmyndigheten, är allmänna anvisningar för myndigheter om tillämpningen av bestämmelserna en tillräcklig och allmängiltigare metod. Myndigheterna ska försäkra sig om att anvisningarna är enhetliga och likformiga. Därmed omfattar ändrade 1 punkten det som föreskrivs i gällande 1 mom. 2 punkten.

Momentets *2 punkt* motsvarar den nuvarande 3 punkten, men i och med Finlands medlemskap i Nato tillfogas Nordatlantiska fördragsorganisationen som ett eventuellt organ som utfärdar bestämmelser, föreskrifter eller anvisningar. Till punkten fogas också myndigheternas anvisningar om tillämpningen av internationellt organs bestämmelser och anvisningar. I likhet med 1 mom. innehåller även 2 punkten såväl informationssäkerhet som cybersäkerhet och beredskap.

Momentets *3 punkt* överensstämmer med den nuvarande 4 punkten och momentets *4 punkt* överensstämmer med den nuvarande 5 punkten, med den skillnaden att båda punkterna omfattar såväl bestämmelser, föreskrifter och anvisningar om informationssäkerhet som bestämmelser, föreskrifter och anvisningar om samt krav om beredskap och cybersäkerhet.

Paragrafens *2 mom*. ändras så att det innehåller bestämmelser om de faktorer som ska beaktas vid fastställandet av bedömningsgrunderna och föremålet för en bedömning.

Med fastställande av bedömningsgrunderna avses fastställande av krav som är lagstadgade och som valts ut baserat på en riskbedömning utifrån den helhet av bedömningsgrunder som föreskrivs i 1 mom. Med föreskrivna krav avses exempelvis bestämmelserna i offentlighetslagen, informationshanteringslagen och förordningen om säkerhetsklassificering. Utarbetandet av en riskbedömning baseras på identifiering av hot. Hoten är allmänt kända informationssäkerhetshot som gäller informationssystem och datakommunikation oavsett sektor. Hoten är också särskilda informationssäkerhetshot mot föremålet för bedömningen som kan hänföra sig till exempelvis den betydelse som det system som bedöms har för den samhälleliga säkerheten, för den nationella säkerheten, för myndighetens verksamhet, med tanke på illasinnade aktörer när det gäller intresset för verksamheten för föremålet för bedömningen, för tillgången till tjänster för sammanslutningar och medborgare eller vissa tekniska metoder för genomförande. Vid en riskbedömning för fastställande av bedömningsgrunder ska även kraven på tillförlitlighet, integritet, tillgänglighet och kontinuitetshantering för de uppgifter som behandlas i föremålet för bedömningen samt kraven på den tekniska metoden för genomförande beaktas. Vid identifieringen av kraven beaktas exempelvis den administrativa, funktionella, fysiska och tekniska säkerheten, kontinuitetshanteringen, beredskapen och dataskyddet. En bedömning kan även baseras på bedömningskriterier som är baserade på en mindre mängd krav.

Med fastställande av föremålet för bedömningen avses de avgränsningar som görs vid planeringen av en bedömning. Föremålet för bedömningen kan variera alltifrån en arbetsstation till ett nätverk av många verksamhetsställen eller exempelvis vara en multinationell leverantörs molntjänst som används i omfattande grad inom en organisation. Avgränsningen av föremålet för bedömningen omfattar sådana delar av informationssystem eller datakommunikation som har väsentliga konsekvenser för informationssäkerheten i och beredskapen hos de uppgifter som behandlas. Till exempel är det ofta motiverat att inkludera terminalutrustning för informationssystemet, användningsställena och de förvaltningslösningar som används för underhåll i bedömningen.

I momentet föreskrivs också att det vid bedömningar som begärs av bedömningsmyndigheter är på bedömningsmyndigheternas ansvar att fastställa bedömningsgrunderna. Enligt god förvaltning ska bedömningsmyndigheterna höra den som begär bedömningen innan bedömningsgrunderna fastställs. På så sätt säkerställs utnyttjandet av bedömningsmyndigheternas sakkunskap och ändamålsenligheten för bedömningarna som stöd för riskhanteringen för den myndighet som begär bedömningen. Vid behov ger bedömningsmyndigheten myndigheten råd under planeringen av bedömningen eller medan bedömningen framskrider, i och med att genomförandet preciseras eller ändras.

Vid självbedömningar som utförs av en myndighet och bedömningar som en tjänsteleverantör utför på uppdrag av en myndighet fastställer myndigheten bedömningsgrunderna, föremålet för bedömningen och inriktningen för den. Lagen om bedömningsorgan innehåller bestämmelser om bedömningsgrunderna vid ett uppdragsförhållande mellan ett bedömningsorgan för informationssäkerhet och dess kund.

Till paragrafen fogas ett nytt *3 mom*. med bestämmelser om fastställande av bedömningsgrunderna för säkerhetskritiska lösningar och beredningen av sådana. Bedömningsmyndigheten fastställer lämpliga bedömningsgrunder för lösningen utifrån vad som föreskrivs om bedömningsgrunderna i 1 mom. efter att ha hört tillverkaren av den säkerhetskritiska lösningen i enlighet med god förvaltning. Fastställandet av bedömningsgrunder kan göras bäst i form av ett samarbete mellan bedömningsmyndigheten och tillverkaren. Det gäller i synnerhet vid sådana bedömningar där säkerheten kräver bedömning redan i utvecklingsstadiet. En bedömning stöder därmed även tillverkarens utvecklings- och planeringsarbete.

Vid fastställandet av bedömningsgrunderna beaktas sådana säkerhetshot som vanligen påverkar lösningen på det sätt som beskrivs i motiveringen till 2 mom. Dessutom beaktas säkerhetsklassen, säkerheten vid tillverkningen och beredskapen att uppfylla de internationella förpliktelserna som gäller informationssäkerhet. Med säkerheten vid tillverkningen avses faktorer som hänför sig till tillverkningsföretaget och leveranskedjan samt en säker produktutveckling, planering och tillverkning, säkert underhåll och andra åtgärder. Med beredskapen att uppfylla internationella förpliktelser avses att målet med bedömningen är att främja tillverkarens möjligheter att för sin lösning även få ett sådant godkännande som eventuellt krävs enligt de internationella förpliktelserna som gäller informationssäkerhet. I detta avseende kan olika källor till de internationella förpliktelserna som gäller informationssäkerhet direkt utnyttjas som en del av bedömningsgrunderna eller grunderna fastställas så att fortsatt utveckling för att uppfylla de internationella förpliktelserna som gäller informationssäkerhet är möjlig.

7 a § *Utredningar som hänför sig till bedömningar av tillverkare av säkerhetskritiska lösningar*. Till lagen fogas en ny 7 a § med bestämmelser om utredningar som hänför sig till bedömningar av tillverkare av säkerhetskritiska lösningar.

I *1 mom*. i paragrafen föreskrivs Transport- och kommunikationsverket en ny skyldighet när det gäller förfarandet som innebär att verket vid en sådan bedömning av en säkerhetskritisk lösning och av dess tillverkning som avses i 4 § 2 mom. 1 punkten ska ansöka om en sådan säkerhetsutredning av företag som avses i säkerhetsutredningslagen i fråga om den tillverkare som ansöker om bedömningen. Dessutom föreskrivs att godkännandet av en säkerhetskritisk lösning förutsätter att det i den säkerhetsutredning av företag som gäller tillverkaren inte har framkommit något som utifrån en helhetsbedömning skulle äventyra tillverkningens säkerhet och tillförlitlighet i synnerhet med hänsyn till riskerna för utländsk påverkan. Med tillverkningens säkerhet och tillförlitlighet avses till exempel ägandet av företaget, de ansvariga personerna, den ekonomiska situationen, leveranskedjorna som hänför sig till tillverkningen av säkerhetskritiska lösningar samt informationssäkerheten för lokaler och sådana informationssystem och sådan datakommunikation som påverkar tillverkningen. Betydelsen av de faktorer som hänför sig till beredskap ska sättas i relation till säkerhetsklassen och karaktären för den säkerhetskritiska lösningen och hur utsatt den är för att dess tillförlitlighet ska äventyras.

Paragrafens *2 mom*. innehåller bestämmelser om situationer där en internationell standard används som en del av bedömningsgrunderna och det är möjligt att ackreditera kompetensen enligt den med hjälp av FINAS ackrediteringsförfarande som föreskrivs i lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven. Förfarandet är inte obligatoriskt, utan Transport- och kommunikationsverket kan överväga grunderna för godkännande. Grunderna för godkännande kan omfatta behandling av internationella uppgifter med särskilt skydd eller säkerhetsklassificerade uppgifter, vilket kan påverka möjligheten att använda ackrediteringstjänsten FINAS smidigt.

Förslaget möjliggör också att en ackreditering som tillverkaren eventuellt fått redan tidigare kan beaktas som en del av grunderna för godkännande. Vid bedömning av tillverkare av lösningar för skydd mot informationsläckage via diffus strålning kan ansökan gälla godkännande av själva tillverkaren som ett TEMPEST-företag. Skydd mot informationsläckage via diffus strålning är ett snävt tekniskt specialområde som omfattar de högsta säkerhetsklasserna. Som bedömningsgrunder används i första hand internationella källor som utarbetats för skydd av säkerhetsklassificerade uppgifter. Vid bedömning av tillverkningsförfaranden kan samma standarder användas som även används inom andra tillverkningssektorer, såsom ackrediteringar enligt ISO/IEC 17025 och ISO/IEC 9001. Därmed kan FINAS ackreditering användas vid bedömning av standardenligheten för tillverkarens kompetens. Vid ackreditering som beaktar godkännandet av ett TEMPEST-företag som en grund är det inte nödvändigt att beakta detaljerade säkerhetsklassificerade tekniska substansuppgifter, utan att processerna är enhetliga och jämförbara.

8 § *Utfärdande av bedömningsrapport, beslut om godkännande och utlåtande om godkännande.* Paragrafens rubrik ändras så att den gäller utfärdande av bedömningsrapporter, beslut om godkännande och utlåtande om godkännande i stället för utfärdande av intyg.

Paragrafens *1 mom*. ändras så att det innehåller bestämmelser om bedömningsrapporter som ska utarbetas om bedömningar. Bedömningsrapporter ska utarbetas för alla bedömningar som utförs enligt det förfarande som avses i föreslagna 3 § 1 mom.

Utifrån resultatet av bedömningen utarbetar den som utför en bedömning en rapport över nivån för informationssäkerhet och beredskap och eventuella risker för föremålet för bedömningen. Rapporten ska innehålla uppgifter om föremålet för bedömningen, vilka bedömningsgrunder som använts, bedömningens omfattning och vilka observationer som gjorts. Med bedömningens omfattning avses till exempel de autentiseringsmetoder som använts, hur djupgående bedömningen är, såsom vilka penetrationstest som använts vid den tekniska bedömningen, eller granskning av koden samt bedömningens tidsmässiga och organisatoriska omfattning. I rapporten kan lindriga eller till och med kraftiga avvikelser vid genomförandet av bedömningsgrunderna tas upp. Myndigheter behöver bedömningsrapporter när de fattar beslut om kvarstående risker samt ibruktagning och användning av informationssystem eller datakommunikation.

Syftet med en bedömningsrapport är att förtydliga myndigheternas ansvar när det gäller informationssäkerheten i deras informationssystem och datakommunikation. Genom användningen av bedömningsrapporter förbättras och harmoniseras kvaliteten på de beslut som myndigheterna fattar när det gäller åtgärder för informationssäkerhet och beredskap samt kvarstående risker i informationssystem och datakommunikation, eftersom bedömningsrapporterna utökar myndigheternas kunskapsunderlag om riskerna när det gäller förutsättningarna, informationssystem och datakommunikation.

Paragrafens *2 mom*. ändras så att det innehåller bestämmelser om bedömningsmyndigheternas uppgift att meddela beslut om godkännande och ge utlåtanden om godkännande, när en myndighet har ansökt om godkännande enligt föreslagna 3 c § och det informationssystem eller den datakommunikation som ska bedömas uppfyller de krav som ställs i bedömningen. Dessutom innehåller momentet bestämmelser om uppgifter som har betydelse för beslut om godkännande och utlåtanden om godkännande. I beslutet eller utlåtandet ska det antecknas uppgifter om det föremål för bedömningen som godkänts av bedömningsmyndigheten och dess tekniska avgränsning, vilka bedömningsgrunder som använts, bedömningens omfattning, resultatet av bedömningen och kvarstående risk samt vid behov uppgift om giltighetstiden.

För formen på och innehållet i ett godkännande av informationssystem som godkänts för behandling av EU:s eller Natos säkerhetsklassificerade uppgifter finns olika krav i olika situationer, och till formen kan de utgöra exempelvis utlåtanden om godkännande, tillfälliga utlåtanden eller beslut om godkännande. Konsekvenserna av dessa utlåtanden och beslut i bedömningsprocessen bestäms av de internationella förpliktelserna som gäller informationssäkerhet. Förfarandena varierar beroende på om det är fråga om ett system som EU eller Nato levererar till Finland eller ett internationellt uppbyggt system som är avsett för behandling av EU:s eller Natos säkerhetsklassificerade uppgifter. Vid bedömningen av ett internationellt system ansvarar systemets ansvarsmyndighet för godkännandet och i ett utlåtande om godkännande för godkännandet av den kvarstående risk som uppkommer. Ansvarsmyndigheten ska beakta resultatet av den oberoende bedömningen. Vid bedömningen av ett internationellt system ges ett utlåtande om godkännande genom ett beslut och i vissa situationer ges ett eventuellt tillfälligt utlåtande om godkännande genom ett tillfälligt beslut, vilket innehåller villkoren för att ett egentligt utlåtande om godkännande ska kunna ges. Vid bedömningen av ett levererat system ligger däremot fokus för den bedömning som görs internationellt vanligen på de skydd som omger det levererade informationssystemet, såsom den fysiska säkerheten, personalsäkerheten och skydden mot informationsläckage via diffus strålning. Baserat på dessa skydd utarbetas ett utlåtande om överensstämmelse med kraven och utlåtandet om godkännande ges vanligen av något av EU:s eller Natos organ.

Lagen om bedömningsorgan innehåller bestämmelser om intyg som beviljas av en bedömningsmyndighet för informationssäkerhet.

Till paragrafen fogas ett nytt *3 mom*. med bestämmelser om Transport- och kommunikationsverkets nya uppgift att meddela finländska tillverkare ett sådant förvaltningsbeslut om godkännandet av tillverkarens ansökan om bedömning av en säkerhetskritisk lösning och dess tillverkning som kan överklagas och av vilket resultatet av bedömningen framgår. Om den säkerhetskritiska lösningen uppfyller bedömningskraven, är beslutet ett beslut om godkännande för lösningen, av vilket giltighetstiden för godkännandet och de villkor som behövs för en säker användning av lösningen ska framgå. Godkännandet är i regel tillfälligt, eftersom den teknologiska utvecklingen och hotmiljöns utveckling kräver att lösningarna utvecklas tekniskt och bedöms tidvis. Användning av lösningarna vid skydd för säkerhetsklassificerade uppgifter kräver vanligen vissa slags val eller definitioner vid användningen av en lösning eller när det gäller dess driftsmiljö. Sådana villkor för val och definitioner som hänför sig till säker användning kan anges i beslutet eller till exempel i en bruksanvisning, det vill säga en användarpolicy, som ges i en bilaga till beslutet. Ett beslut om godkännande som gäller en tillverkare av en lösning för skydd mot informationsläckage via diffus strålning, det vill säga TEMPEST-utrustning, kan innehålla sådana villkor som behövs för att säkerställa att tillverkningen är tillförlitlig.

Om kraven för en säkerhetskritisk lösning eller dess tillverkning inte uppfylls, kan tillverkaren använda sig av den bedömningsrapport och det beslut som den fått vid utvecklingen och tillhandahållandet av lösningen.

8 a § *Förteckning över godkända säkerhetskritiska lösningar och tillverkare*. Paragrafen ändras så att den, i stället för att innehålla bestämmelser om myndigheternas skyldighet att skaffa intyg, föreskriver en ny uppgift för Transport- och kommunikationsverket som innebär att det ska föra och offentliggöra en förteckning över godkända säkerhetskritiska lösningar och tillverkare.

I paragrafen föreskrivs att Transport- och kommunikationsverket, när det godkänner en säkerhetskritisk lösning enligt den uppgift som föreskrivs i föreslagna 4 § 2 mom. 1 punkten och när det lämnar sådana beslut om godkännande som avses i föreslagna 8 § 3 mom. om

huruvida en säkerhetskritisk lösning och dess tillverkning överensstämmer med kraven, ska publicera uppgifter om lösningarna och dess tillverkare i en offentlig förteckning. Om det i ett beslut om överensstämmelse med kraven konstateras att den säkerhetskritiska lösning som bedömts inte uppfyller de fastställda kraven, publiceras inga uppgifter om beslutet. Syftet med förteckningen är att tillhandahålla information om utbudet för myndigheter och företag som behöver säkerhetskritiska lösningar. Förfarandet överensstämmer med de förteckningar som hänför sig till skydd av EU:s och Natos säkerhetsklassificerade uppgifter.

Dessutom innehåller paragrafen bestämmelser om de uppgifter som till tillämpliga delar åtminstone ska framgå av förteckningen, beroende på lösning eller tillverkare. Enligt *1 punkten* i paragrafen ska namnet på den säkerhetskritiska lösningen, dess användningsändamål och dess version framgå av förteckningen. Med användningsändamål avses till exempel produktens eller tjänstens typ eller tekniska användningsändamål som godkännandet gäller. Till exempel kan användningsändamålet för en krypteringslösning vara kryptering av material eller kryptering av datakommunikation.

Enligt *2 punkten* i paragrafen ska det av förteckningen framgå den säkerhetsklass för vilken lösningen har konstaterats ge ett tillräckligt skydd. I förteckningen anges uppgifter baserat på den nationella säkerhetsklassen och vid behov om bedömningar som gjorts av EU eller Nato baserat på säkerhetsklassen.

Enligt *3 punkten* i paragrafen ska tillverkaren av den säkerhetskritiska lösningen framgå av förteckningen. Om godkännandet gäller en tillverkare av TEMPEST-utrustning, kan uppgifter om tillverkaren och området för godkännande vara tillräckligt, och inga lösningar, produkter eller versioner behöver nödvändigtvis preciseras.

Enligt *4 punkten* i paragrafen ska godkännandets giltighet samt ändring eller upphörande av godkännandet framgå av förteckningen. Uppgifter om giltighet, ändringar eller upphörande är viktiga vid planering av upphandling av lösningar. Ändringar kan till exempel gälla höjande eller sänkande av säkerhetsklassen eller versionsändringar. Giltigheten kan upphöra på tillverkarens initiativ, om ingen fortsatt giltighet begärs. Giltigheten kan även upphöra genom ett beslut som Transport- och kommunikationsverket fattat enligt 10 §, om lösningen eller tillverkaren inte längre uppfyller kraven för godkännande.

Enligt *5 punkten* i paragrafen ska de villkor och begränsningar för en säker användning som hänför sig till godkännandet framgå av förteckningen. Med villkor för en säker användning avses till exempel en användarpolicy (*SecOps, det vill säga Security Operating Rules*) där det på ett tekniskt sätt redogörs för de användningssätt som krävs för det skydd som behövs för säkerhetsklassen. En användarpolicy eller anvisningar för en lösning kan vara sekretessbelagda, men förteckningen kan innehålla de offentliga uppgifter om dess existens som behövs. Ett godkännande kan också innebära tekniska begränsningar och avgränsningar, vilka det är lämpligt att ange i förteckningen.

8 b § *Införande av uppgifter i registret över säkerhetsutredningar och avförande av anteckning*. Det föreslås att paragrafen upphävs eftersom registret över säkerhetsutredningar endast har använts i liten utsträckning för det syfte som föreskrivs i paragrafen.

9 § *Upprätthållande och uppföljning av informationssäkerheten*. Paragrafen ändras så att den nuvarande bestämmelsen som innebär att den som fått ett intyg förbinder sig att upprätthålla informationssäkerhetsnivån ersätts med en skyldighet för den som fått ett beslut eller utlåtande ska upprätthålla informationssäkerheten i enlighet med utlåtandet eller beslutet. En anmälan om ändring som gäller informationssäkerheten ska göras till den bedömningsmyndighet som lämnat

beslutet eller gett utlåtandet. Tröskeln för anmälningar om ändring sänks från att vara ändringar som inverkar på informationssäkerhetsnivån till att vara ändringar som kan inverka på de krav som anges i beslutet eller utlåtandet.

Bestämmelser om bedömningsmyndighetens rätt att få information, utföra inspektioner och få tillträde till lokaler och system finns i 6 §.

10 § *Återkallande av beslut om godkännande eller utlåtande om godkännande.* Paragrafen och dess rubrik ändras så att de motsvarar den föreslagna ändringen av 8 § genom att paragrafens bestämmelser om återkallande av intyg ersätts med bestämmelser om återkallande av beslut om godkännande eller utlåtande om godkännande. Dessutom ersätts Kommunikationsverket med bedömningsmyndigheten, så att paragrafen gäller båda bedömningsmyndigheterna.

11 § *Ändringssökande*. Det föreslås att paragrafen ändras genom att Kommunikationsverket ersätts med bedömningsmyndigheten och hänvisningen till den upphävda förvaltningsprocesslagen (586/2966) ersätts med en hänvisning till den gällande lagen om rättegång i förvaltningsärenden (808/2019).

12 § *Avgifter*. Paragrafens ordalydelse och hänvisning till lagen om grunderna för avgifter till staten (150/1992) uppdateras, Kommunikationsverket ersätts med bedömningsmyndigheten och hänvisningen till intyg ersätts med en hänvisning till en bedömningsrapport, ett utlåtande eller ett beslut som avses i föreslagna 8 §. Dessutom fogas rådgivning av en bedömningsmyndighet till de avgiftsbelagda tjänsterna. Ändringen överensstämmer delvis med nuläget och är enhetlig med Transport- och kommunikationsverkets rådande avgiftsförordning.

7.2 Lag om bedömningsorgan för informationssäkerhet

1 § *Lagens syfte*. Paragrafen kompletteras så att lagens syfte, utöver de gällande bestämmelserna, är att utfärda bestämmelser om ett förfarande genom vilket myndigheter kan skaffa en oberoende bedömning av informationssäkerheten och beredskapen. Den föreslagna ändringen av paragrafen är enhetlig med föreslagna 3 § i bedömningslagen enligt vilken en bedömning som genomförts av ett godkänt bedömningsorgan för informationssäkerhet är ett av förfarandena för bedömning av informationssäkerheten i och beredskapen hos myndigheternas informationssystem och datakommunikation. Även till sin karaktär är den föreslagna ändringen av paragrafen förtydligande, i och med att myndigheterna redan med stöd av den gällande lagen har kunnat skaffa informationssäkerhetsbedömningar av godkända bedömningsorgan för informationssäkerhet.

2 § *Lagens tillämpningsområde.* Lagens tillämpningsområde preciseras och till *1 mom*. i paragrafen fogas, i enlighet med vad som enligt förslaget fogas till bedömningslagen, att bedömningsorgan för informationssäkerhet framöver har till uppgift att på uppdrag bedöma nivån på såväl informationssäkerheten i som beredskapen hos informationssystem eller datakommunikation. I 1 mom. i paragrafen beaktas dessutom den ämbetsverksreform som utförts inom transport- och kommunaktionsministeriets förvaltningsområde, varvid Kommunikationsverket upphörde att existera den 1 januari 2019 och Transport- och kommunikationsverket utgör den nya myndigheten för kommunikationsförvaltning.

Paragrafens *2 mom*. ändras så att det överensstämmer med de ändringar som föreslås för bedömningslagen. Paragrafens hänvisning till Kommunikationsverkets uppgifter som föreskrivs annanstans uppdateras till bedömningsmyndigheternas uppgifter som föreskrivs annanstans, och utöver bedömning av informationssäkerheten beaktas bedömning av beredskapen i momentet. Dessutom ändras momentets hänvisning till säkerhetsutredningar som

gäller sammanslutningar så att den överensstämmer med den nuvarande benämningen säkerhetsutredning som gäller företag.

3 § *Ansökan om godkännande av bedömningsorgan*. Paragrafens *1 mom*. förtydligas så att bedömningsorgan för informationssäkerhet kan ansöka hos Transport- och kommunikationsverket om godkännande både för sin verksamhet och för kompetensområdet för en bedömning. De kompetensområden som godkänts för ett bedömningsorgan för informationssäkerhet avgränsar vilka bedömningskriterier för informationssäkerhet och beredskap som verket kan använda vid sina bedömningsuppgifter. I samband med ansökan ska bedömningsorgan för informationssäkerhet ange vilket kompetensområde de ansöker om godkännande för. Ett godkänt bedömningsorgan för informationssäkerhet kan senare utvidga sitt verksamhetsfält och ansöka om godkännande för ytterligare kompetensområden. Möjligheten att ansöka om godkännande för ett nytt kompetensområde gäller sådana ytterligare kompetenser för godkända bedömningsorgan för informationssäkerhet som hänför sig till sådana kompetensområden som är förenliga med de bedömningsgrunder som föreskrivs i 10 § i lagen om bedömningsorgan och som organet inte ännu har. Enligt föreslagna 5 § 3 mim. krävs framöver inte längre alltid FINAS ackreditering för ytterligare kompetensområden. I stället krävs även framöver FINAS ackreditering för ett kompetensområde inom informationssäkerhet eller beredskap för att ett organ ska godkännas som bedömningsorgan för informationssäkerhet.

Dessutom ändras Kommunikationsverket i 1 mom. till Transport- och kommunikationsverket genom en teknisk ändring.

4 § *Behandlingen av ansökan.* Till *1 mom*. i paragrafen fogas säkerhetsutredning av företag som en ny metod för att utreda tillförlitligheten hos ett bedömningsorgan. En säkerhetsutredning av företag möjliggör utredning och uppföljning av ägarförhållandena för ett bedömningsorgan för informationssäkerhet samt säkerhetsutredningar och uppföljningar av oförvitligheten hos de ansvariga personerna. Säkerhetsutredningar av företag omfattar även lokaler och informationssystem som ägs av bedömningsorganet för informationssäkerhet, varvid deras säkerhet inte behöver granskas separat. Transport- och kommunikationsverket ska ansöka om säkerhetsutredning av företag när bedömningsorgan för informationssäkerhet ansöker om kompetens som gäller bedömning av hanteringen av säkerhetsklassificerade uppgifter. Inom tillämpningsområdet för bedömningslagen utgörs sådan kompetens till exempel av användning av auditeringsverktyget Katakri som en bedömningsgrund i enlighet med instruktionerna av den nationella säkerhetsmyndigheten. I och med att Transport- och kommunikationsverket utgör ansökare av utredningen får det information om skyddspolisens eventuella observationer, vars betydelse för godkännandet av bedömningsorganet verket kan bedöma. Förslaget är motiverat eftersom skyddspolisen kan utnyttja en noga lagstadgad och standardiserad process för att utreda tillförlitligheten hos ett bedömningsorgan.

I situationer där ett bedömningsorgan ansöker om kompetens som gäller hanteringen av något annat än säkerhetsklassificerade uppgifter kan ett utredningsförfarande i enlighet med den gällande lagen fortfarande användas, enligt vilket skyddspolisen reserveras tillfälle att uttala sig om de ansvariga personerna och lokalerna hos ett bedömningsorgan för informationssäkerhet. Till 1 mom. fogas dessutom ordet utredning, så att det även gäller säkerhetsutredningar av företag.

Utförandet av säkerhetsutredningar av företag vid godkännandet av sådana bedömningsorgan för informationssäkerhet som ansöker om kompetens för bedömning av skyddandet av säkerhetsklassificerade uppgifter gör utredningen och uppföljningen av tillförlitligheten hos bedömningsorgan för informationssäkerhet effektivare och tydligare. Förfarandet för godkännande förtydligas när det gäller Transport- och kommunikationsverket, skyddspolisen

och företag som ansöker om godkännande som bedömningsorgan. Ett intyg om säkerhetsutredning av företag bidrar till att öka myndighetskundernas förtroende för bedömningsorganen.

Dessutom ändras Kommunikationsverket i 1 mom. till Transport- och kommunikationsverket genom en teknisk ändring.

Verkets möjlighet enligt *2 mom*. i paragrafen att ge utomstående sakkunniga uppgifter som utförs på uppdrag ändras så att den endast gäller biträdande uppgifter. Det är fråga om samma slags biträdande bedömningsuppgifter som ges till utomstående sakkunniga som de som föreskrivs i 4 a § i bedömningslagen. Paragrafens innehåll preciseras också så att de utlåtanden som avses i den upprättas av myndigheter. Transport- och kommunikationsverket kan begära utlåtanden av såväl skyddspolisen som exempelvis sådana myndigheter som har styrnings- och övervakningsbehörigheter för den reglering som utgör den ansökta kompetensgrunden. En sådan myndighet är exempelvis Institutet för hälsa och välfärd när det är fråga om sådan bedömning av hanteringen av kunduppgifter enligt bestämmelser som institutet utfärdat som föreskrivs som en uppgift för ett godkänt bedömningsorgan för informationssäkerhet i lagen om behandling av kunduppgifter inom social- och hälsovården (703/2023). Till 2 mom. fogas dessutom straffrättsligt tjänsteansvar för dem som utför biträdande uppgifter och en hänvisning till skadeståndslagen (412/1974).

I 2 mom. i paragrafen ändras Kommunikationsverket till Transport- och kommunikationsverket genom en teknisk ändring.

5 § *Godkännande av bedömningsorgan.* Paragrafens *1 mom. 1–3 och 5 punkten* överensstämmer med den gällande regleringen. Till *4 punkten* i momentet fogas, som ett villkor för att ett bedömningsorgan för informationssäkerhet ska bedömas, att det i den säkerhetsutredning av företag som gäller organet inte har framkommit någon sådan omständighet som hänför sig till ägarförhållandena för bedömningsorganet, underentreprenader, den ekonomiska situationen eller säkerheten för personal, lokaler och informationssystem som utifrån en helhetsbedömning skulle äventyra företagets och dess ansvariga personers tillförlitlighet och förmåga att sköta sina åtaganden, med beaktande av även risken för utländsk påverkan vid bedömningsuppgifter som hänför sig till bedömning av hanteringen av myndigheters säkerhetsklassificerade uppgifter. Till 1 mom. 4 punkten fogas dessutom ett villkor som innebär att organet ska ha en övervakad metod som bedömts som tillförlitlig med vars hjälp tillförlitligheten hos personalen säkerställs. Bedömningsorganet ska ha processer och anvisningar för att sörja för personalsäkerheten. Med personalsäkerheten avses metoder för att säkerställa personers informationssäkerhetsansvar och skyldigheter, informationssäkerhetskunskaper och bakgrundskontroller samt förvaltning av risker som hänför sig till nyckelpersoner. Dessutom omfattar dessa förfaranden förhindrande av missbruk, såsom identifierande och undvikande av farliga arbetskombinationer, rotation av arbetsuppgifter och upphörande av anställningsförhållanden eller avtal. När ett bedömningsorgan för informationssäkerhet ansöker om sådan kompetens som gäller bedömning av hanteringen av säkerhetsklassificerade uppgifter, är bedömning av tillförlitligheten en uppgift enligt föreslagna 4 § genom att ansöka om en säkerhetsutredning av företag. Som en del av säkerhetsutredningen av företag säkerställs även säkerheten för organets lokaler och databehandling. I sådana situationer där ingen säkerhetsutredning av företag görs ska Transport- och kommunikationsverket på andra sätt försäkra sig om att villkoren uppfylls.

Paragrafens *2 mom.* överensstämmer med den gällande regleringen, det vill säga innehåller bestämmelser om att uppfyllandet av de krav som avses i 1 mom. 1–3 punkten ska visas genom det förfarande som föreskrivs i lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (920/2005).

Paragrafens *3 mom*. ändras så att det innehåller bestämmelser om Transport- och kommunikationsverkets möjlighet att, efter att ha hört de myndigheter som är centrala när det gäller godkännandet, fatta beslut om godkännande för ett nytt kompetensområde åt ett godkänt bedömningsorgan trots vad som föreskrivs i 2 mom. Enligt 2 mom. i den gällande paragrafen ska oberoendet och kompetensen hos ett bedömningsorgan för informationssäkerhet visas på det sätt som anges i lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven, det vill säga genom en ackreditering av den nationella ackrediteringsenheten FINAS. Syftet med ändrade 3 mom. är att möjliggöra godkännande av ytterligare kompetenser på ansökan av ett bedömningsorgan för informationssäkerhet genom Transport- och kommunikationsverkets beslut i stället för att FINAS ansvarar för att utreda villkoren för kompetensen genom ackreditering. Därmed ansvarar FINAS inte heller för uppföljningen av dessa ytterligare kompetenser eller att de är uppdaterade, utan det ansvarar Transport- och kommunikationsverkets styrnings- och övervakningsfunktion för i sin helhet.

De behov som bedömningsorgan för informationssäkerhet har av (ytterligare) kompetenser hänför sig ofta till säkerhetslösningar för myndigheters informationssystem, de bestämmelser som gäller dem och de myndighetsanvisningar och myndighetsförfaranden som gäller tillämpningen av bestämmelserna och som även har koppling till den internationella säkerheten. Det är i det närmaste en liten grupp behöriga myndighetsaktörer, såsom Transport- och kommunikationsverket eller vissa myndigheter som ansvarar för att informationssystem inom social- och hälsovården uppfyller kraven, som har den sakkunskap som krävs för dessa kompetensbehov. FINAS ackrediteringsprocess baserar sig på internationella ackrediteringsstandarder som tillämpas på olika slags marknadsaktörers kompetens när det gäller enhetliga och jämförbara bedömningar, men som inte stöder de särdrag hos den nationella informationssäkerhetsregleringen som beskrivs ovan. Beviljande av godkännande för ett bedömningsorgan för informationssäkerhet och bevarande av den statusen kräver även framöver en giltig ackreditering av FINAS för något kompetensområde inom informationssäkerhet som är tillräckligt allmänt, eftersom ackrediteringsförfarandet bidrar till att säkerställa förmågan hos bedömningsorganet för informationssäkerhet att konsekvent iaktta de verksamhetsprocesser som tryggar enhetligheten och jämförbarheten. Därmed är det även framöver motiverat att vid godkännandet av ett bedömningsorgan för informationssäkerhet kräva exempelvis ackreditering för en kompetens i enlighet med den allmänna standardserien för informationssäkerhet, ISO/IEC 27000. Dock krävs ackrediteringsförfarandet alltså inte nödvändigtvis när ett redan godkänt bedömningsorgan för informationssäkerhet ansöker om ett nytt kompetensområde enligt de bedömningsgrunder som föreskrivs i 10 § i lagen. Även i EU-regleringen erkänns ett godkännande av kompetens som gjorts av en behörig myndighet i stället för ackreditering av en ackrediteringsenhet. Exempelvis i artikel 42 i cyberresiliensförordningen (EU) 2024/2847 (s.k. CRA) finns bestämmelser om ett sådant alternativ.

Vid övervägandet av godkännandeförfarandet för ytterligare kompetenser och utredandet av kompetenser ska Transport- och kommunikationsverket höra sådana myndigheter som är centrala för godkännandet. Beroende på fallet är dessa exempelvis FINAS för eventuellt tillämpliga standarder och de myndigheter som har sådana myndighetsuppgifter som den ansökta kompetensgrunden hänför sig till. Det föreslagna hörandet av centrala myndigheter baserar sig på det bistående av en annan myndighet som anges i 10 § i förvaltningslagen. Genom hörande och andra utredningar som behövs ska Transport- och kommunikationsverket säkerställa den ytterligare kompetensen och att uppfyllandet av kraven i 1 mom. 1–3 punkten inte äventyras när det gäller den ytterligare kompetensen. Enligt jämlikhetskravet för god förvaltning ska Transport- och kommunikationsverket säkerställa jämlik behandling av de ansökande. Därmed ska grunderna och förfarandet för beviljande av ytterligare kompetensområden vara de samma för alla ansökande. Syftet med det nya förfarandet är också att göra processen för godkännande av nya kompetensområden enklare och smidigare och

minska de kostnader och den administrativa börda som de innebär för bedömningsorganen för informationssäkerhet.

Paragrafens *4 mom*. överensstämmer med 3 mom. i den gällande lagen med den skillnaden att en teknisk ändring görs i momentet, vilket innebär att Kommunikationsverket uppdateras till Transport- och kommunikationsverket.

Till paragrafen fogas ett nytt *5 mom*. som överensstämmer med 4 mom. i den gällande lagen. Momentet innehåller alltså bestämmelser om att ett godkännande är tillfälligt och om villkoren för godkännande.

6 § *Återkallelse av godkännande av bedömningsorgan.* Paragrafens *1 mom*. ändras så att Transport- och kommunikationsverket har möjlighet att återkalla både hela godkännandet av ett bedömningsorgan och ett enskilt kompetensområde som godkänts för bedömningsorganet för informationssäkerhet. Försummelser och brister i verksamheten för ett bedömningsorgan för informationssäkerhet kan hänföra sig till det allmänna agerandet som bedömningsorgan för informationssäkerhet eller bara bedömningar inom ett visst kompetensområde, varför en återkallelse av godkännande vid behov ska kunna avgränsas till endast en del av bedömningsorganets verksamhet, exempelvis ett enskilt godkänt kompetensområde. En återkallelse av godkännandet för ett kompetensområde gör det möjligt att ingripa i verksamheten endast till den del som det behövs. Återkallelse av ett enskilt kompetensområde innebär att bedömningsorganet kan fortsätta sin bedömningsverksamhet inom de kompetensområden i vilka inga problem eller brister har observerats. Beslut om återkallelse av godkännande för ett kompetensområde fattas av Transport- och kommunikationsverket.

I 1 mom. i paragrafen görs dessutom en teknisk ändring som innebär att Kommunikationsverket uppdateras till Transport- och kommunikationsverket.

I *2 mom.* i paragrafen görs samma tekniska ändring som i 1 mom., det vill säga Kommunikationsverket uppdateras till Transport- och kommunikationsverket.

7 § *Transport- och kommunikationsverkets rätt att få information samt inspektionsrätt.* Paragrafens rubrik ändras så att Kommunikationsverket ändras till Transport- och kommunikationsverket och ett omnämnande om Transport- och kommunikationsverkets rätt att få information tillfogas.

Paragrafens *1 mom*. ändras så att den inspektionsrätt som föreskrivs i paragrafen utvidgas till att även omfatta lokalerna hos en underleverantör till ett bedömningsorgan för informationssäkerhet, och utöver Transport- och kommunikationsverket gäller detta de sakkunniga som biträder verket, i stället för de sakkunniga som handlar på uppdrag av verket. Dessutom preciseras paragrafens ordalydelse så att en sakkunnig kan biträda Transport- och kommunikationsverket i utförandet av inspektioner, men inspektionsrätten föreskrivs tillfalla Transport- och kommunikationsverket. Ändringen överensstämmer med den möjlighet att ge endast biträdande uppgifter till utomstående sakkunniga som föreslås för 4 § 2 mom. En utomstående expert som utför en biträdande uppgift kan användas för sådana inspektioner som gäller lokaler och metoder som används av ett bedömningsorgan för informationssäkerhet och dess underleverantör som avses i 9 a §. Dessutom görs en teknisk ändring i momentet vilken innebär att Kommunikationsverket uppdateras till Transport- och kommunikationsverket.

Till paragrafen fogas ett nytt *2 mom*. med bestämmelser om Transport- och kommunikationsverkets rätt att få information, om vilken det föreskrivs tidigare i 8 § 2 mom. i den gällande lagen. Transport- och kommunikationsverkets behörigheter kompletteras så att

Transport- och kommunikationsverket framöver har möjlighet att, trots sekretessbestämmelser eller andra begränsningar som gäller utlämnande av uppgifter, på begäran få de uppgifter som är nödvändiga för tillsynen över att ett bedömningsorgan för informationssäkerhet uppfyller de krav som ställs på dess verksamhet. Rätten att få information gäller sådana uppgifter som överlåts av skyddspolisen, den nationella ackrediteringsenheten, den myndighet som styr eller övervakar tillämpningen av bedömningsgrunden för kompetensområdet, bedömningsorganet samt dess underleverantörer och kunder och som kan vara sekretessbelagda exempelvis i form av företagshemligheter eller uppgifter om säkerhetsarrangemang eller beredskapen för myndigheter som utgör bedömningsorganets kunder.

8 § *Bedömningsorganens anmälningsskyldighet.* Omnämnandet av bedömningsorganens upplysningsskyldighet stryks ur paragrafens rubrik.

Paragrafen ändras så att den framöver endast innehåller ett moment som överensstämmer med 1 mom. i den gällande lagen, med den tekniska ändringen att Kommunikationsverket ändras till Transport- och kommunikationsverket.

De bestämmelser om Transport- och kommunikationsverket som finns i 2 mom. i den nuvarande paragrafen finns framöver i 7 § 2 mom. i lagen.

Rubriken på 3 kap. ändras så att den även omfattar beredskap. Framöver är rubriken Bedömning av informationssäkerhet och beredskap.

9 § *Bedömningsorganens uppgifter.* Till *1 mom*. i paragrafen fogas, i enlighet med de föreslagna ändringarna i bedömningslagen, en uppgift att bedöma beredskapen. Dessutom ändras 1 mom. 1 punkten så att lokalerna ska inspekteras i situationer där det behövs. Inspektion av lokalerna är inte en bestämd del av varje bedömning. Den som begär en bedömning kan ha en utredning av säkerheten i lokalerna sedan tidigare som utförts av ett bedömningsorgan eller en myndighet. Den som begär en bedömning kan också ha ett annat skäl till att inte begära en bedömning av lokalerna. Framöver antas användningen av olika slags molnteknik och tjänster som tillhandahålls genom andra datanät öka, och det är inte i praktiken möjligt att i alla situationer inspektera lokalernas säkerhet i samma omfattning. Det är dock viktigt att bedömningsorganen sörjer för att eventuella begränsningar i omfattningen för en inspektion framgår tydligt av bedömningsrapporten eller intyget.

Paragrafens *3 mom*. ändras så att det gäller utarbetandet av en bedömningsrapport i stället för ett intyg. Ett godkänt bedömningsorgan för informationssäkerhet ska utarbeta en bedömningsrapport om alla bedömningar som den utför och av rapporten ska det framgå uppgifter om bedömningsobjektet, vilka bedömningsgrunder som använts, bedömningens omfattning, det vill säga exempelvis tekniska begränsningar eller uppgifter om verifieringsförfaranden, och de observationer som gjorts. En bedömningsrapport kan även innehålla bedömningsorganets analys av de risker som de observerade avvikelserna kan innebära. Den föreslagna ändringen överensstämmer med den föreslagna ändringen i bedömningslagen, men bestämmelser om kraven på förfarandena för bedömningsorganens verksamhet finns även i detta fall i lagen om bedömningsorgan.

Till paragrafen fogas ett nytt *4 mom*. som motsvarar 3 mom. i den gällande paragrafen med den skillnaden att ett godkänt bedömningsorgan för informationssäkerhet framöver kan utfärda intyg på begäran eller om det särskilt föreskrivs om det. Speciallagstiftning om intyg som utfärdats av ett godkänt bedömningsorgan för informationssäkerhet finns till exempel i regleringen av social- och hälsovårdssektorn. Om det inte finns någon speciallagstiftning om ett intyg kan den som begär en bedömning besluta om den ska begära både en bedömningsrapport

och ett intyg. Ett intyg kan behöva begäras till exempel om den som begär bedömningen behöver kunna bevisa för en utomstående att dess verksamhet är informationssäker. Det nya 4 mom. skiljer sig från det gällande 3 mom. även på så sätt att det framöver hänvisas till lokalerna och verksamheten för bedömningsobjektet genom uttrycket bedömningsobjektet. Syftet med ändringen är att se till att förutsättningarna för utfärdande av intyg överensstämmer med den föreslagna ändringen i 1 mom. i paragrafen. Dessutom preciseras listan över innehållet i sådana intyg och giltighetstiden av intyget ska framöver framgå av intyget. En tredje part som förlitar sig på ett intyg på basis av giltighetstiden för intyget kan bedöma hur länge den information som fåtts genom bedömningen är tillförlitlig.

9 a § *Underleverantörer.* Till lagen fogas en ny 9 a § med bestämmelser om ramvillkoren för underleverantörer. Paragrafen förtydligar villkoren för verksamheten för ett godkänt bedömningsorgan för informationssäkerhet, gör regleringen lättare att förutse och minskar därmed tolkningsfrågor som hänför sig till planering av verksamheten samt främjar kundernas förtroende för organens verksamhet.

I *1 mom*. i paragrafens föreskrivs att ett godkänt bedömningsorgan för informationssäkerhet får lägga ut en uppgift i anslutning till bedömningen på underentreprenad till ett annat bolag som hör till samma koncern eller till någon annan underleverantör endast om koncernbolaget eller underleverantören uppfyller förutsättningarna för godkännande av ett bedömningsorgan för informationssäkerhet. Med utläggande på underentreprenad avses användning av ett dotter-, syster- eller moderbolag som tillhör koncernen eller någon annan underleverantör. I 1 mom. föreskrivs dessutom att en utredning om underentreprenaden ska lämnas till Transport- och kommunikationsverket baserat på vilken verket bedömer huruvida förutsättningarna uppfylls.

Endast sådana funktioner som ett godkänt bedömningsorgan för informationssäkerhet själv har kompetens att utföra kan läggas ut på underentreprenad, och organet ska kunna kontrollera underleverantörens verksamhet i alla skeden. Det godkända bedömningsorganet för informationssäkerhet har fortfarande det fulla ansvaret för sina funktioner i situationer där utomstående aktörer används för vissa uppgifter.

Paragrafens *2 mom*. innehåller bestämmelser om underleverantörernas villkor när det gäller uppgifter som hänför sig till bedömning av hanteringen av säkerhetsklassificerad information. Enligt förslaget är det möjligt att lägga ut sådana uppgifter på underentreprenad eller låta dem utföras av ett dotterbolag endast om det avtalas om det med kunden separat. Avtals- och informationsskyldighet när det gäller underleverantörer vid bedömning av hanteringen av säkerhetsklassificerad information gör bedömningsorganets verksamhet mer transparent för kundmyndigheter och företag.

10 § *Bedömningsgrunder för informationssäkerhet och beredskap*. Till paragrafens rubrik fogas beredskap i enlighet med den föreslagna ändringen av tillämpningsområdet. De bedömningsgrunder för informationssäkerhet och beredskap som föreskrivs i paragrafen ändras så att de är förenliga med de föreslagna ändringarna i 7 § i bedömningslagen.

Till den inledande meningen i *1 mom*. i paragrafen fogas ett omnämnande av att de bedömningsgrunder som används för valet av bedömningsobjekt, det vill säga begäran, beror på vilka bedömningsgrunder som har godkänts som kompetensområden för bedömningsorganet för informationssäkerhet.

Momentets *1 punkt* ändras så att i lag eller förordning föreskrivna krav på informationssäkerhet, cybersäkerhet eller beredskap som gäller myndigheternas verksamhet samt myndigheternas anvisningar om tillämpningen av kraven kan användas som bedömningsgrund.

I enlighet med det som föreslås för bedömningslagen föreslås att bestämmelserna om myndigheternas anvisningar tillämpas allmänt i stället för att anvisningar nämns för specifika myndigheter, såsom finansministeriet och den nationella säkerhetsmyndigheten. Detta är en tillräcklig och allmängiltigare definition. Därmed ingår nuvarande 1 mom. 2 punkten i den ändrade 1 punkten.

Momentets *2 punkt* motsvarar den nuvarande 3 punkten, men i och med Finlands medlemskap i Nato tillfogas Nordatlantiska fördragsorganisationen som ett eventuellt organ som utfärdar bestämmelser, föreskrifter eller anvisningar. Till punkten fogas också myndigheternas anvisningar om tillämpningen av internationellt organs bestämmelser och anvisningar. I likhet med 1 mom. innehåller även 2 punkten såväl informationssäkerhet som cybersäkerhet och beredskap. Trots att bestämmelser utfärdas om internationella källor i form av bedömningsgrunder, inverkar regleringen av de internationella förpliktelserna som gäller informationssäkerhet på möjligheten för bedömningsorgan för informationssäkerhet att få sådan kompetens som hänför sig till förpliktelserna för informationssäkerhet för bedömning av hanteringen av säkerhetsklassificerade uppgifter.

Momentets *3 punkt* överensstämmer med den nuvarande 4 punkten och momentets *4 punkt* överensstämmer med den nuvarande 5 punkten, med den skillnaden att båda punkterna omfattar såväl bestämmelser, föreskrifter och anvisningar om informationssäkerhet som bestämmelser, föreskrifter och anvisningar om samt krav om beredskap och cybersäkerhet.

11 § *Avgifter*. Paragrafens ordalydelse och hänvisning till lagen om grunderna för avgifter till staten (150/1992) uppdateras i enlighet med det som föreslås för bedömningslagen. Dessutom ändras paragrafen så att Transport- och kommunikationsverket har möjlighet att ta ut en avgift för behandlingen av ärenden som gäller tillsyn över bedömningsorgan för informationssäkerhet. Ändringen överensstämmer delvis med nuläget och är enhetlig med Transport- och kommunikationsverkets rådande avgiftsförordning. I paragrafen görs dessutom en teknisk ändring som innebär att Kommunikationsverket ändras till Transport- och kommunikationsverket.

12 § *Ändringssökande*. Paragrafens hänvisning till den upphävda förvaltningsprocesslag (586/1996) stryks och till paragrafen fogas en hänvisning till lagen om rättegång i förvaltningsärenden (808/2019). I paragrafen görs dessutom en teknisk ändring som innebär att Kommunikationsverket ändras till Transport- och kommunikationsverket.

13 § *Tillämpning av bestämmelser om tjänsteansvar och god förvaltning*. Paragrafens rubrik kompletteras så att den även innehåller ett omnämnande av tillämpningen av bestämmelser om tjänsteansvar.

Listan över de allmänna lagarna om förvaltning som tillämpas kompletteras i *1 mom*. i paragrafen, och till momentet fogas en hänvisning till samiska språklagen (1086/2003), dataskyddslagen (1050/2018) och lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003). Tillämpningen av de allmänna lagarna om förvaltning binds till skötseln av offentliga förvaltningsuppgifter som utförs av bedömningsorgan för informationssäkerhet. Offentliga förvaltningsuppgifter är sådana uppgifter för godkända bedömningsorgan för informationssäkerhet som föreskrivs i lagen om bedömningsorgan. Uppgifterna är likställda med de bedömningsuppgifter för bedömningsmyndigheter som föreskrivs i bedömningslagen. Dessutom innehåller exempelvis kunduppgiftslagen och lagen om sekundär användning bestämmelser om de krav som innebär att en bedömning som utförts av eller ett intyg som utfärdats av ett bedömningsorgan för informationssäkerhet behövs för aktörerna. Utförandet av en sådan bedömning eller utfärdandet av ett sådant intyg kan anses innebära utövning av

offentlig makt. Vid utövning som utförs av bedömningsorgan för informationssäkerhet tillämpas inte de allmänna lagarna om förvaltning på annat än sådan verksamhet som är förenlig med lagen om bedömningsorgan.

Till paragrafen fogas ett nytt *2 mom*. med bestämmelser om tjänsteansvaret för ansvarspersoner och personer som är anställda vid ett bedömningsorgan för informationssäkerhet samt personer som är anställda hos underleverantörer. Det straffrättsliga tjänsteansvaret baserar sig på att den verksamhet för ett godkänt bedömningsorgan för informationssäkerhet som är förenlig med lagen om bedömningsorgan anses vara en offentlig förvaltningsuppgift. Till slutet av 2 mom. fogas dessutom en informativ bestämmelse om att bestämmelser om skadeståndsansvar finns i skadeståndslagen.

13 a § *Registrering av uppgifter i registret över säkerhetsutredningar* I paragrafen görs tekniska ändringar som innebär att Kommunikationsverket ändras till Transport- och kommunikationsverket och termen godkända bedömningsorgan för informationssäkerhet används i paragrafen i stället för godkända bedömningsorgan.

7.3 Säkerhetsutredningslagen

18 § *Överensstämmelse med säkerhetskraven som en allmän förutsättning.* Det föreslås att paragrafens *2 mom*. ska ändras så att dess hänvisning till ett intyg i enlighet med bedömningslagen ändras enligt förslaget för 8 § i bedömningslagen så att paragrafen gäller ett beslut eller utlåtanden i enlighet med bedömningslagen.

48 § *Registret över säkerhetsutredningar och registrets ändamål samt registrering av uppgifter*. Det föreslås att paragrafen ändras så att 4 mom. 1 punkten stryks. Ändringen behövs eftersom det föreslås att 8 b § i bedömningslagen stryks.

8 Bestämmelser på lägre nivå än lag

I propositionen föreslås att 8 a § i bedömningslagen ändras så att paragrafen framöver ska innehålla bestämmelser om förteckningen över godkända säkerhetskritiska lösningar och tillverkare. I bedömningslagens gällande 8 a § föreskrivs en möjlighet att genom förordning av statsrådet föreskriva att ett intyg ska skaffas i fråga om informationssystem eller datakommunikation som en statsförvaltningsmyndighet bestämmer över och där handlingar som hör till säkerhetsklass I eller II behandlas. Det föreslås att detta bemyndigande att utfärda förordning ska utgå när paragrafen ändras. Bemyndigandet att utfärda förordning har inte använts under dess giltighetstid.

9 Ikraftträdande

Lagarna föreslås träda i kraft under hösten 2026.

Ändringarna av bedömningslagen innehåller övergångsbestämmelser, eftersom alla myndigheter inte har beredskap eller möjlighet att omedelbart när lagen träder ikraft tillämpa den nya lagen och iaktta dess bestämmelser. Myndigheterna använder ett stort antal informationssystem och datakommunikation som har införts vid olika tidpunkter, och det beräknas ta flera år att anpassa deras förfaranden för bedömning av informationssäkerhet och beredskap till de föreslagna nya bedömningsskyldigheterna på grund av systemens komplexitet. Dessutom råder det osäkerhet om tillgången på erforderliga bedömningar på grund av de nuvarande knappa finansiella resurserna och bedömningsresurserna.

I bedömningslagen föreslås en övergångsperiod då statsförvaltningsmyndigheterna inom fem år ska bedöma sina informationssystem och sin datakommunikation i enlighet med de föreslagna nya skyldigheterna som föreskrivs i 3 a § i bedömningslagen, dock så att bedömningen av system som behandlar uppgifter som hör till säkerhetsklass I och II ska begäras av bedömningsmyndigheten inom två år från ikraftträdandet av lagen, och bedömningen av system som behandlar uppgifter som hör till säkerhetsklass III ska begäras av bedömningsmyndigheten eller skaffas av ett bedömningsorgan inom tre år från ikraftträdandet, om inte myndigheten på basis av en riskbedömning anser det onödigt. Även andra än statsförvaltningsmyndigheterna bör bedöma informationssäkerheten i och beredskapen hos sina informationssystem och sin datakommunikation som behandlar uppgifter som hör till säkerhetsklass I, II och III inom samma tidsgränser som statsförvaltningsmyndigheterna, dvs. system som behandlar uppgifter som hör till säkerhetsklass I och II inom två år och system som behandlar uppgifter som hör till säkerhetsklass III inom tre år från lagens ikraftträdande.

Ett intyg över överensstämmelse med kraven på informationssäkerhet som har utfärdats i enlighet med gällande bedömningslag anses motsvara det i 8 § i bedömningslagen föreslagna beslutet eller utlåtandet om kravöverensstämmelse och är giltigt under den tid som anges i intyget. Om det för ett informationssystem eller för datakommunikation finns ett giltigt intyg om överensstämmelse med informationssäkerhetskraven behöver systemet följaktligen inte omprövas när den föreslagna lagstiftningen träder i kraft. Systemets informationssäkerhet bör upprätthållas i enlighet med vad som föreslås i 9 § i bedömningslagen.

I ändringarna av lagen om bedömningsorgan ingår en övergångsbestämmelse, eftersom bedömningsorgan som vid tidpunkten för lagens ikraftträdande är godkända kan ha giltiga kompetensområden som godkänts för bedömning av hanteringen av säkerhetsklassificerad information, såsom Katakri kompetensområden för säkerhetsklass IV och säkerhetsklass III. Förutsättningen för godkännande av dessa kompetensområden är enligt föreslagna 4 § och 5 § 1 mom. 4 punkten i lagen om bedömningsorgan en säkerhetsutredning av företag där det inte har framkommit någon sådan omständighet som utifrån en helhetsbedömning skulle äventyra företagets och dess ansvarspersoners tillförlitlighet och förmåga att sköta sina åtaganden i fråga om bedömningsuppgiften. Enligt föreslagna 4 § i lagen om bedömningsorgan ska Transport- och kommunikationsverket ansöka om säkerhetsutredningar av företagen i fråga. När de föreslagna ändringarna träder i kraft kan bedömningsorganen för informationssäkerhet inte genast uppfylla de nya kraven för godkännande av bedömningskompetens för hantering av säkerhetsklassificerad information.

En övergångsperiod föreslås i lagen om bedömningsorgan så att lagens krav i 4 § och 5 § 1 mom. 4 punkten i fråga om säkerhetsutredningar av företag omfattas av en övergångsperiod på två år. Transport- och kommunikationsverket ska enligt 4 § i lagen om bedömningsorgan ansöka om säkerhetsutredning av företag för de godkända bedömningsorgan för informationssäkerhet som före ikraftträdandet av den föreslagna ändringen har godkänts för kompetensområdet för bedömning av hantering av säkerhetsklassificerad information, senast inom två år från lagens ikraftträdande. Transport- och kommunikationsverket bör beakta bedömningsorganens önskemål om tidpunkten för ansökan om sådana utredningar. Om ett godkänt bedömningsorgan efter lagens ikraftträdande ansöker om en ny kompetens för bedömning av hantering av säkerhetsklassificerad information, ska en ansökan om säkerhetsutredning av företag göras i samband med behandlingen.

10 Förhållande till grundlagen samt lagstiftningsordning

Propositionen innehåller förslag som är betydelsefulla med avseende på skyddet för privatlivet, personuppgifter och meddelandehemligheten som tryggas i 10 §, skyddet av egendom som

tryggas i 15 §, näringsfriheten som tryggas i 18 § och överföringen av förvaltningsuppgifter på andra än myndigheter som föreskrivs i 124 § i grundlagen. Dessutom har propositionen bedömts med avseende på dess organisatoriska tillämpningsområde.

Offentlig förvaltningsuppgift

I propositionen föreslås bestämmelser i 4 a § i bedömningslagen om uppgifter för att bistå bedömningsverksamheten och i 4 § 2 mom. i lagen om bedömningsorgan om biträdande uppgifter i anknytning till Transport- och kommunikationsverkets bedömning av ansökningar från bedömningsorgan för informationssäkerhet. Förslagen är betydelsefulla med tanke på grundlagens 124 §, enligt vilken offentliga förvaltningsuppgifter kan anförtros andra än myndigheter endast genom lag eller med stöd av lag, om det behövs för en ändamålsenlig skötsel av uppgifterna och det inte äventyrar de grundläggande fri- och rättigheterna, rättssäkerheten eller andra krav på god förvaltning. Uppgifter som innebär betydande utövning av offentlig makt får dock bara ges till myndigheter. Utgångspunkten för de bedömningar som bedömningsmyndigheter gör i enlighet med bedömningslagen är dock att de själva utför bedömningen. Bedömningen får inte heller med stöd av 4 a § i sin helhet överlåtas på utomstående sakkunniga, utan ansvaret för att utföra bedömningen kvarstår hos bedömningsmyndigheten även om den beslutar anlita utomstående sakkunniga som hjälp. Detsamma gäller för förslaget i 4 § 2 mom. i lagen om bedömningsorgan, där utgångspunkten är att Transport- och kommunikationsverket ansvarar för handläggningen av ansökningar.

I sin utlåtandepraxis har grundlagsutskottet konstaterat att det kan vara lämpligt att inspektioner på grund av särskilda yrkesmässiga och tekniska aspekter på de omständigheter som tillsynen gäller utförs av sakkunniga som myndigheterna befullmäktigat därtill (GrUU 40/2002 rd, s. 3, GrUU 44/2016 rd, s. 5). Nödvändighetskravet kan bli uppfyllt exempelvis i fall där granskningen förutsätter kompetens eller resurser som saknas hos myndigheterna (GrUU 29/2013 rd, s. 2/I). Enligt föreslagna 4 a § i bedömningslagen kan utomstående sakkunniga anlitas, om det är nödvändigt på grund av bedömningens art, de tillgängliga resurserna eller tekniska skäl som hänför sig till bedömningen. Enligt föreslagna 4 a § 2 mom. i bedömningslagen läggs bedömningsuppgifterna i praktiken ut på Teknologiska forskningscentralen VTT Ab när bedömningen kräver sådan teknisk specialkompetens och resurser som bedömningsmyndigheten inte har möjlighet eller det inte är ändamålsenligt att tillhandahålla.

Grundlagsutskottet har ansett att respekten för de grundläggande fri- och rättigheterna, rättssäkerheten och kraven på god förvaltning kan tryggas genom att de som utför tillsynen är lämpliga och kompetenta för uppgiften (GrUU 5/2006 rd, s. 8/I, GrUU 67/2002 rd, s.5/I–II och GrUU 2/2002 rd, s. 2/II). Enligt föreslagna 4 a § i bedömningslagen ska de utomstående sakkunniga ha den utbildning som uppgiften kräver.

Grundlagsutskottet har i fråga om respekten för de grundläggande fri- och rättigheterna, kraven på rättssäkerhet och god förvaltning vidare ansett att de allmänna förvaltningslagarna ska iakttas när inspektionerna utförs och att de som handlägger ärenden handlar under tjänsteansvar (GrUU 20/2006 rd, s. 2, GrUU 46/2002 rd, s. 9, GrUU 33/2004 rd, s. 7/II, GrUU 11/2006 rd, s. 3). Enligt föreslagna 4 a § i bedömningslagen och 4 § 2 mom. i lagen om bedömningsorgan tillämpas på utomstående sakkunniga och på anställda vid Teknologiska forskningscentralen VTT Ab bestämmelserna om straffrättsligt tjänsteansvar när de sköter uppgifter enligt dessa paragrafer. Det är numera inte längre nödvändigt att med anledning av 124 § i grundlagen ta in en hänvisning till de allmänna förvaltningslagarna i lagen, om det av förslaget klart framgår att de allmänna förvaltningslagarna tillämpas på verksamhet som avses i 124 § i grundlagen (GrUU 20/2006 rd, s. 2). Om en sådan reglering för tydlighetens skull emellertid anses behövlig, måste

hänvisningen vara omfattande för att e contrario-tolkning ska undvikas (GrUU 42/2005 rd, s. 3). Det föreslås att hänvisningen till de allmänna förvaltningslagarna i 13 § i lagen om bedömningsorgan hålls kvar och kompletteras så att förteckningen blir heltäckande. I propositionen preciseras också att uppgifterna för bedömningsorganen för informationssäkerhet enligt lagen om bedömningsorgan är offentliga förvaltningsuppgifter vars skötsel omfattas av de allmänna förvaltningslagarna. Syftet är att förtydliga den utgångspunkt som omfattades i samband med antagandet av den nuvarande lagen om bedömningsorgan (RP 45/2011 rd s. 10), och som i praktiken har visat sig vara oklar, om att tillämpningen av de allmänna förvaltningslagarna inte ska vara bunden till skötsel av en offentlig förvaltningsuppgift, utan ska tillämpas på skötseln av alla uppgifter som är förenliga med lagen om bedömningsorgan.

Enligt föreslagna 9 a § får ett godkänt bedömningsorgan för informationssäkerhet lägga ut en uppgift som hör till bedömningsorganet på en underleverantör. I sin praxis har grundlagsutskottet i princip förhållit sig avvisande till att en offentlig förvaltningsuppgift som överförts till en enskild delegeras vidare (subdelegering). Det har dock inte funnits grunder för något absolut förbud i situationer där uppgiften har varit av teknisk art och underleverantören har berörts av samma kvalitetskrav och motsvarande tillsyn som den primära serviceproducenten (GrUU 26/2017 rd, s. 51, GrUU 6/2013 rd, s. 4). Enligt den föreslagna regleringen är ett godkänt bedömningsorgan för informationssäkerhet skyldigt att lämna en utredning om underentreprenader till Transport- och kommunikationsverket som övervakar att underleverantören i tillämpliga delar uppfyller de i lagen fastställda förutsättningarna för godkännande av ett bedömningsorgan. Ett godkänt bedömningsorgan för informationssäkerhet är också juridiskt ansvarigt för arbeten som organet har lagt ut på en underleverantör och bär helhetsansvaret i förhållande till kunden. Anlitandet av underleverantörer i samband med den föreslagna lagen anses följaktligen inte utgöra sådan subdelegering som är problematisk med avseende på 124 § i grundlagen, eftersom det är fråga om uppgifter av teknisk karaktär och samma krav gäller för underleverantörer som för godkända bedömningsorgan för informationssäkerhet.

Näringsfrihet

Propositionen innehåller förslag som är betydelsefulla med avseende på näringsfriheten enligt 18 § 1 mom. i grundlagen. Genom näringsfriheten tryggas var och en i enlighet med lag rätt att skaffa sig sin försörjning genom arbete, yrke eller näring som han eller hon valt fritt. Bestämmelsen möjliggör begränsningar av företagsfriheten, men förutsätter att sådana begränsningar genomförs på lagnivå. En sådan reglering måste också uppfylla övriga allmänna krav på en lag som begränsar de grundläggande fri- och rättigheterna. Begränsningar i näringsfriheten bör vara exakta och noggrant avgränsade och deras omfattning och villkor ska framgå av lagen (GrUU 16/2003 rd, s. 2/I)

I 3 a § i bedömningslagen föreslås förnyade bedömningsförfaranden där det till förfarandena läggs till myndigheters självbedömningar och bedömningar som en tjänsteleverantör utför på uppdrag av en myndighet, utöver de bedömningsförfaranden som anges i nuvarande lag, dvs. bedömningar som utförs av ett bedömningsorgan för informationssäkerhet och av en bedömningsmyndighet. Syftet med propositionen är att göra bedömningarna smidigare och förbättra tillgången på dem genom att till vissa delar öppna bedömningsverksamheten också för privata tjänsteleverantörer. För tjänsteleverantörer som arbetar på uppdrag av en myndighet är regleringen betydelsefull också med tanke på näringsfriheten enligt 18 § 1 mom. i grundlagen. Den föreslagna ändringen av bedömningslagen öppnar upp för nya affärsmöjligheter för företag som erbjuder utvärderingstjänster. Å andra sidan är förslaget att tjänsteleverantörernas bedömningar ska begränsas till informationssystem där det behandlas uppgifter som är offentliga, sekretessbelagda eller som hör till högst säkerhetsklass IV. Begränsningen är baserad

på att hanteringen av säkerhetsklassificerad information är förenad med strängare krav på datasekretess, mer begränsade åtkomsträttigheter samt större risker om informationen obehörigen röjs. Tjänsteleverantörer kan dessutom ansöka om att bli bedömningsorgan för informationssäkerhet om de vill bedöma informationssystem och datakommunikation som hanterar information som hör till säkerhetsklass III. Förslaget anses inte vara problematiskt med tanke på näringsfriheten, eftersom det på lagnivå ska föreskrivas noggrant avgränsade bestämmelser om förutsättningarna för att tillåta tjänsteleverantörers bedömningar med syftet att skydda säkerhetsklassificerad information.

Propositionen innehåller även ett förslag om att begränsa de bedömningar som bedömningsorganen för informationssäkerhet utför till informationssystem och datakommunikation som hanterar uppgifter högst i säkerhetsklass III. Det handlar om att lagstifta om det gällande förfarandet, eftersom dessa bedömningsorgan inte har beviljats kompetens för bedömning av hantering av säkerhetsklassificerad information som klassificerats högre än säkerhetsklass III. Detta motiveras av den särskilt höga och betydande risknivån hos informationssystem och datakommunikation som hanterar information klassificerad i säkerhetsklass I och II samt av den särskilda kompetens som bedömningsmyndigheten har om de funktionella kraven, verksamhetsmiljön och säkerhetsarrangemangen för informationssystem och datakommunikation som hanterar information klassificerad i säkerhetsklass I och II. Förslaget anses inte vara problematiskt med tanke på näringsfriheten, eftersom förslaget är att på lagnivå föreskriva noggrant avgränsade bestämmelser om förutsättningarna för att tillåta bedömningar av bedömningsorgan för informationssäkerhet med syftet att skydda säkerhetsklassificerad information.

Förhållandet till grundlagens krav när det gäller förfarandet för godkännande av bedömningsorgan för informationssäkerhet beskrivs i förarbetena till den gällande lagen om bedömningsorgan (RP 45/2011 rd s. 14). I 4 § i lagen om bedömningsorgan föreslås att en säkerhetsutredning av företag ska läggas till som en del av godkännandeprocessen för bedömningsorgan när det gäller kompetensområdet för bedömning av hantering av säkerhetsklassificerad information. Den föreslagna ändringen bedöms inte påverka den grundlagsbedömning avseende näringsfriheten som gjordes i samband med antagandet av den gällande lagen om bedömningsorgan, eftersom godkännandeprocessen för bedömningsorganen förblir oförändrad med undantag för det ovan angivna tillägget.

Föreslagna 4 § i bedömningslagen ger tillverkare av säkerhetskritiska lösningar möjlighet att ansöka om en bedömning av överensstämmelse med kraven på informationssäkerhet för en säkerhetskritisk lösning som tillverkats i Finland. I lagen föreslås dock inte någon bedömning av överensstämmelse med kraven som villkor för marknadstillträde. Trots det som sägs ovan kan ett återkallande av beslutet i praktiken påverka verksamheten hos tillverkare av säkerhetskritiska lösningar. Därför kan ett återkallande av beslutet vara av betydelse med tanke på den näringsfrihet som garanteras i 18 § i grundlagen, även om förslaget inte avser tillstånd som krävs för näringsverksamhet. När det gäller bestämmelser om näringsverksamhet har grundlagsutskottet brukat anse att återkallande av tillstånd är en myndighetsåtgärd som ingriper i individens rättsliga ställning och som då har kraftigare effekter än om en ansökan om tillstånd avslås. Därför har utskottet ansett att det med tanke på proportionaliteten i bestämmelserna är nödvändigt att möjligheten att återkalla ett tillstånd binds vid allvarliga eller väsentliga förseelser eller försummelser eller vid att de anmärkningar och varningar som eventuellt givits tillståndshavaren inte har lett till korrigering av påtalade brister i verksamheten (GrUU 20/2006 rd, s. 3/I). Även om en bedömning av en säkerhetskritisk lösning inte är en förutsättning för att bedriva näringsverksamheten, innehåller 10 § i bedömningslagen ett förslag om att den som fått beslutet ska höras och ges tillfälle att avhjälpa bristen innan beslutet eventuellt återkallas. Förslaget anses inte vara problematiskt med tanke på näringsfriheten, eftersom lagen inte avses

reglera villkoren för att bedriva näringsverksamhet och ett återkallande av godkännandebeslutet ska föregås av en möjlighet för den som fått beslutet att avhjälpa bristen.

Rätt att få information

Grundlagsutskottet har i sin praxis ansett att rätten till information som går före sekretessbestämmelserna i sista hand går ut på att den myndighet som är berättigad till informationen i och med sina egna behov åsidosätter de grunder och intressen som är skyddade med hjälp av den sekretessplikt som gäller myndigheten som innehar informationen. Grundlagsutskottet har vid bedömning av bestämmelserna om myndigheternas rätt att få och skyldighet att lämna ut uppgifter med avseende på skyddet för privatliv och personuppgifter i 10 § 1 mom. i grundlagen noterat bland annat vad och vem rätten att få uppgifter gäller och hur rätten är kopplad till nödvändighetskriteriet. Myndigheternas rätt att få uppgifter och möjlighet att lämna ut uppgifter kan enligt utskottet gälla ”behövliga uppgifter” för ett visst syfte, om lagen ger en uttömmande förteckning över uppgiftsinnehållet. Om innehållet däremot inte anges i form av en förteckning, ska det i lagstiftningen ingå ett krav på att ”uppgifterna är nödvändiga” för ett visst syfte (bl.a. GrUU 10/2014 rd, s. 6/I, GrUU 19/2012 rd, s. 3–4 och GrUU 62/2010 rd, s. 4/I.

Propositionen innehåller ett förslag om samarbete mellan de bedömningsmyndigheter som avses i 4 b § i bedömningslagen, det vill säga Transport- och kommunikationsverket och den av Huvudstaben utsedda säkerhetsmyndigheten, samt om rätten att få sådana uppgifter som är nödvändiga när det gäller skötseln av bedömnings- och samordningsuppgifter, trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter. I 7 § i lagen om bedömningsorgan föreslås ett tillägg om att Transport- och kommunikationsverket ska ha rätt att få information av skyddspolisen, den nationella ackrediteringsenheten, den myndighet som styr eller övervakar tillämpningen av bedömningsgrunden för kompetensområdet, bedömningsorganet samt dess underleverantörer och kunder, trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter, om de uppgifter som är nödvändiga för tillsynen över att ett bedömningsorgan för informationssäkerhet uppfyller de krav som ställs på dess verksamhet. I båda fallen krävs att uppgifterna är nödvändiga för att myndigheten ska kunna fullgöra sina lagstadgade uppgifter. Nödvändigheten innebär att det syfte för vilket dessa uppgifter begärs inte kan uppnås utan exempelvis säkerhetsåtgärder för informations- och kommunikationssystem, uppgifter om beredskap för olyckor eller undantagstillstånd eller uppgifter som rör privata affärs- eller yrkeshemligheter.

Dessutom innehåller propositionen en ändring av 6 § i bedömningslagen, där det föreslås en precisering av förteckningen över de objekt bedömningsmyndigheten har rätt att få information om. Dessutom föreslås att rätten att få information och tillträde till informationssystem, datakommunikation och lokaler ska kopplas till nödvändighetskriteriet för att utföra uppgifterna, i stället för till behovskriteriet. På det sättet skyddas de intressen bättre som skyddas av sekretessplikten för de myndigheter och företag som förfogar över uppgifter och system.

Skydd för personuppgifter

Grundlagsutskottet har betonat att det i den mån som EU-lagstiftningen kräver reglering på det nationella planet eller möjliggör sådan tas hänsyn till de krav som de grundläggande fri- och rättigheterna och de mänskliga rättigheterna ställer när det nationella handlingsutrymmet utnyttjas (se t.ex. GrUU 1/2018 rd, GrUU 25/2005 rd). Utskottet har framhållit att det därför finns anledning att särskilt i fråga om bestämmelser som är av betydelse med hänsyn till de grundläggande fri- och rättigheterna tydligt klargöra ramarna för det nationella

handlingsutrymmet (se t.ex. GrUU 17/2019 rd, s. 2–3, GrUU 29/2018 rd, s. 3, GrUU 26/2018 rd, s. 4, GrUU 14/2018 rd, s. 7, GrUU 1/2018 rd, s. 3, GrUU 26/2017 rd, s. 42, GrUU 2/2017 rd, s. 2 och GrUU 44/2016 rd, s. 4).

I de ändringar av 3, 7, 8 och 9 § i bedömningslagen samt i de nya 3 a–3 c § som ingår i propositionen föreskrivs om förfaranden för bedömning av informationssäkerhet och beredskap i myndigheters informationssystem och datakommunikation, myndigheternas bedömningsskyldigheter, påvisande av överensstämmelse med kraven, bedömningsgrunder, bedömningsrapport, beslut om godkännande eller utlåtande om godkännande samt upprätthållande och uppföljning av informationssäkerheten. Syftet med regleringen är att säkerställa informationssäkerheten i myndigheternas informationssystem och datakommunikation. Regleringen påverkar även behandlingen av personuppgifter i den mån personuppgifter behandlas i myndigheternas informationssystem och datakommunikation. Behandlingen av personuppgifter i myndigheternas system hänger samman med de grunder som avses i artikel 6.1 c och e i dataskyddsförordningen. Bestämmelser om grunderna för behandlingen av dessa föreskrivs antingen i dataskyddslagen eller i speciallagar. Enligt dataskyddsförordningens artikel 6.3 får personuppgifter med stöd av nationell reglering enligt punkt 1 c och e behandlas inbegripet åtgärder för att tillförsäkra en laglig och rättvis behandling. Bestämmelserna om bedömning av informationssäkerhet och beredskap kan betraktas som åtgärder för att tillförsäkra en laglig och rättvis behandling av uppgifter i syfte att genomföra skyddet av personuppgifter.

Hemfrid

Det föreslås att rätten enligt 6 § 1 mom. i bedömningslagen att få tillträde till lokaler där uppgifter som gäller informationssystem, datakommunikation eller säkerhetskritiska lösningar behandlas breddas så att alla bedömningsmyndigheter som omfattas av lagen ska ha rätt att utföra inspektioner i enlighet med paragrafen. Vidare läggs enligt förslaget till 6 § 2 mom. en rätt att utföra inspektioner i lokalerna hos en tillverkare av lösningar för skydd mot informationsläckage via diffus strålning och hos dennes underleverantörer. Enligt 7 § 1 mom. i lagen om bedömningsorgan ska den rätt som Transport- och kommunikationsverket och sakkunniga som bistår verket har att inspektera lokalerna hos ett bedömningsorgan för informationssäkerhet som ansöker om godkännande eller som är godkänt utvidgas till att även omfatta en i lagens 9 a § avsedd underleverantör till bedömningsorganet.

Bestämmelserna är av betydelse med tanke på den hemfrid som föreskrivs i 10 § 1 mom. i grundlagen. I samband med antagandet av den gällande bedömningslagen och lagen om bedömningsorgan har inspektionsrätten granskats ur grundlagsperspektiv och det har fastställts att det varken är meningen eller nödvändigt att utvidga inspektionen till lokaler som omfattas av hemfrid. För tydlighetens skull och för att beakta grundlagens bestämmelser om hemfrid har sådana utrymmen uttryckligen undantagits från inspektionsrätten i bestämmelsen (bl.a. GrUU 2/2002 rd, GrUU 18/2006 rd. Det är inte meningen att denna begränsning ska ändras i samband med denna proposition vad gäller inspektionsrätten enligt 6 § 1 mom. i bedömningslagen eller 7 § 1 mom. i lagen om bedömningsorgan. Avsikten är att utvidga begränsningen så att den även omfattar den föreslagna inspektionsrätten enligt 6 § 2 mom. i bedömningslagen.

Egendomsskydd

I 6 § i bedömningslagen föreskrivs att bedömningsmyndigheten får vidta de inspektionsåtgärder som bedömningen kräver. Förslaget är av betydelse med hänsyn till det egendomsskydd som tryggas i 15 § 1 mom. i grundlagen. Egendomsskyddet omfattar utöver den principiella rätten för en ägare att disponera och använda sin egendom på önskat sätt också rätten att råda över den

(GrUU 41/2006 rd, s. 2, GrUU 49/2005 rd, s. 2, GrUU 15/2005 rd, s. 2). Enligt grundlagsutskottets praxis kan ägarens rättigheter begränsas genom lag, förutsatt att regleringen uppfyller de allmänna förutsättningarna för begränsning av de grundläggande fri- och rättigheterna.

Inspektionsåtgärder och med dem förenad teknisk testning är ett nödvändigt förfarande vid bedömningen av informationssäkerheten i informationssystem, datakommunikation och säkerhetskritiska lösningar. Genom tekniska tester kan rapporter som erhållits via dokumentation verifieras och informationssystemets eller den säkerhetskritiska lösningens förmåga att skydda sig mot olika hot mot informationssäkerheten observeras.

Förslaget bedöms vara exakt och noggrant avgränsat med avseende på de allmänna villkoren för begränsning av de grundläggande fri- och rättigheterna samt tillräckligt proportionerligt i förhållande till de mål som ligger till grund för propositionen, eftersom inspektionsåtgärderna är kopplade till nödvändighetskravet, reglerade på lagnivå och inte inkräktar på kärnområdet för egendomsskyddet.

Organisatorisk tillämpning

De ändringar som föreslås i bedömningslagen avses gälla de högsta laglighetsövervakarna, riksdagens ämbetsverk, republikens presidents kansli samt rättskipningen. Därför bör de föreslagna ändringarna bedömas mot bakgrund av bestämmelserna i grundlagen.

I 3 a § 1 mom. i bedömningslagen föreskrivs enligt förslaget en skyldighet för statsförvaltningsmyndigheter att bedöma informationssäkerheten i och beredskapen hos sina informationssystem och sin datakommunikation med hjälp av de förfaranden som avses i 3 §. I 3 a § 2 mom. i bedömningslagen föreskrivs närmare om valet av bedömningsförfarande och skyldigheten att begära en bedömning av en bedömningsmyndighet eller skaffa en bedömning av ett bedömningsorgan för informationssäkerhet i fråga om sådana informationssystem och sådan datakommunikation där uppgifter som hör till säkerhetsklass I –III. behandlas. Enligt 3 a § 3 mom. tillämpas vad som föreskrivs i 2 mom. inte på verksamhet som bedrivs av skyddspolisen, riksdagens justitieombudsman eller justitiekanslern i statsrådet eller på domstolar, republikens presidents kansli eller riksdagens ämbetsverk.

I propositionen har hänsyn tagits till de högsta laglighetsövervakarnas ställning enligt grundlagen samt till grundlagsutskottets yttrande om denna ställning (GrUU 14/2018 rd). De högsta laglighetsövervakarna omfattas av den föreslagna bestämmelsen i 3 a § 1 mom. om skyldigheten att bedöma informationssäkerheten i och beredskapen hos sina informationssystem och sin datakommunikation med hjälp av de förfaranden som avses i 3 §, men undantas från tillämpningsområdet för föreslagna 2 mom. Följaktligen omfattas de högsta laglighetsövervakarna inte av skyldigheterna avseende valet av bedömningsförfarande, och de är inte skyldiga att begära en bedömning av en bedömningsmyndighet eller skaffa en bedömning av ett bedömningsorgan för informationssäkerhet, utan valet av bedömningsförfarande överlåts till deras eget gottfinnande.

På samma sätt som för de högsta laglighetsövervakarna gäller den bedömningsskyldighet som föreslås i 3 a § 1 mom. i bedömningslagen även riksdagens ämbetsverk, medan de undantas från tillämpningsområdet för föreslagna 3 a § 2 mom. I regleringen har i detta avseende grundlagsutskottets utlåtande beaktats (GrUU 46/2010 rd).

Bedömningslagens 3 a § 2 mom. tillämpas inte heller på domstolarnas verksamhet eller på nämnder som inrättats för att handlägga besvärsärenden. På det sättet beaktas

domstolsväsendets oberoende som garanteras i 3 § 3 mom. i grundlagen samt grundlagsutskottets utlåtanden om att statliga centralförvaltningsmyndigheters styrningsbehörighet inte bör utsträckas till att omfatta styrning av domstolarnas interna förvaltning eller rättskipning (t.ex. GrUU 46/2010 rd och GrUU 14/2018 rd). Däremot kan styrningsbehörigheten utövas på de informationssystem som domstolarna använder, eftersom framställningen av systemen huvudsakligen åligger Rättsregistercentralen och utvecklingen och underhållet av dem Domstolsverket, på vilkas verksamhet de föreslagna bedömningsskyldigheterna ska tillämpas.

Enligt regeringens uppfattning kan lagförslaget med stöd av vad som konstaterats ovan behandlas i vanlig lagstiftningsordning.

Kläm

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

1.

Lag

om ändring av lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation

I enlighet med riksdagens beslut

upphävs i lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011) 8 b §, sådan den lyder i lag 728/2014,

ändras 1–8, 8 a och 9–12 §, av dem 1 § sådan den lyder delvis ändrad i lag 728/2014 och 8 a § sådan den lyder i lag 728/2014, samt

fogas till lagen nya 3 a–3 d, 4 a, 4 b och 7 a § som följer:

1 §

Lagens tillämpningsområde

Denna lag innehåller bestämmelser om bedömning av informationssäkerheten i och beredskapen hos myndigheternas informationssystem och datakommunikation. Denna lag innehåller dessutom bestämmelser om bedömning av informationssäkerheten i säkerhetskritiska lösningar och av informationssäkerheten vid tillverkningen av dem.

Denna lag tillämpas på sådan bedömning av informationssäkerheten i fråga om för hanteringen av särskilt känsligt informationsmaterial avsedda informationssystem, datakommunikationer och säkerhetskritiska lösningar samt tillverkningen av säkerhetskritiska lösningar som förutsätts enligt i lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004) avsedda internationella förpliktelser som gäller informationssäkerhet, om inte något annat föreskrivs i den lagen eller följer av en i den lagen avsedd internationell förpliktelse som gäller informationssäkerhet.

Bestämmelser om Transport- och kommunikationsverkets uppgifter vid utarbetandet av säkerhetsutredningar av företag finns i säkerhetsutredningslagen (726/2014) och bestämmelser om verkets uppgifter i fråga om ärenden som gäller den informationssäkerhet i informationssystem och datakommunikation som krävs enligt internationella förpliktelser som gäller informationssäkerhet finns i lagen om internationella förpliktelser som gäller informationssäkerhet.

2 §

Definitioner

I denna lag avses med

1) *informationssystem* ett helhetsarrangemang som består av databehandlingsutrustning, programvara och annan databehandling,

2) *datakommunikation* ett helhetsarrangemang som består av dataöverföringsnät, dataöverföringsutrustning, programvara och annan databehandling samt förfarandena i anslutning till dem,

3) *myndighet* myndigheter som avses i 4 § 1 mom. i lagen om offentlighet i myndigheternas verksamhet (621/1999),

4) *statsförvaltningsmyndighet* statliga förvaltningsmyndigheter och andra statliga ämbetsverk och inrättningar samt domstolar och andra rättskipningsmyndigheter,

5) *informationssäkerhet* skyddande av informationens tillgänglighet, integritet och konfidentialitet genom administrativa, funktionella och tekniska åtgärder,

6) *beredskap* åtgärder för att sörja för att utnyttjandet av informationssystem och datakommunikation samt den verksamhet som baserar sig på dem fortsätter så störningsfritt som möjligt vid störningar under normala förhållanden samt under sådana undantagsförhållanden som avses i beredskapslagen (1552/2011),

7) *bedömningsorgan för informationssäkerhet* sådana företag, sammanslutningar och myndigheter som avses i lagen om bedömningsorgan för informationssäkerhet (1405/2011) och som Transport- och kommunikationsverket har godkänt i enlighet med den lagen,

8) *säkerhetsklass* säkerhetsklasser som avses i 18 § 1 mom. i lagen om informationshantering inom den offentliga förvaltningen (906/2019) och i den statsrådsförordning som utfärdats med stöd av 4 mom. i den paragrafen,

9) *säkerhetskritiska lösningar* krypteringslösningar, lösningar för skydd mot informationsläckage via diffus strålning och andra informations- och kommunikationstekniska lösningar, produkter, implementeringar eller tjänster som skyddar säkerhetsklassificerad information i informationssystem och datakommunikation,

10) *tillverkare av en säkerhetskritisk lösning* ett företag som ansvarar för utvecklingen, planeringen, tillverkningen, sammanställningen och underhållet av en säkerhetskritisk lösning.

3 §

Förfaranden för bedömning av informationssäkerhet och beredskap

Förfaranden för bedömning av informationssäkerheten i och beredskapen hos informationssystem och datakommunikation är

1) självbedömning som en myndighet genomför,

2) bedömningar som en tjänsteleverantör utför på uppdrag av en myndighet,

3) bedömningar som utförs av ett bedömningsorgan för informationssäkerhet, och

4) bedömningar som utförs av en bedömningsmyndighet som avses i 3 d §.

En myndighet kan utföra en bedömning genom ett förfarande enligt 1 mom. 2 punkten endast om det i det informationssystem eller den datakommunikation som är föremål för bedömningen behandlas uppgifter som är offentliga eller sekretessbelagda eller som högst hör till säkerhetsklass IV. Myndigheten ska då på förhand försäkra sig om tjänsteleverantörens tillförlitlighet i den omfattning som uppdraget förutsätter.

En myndighet kan utföra en bedömning genom ett förfarande enligt 1 mom. 3 punkten endast om det i det informationssystem eller den datakommunikation som är föremål för bedömningen behandlas uppgifter som högst hör till säkerhetsklass III.

3 a §

Bedömningsskyldigheter för statsförvaltningsmyndigheter

En statsförvaltningsmyndighet ska bedöma informationssäkerheten i och beredskapen hos sina informationssystem och sin datakommunikation med hjälp av de förfaranden som avses i 3 § 1 mom.

Statsförvaltningsmyndigheten ska välja bedömningsförfarande på basis av en riskbedömning av informationssystemet eller datakommunikationen, dock så att myndigheten ska

1) begära en bedömning av en bedömningsmyndighet i fråga om sådana informationssystem och sådan datakommunikation där uppgifter som hör till säkerhetsklass I eller II behandlas,

2) begära en bedömning av en bedömningsmyndighet eller skaffa en bedömning av ett bedömningsorgan för informationssäkerhet i fråga om sådana informationssystem och sådan datakommunikation där uppgifter som hör till säkerhetsklass III behandlas, om inte statsförvaltningsmyndigheten på basis av en riskbedömning av informationssystemet eller datakommunikationen beslutar att det är onödigt att begära eller skaffa en bedömning,

3) alltid åtminstone genomföra en självbedömning.

Vad som föreskrivs i 2 mom. tillämpas inte på verksamhet som bedrivs av skyddspolisen, riksdagens justitieombudsman eller justitiekanslern i statsrådet eller på domstolar, nämnder som inrättats för att handlägga besvärsärenden, republikens presidents kansli eller riksdagens ämbetsverk.

3 b §

Bedömningsskyldigheter för andra myndigheter än statsförvaltningsmyndigheter

Andra myndigheter än de som avses i 3 a § ska på det sätt som avses i 3 a § 2 mom. 1 punkten bedöma de av sina informationssystem eller den av sin datakommunikation där uppgifter som hör till säkerhetsklass I eller II behandlas.

Andra myndigheter än de som avses i 3 a § ska på det sätt som avses i 3 a § 2 mom. 2 punkten bedöma de av sina informationssystem eller den av sin datakommunikation där uppgifter som hör till säkerhetsklass III behandlas, om inte myndigheten på basis av en riskbedömning av informationssystemet eller datakommunikationen beslutar att det är onödigt att begära eller skaffa en bedömning, varvid myndigheten ska genomföra en självbedömning.

3 c §

Påvisande av att kraven uppfylls

En myndighet kan begära godkännande av en bedömningsmyndighet för sitt informationssystem eller sin datakommunikation för att visa att kraven på informationssäkerhet uppfylls

1) i situationer som avses i lagen om internationella förpliktelser som gäller informationssäkerhet eller som avses i internationella förpliktelser som gäller informationssäkerhet enligt den lagen,

2) om annat internationellt samarbete än sådant som avses i 1 punkten förutsätter det, eller

3) om det föreskrivs särskilt om påvisande av överensstämmelse med kraven.

3 d §

Bedömningsmyndigheter

Behörig bedömningsmyndighet är Transport- och kommunikationsverket. Om bedömningen gäller informationssäkerheten i och beredskapen hos Försvarsmaktens informationssystem eller datakommunikation eller tillhörande säkerhetskritiska lösningar, är behörig bedömningsmyndighet den utsedda säkerhetsmyndigheten vid Huvudstaben som avses i 4 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet.

De bedömningsuppgifter som hör till den utsedda säkerhetsmyndigheten vid Huvudstaben kan också skötas av en person som hör till Försvarsmaktens avlönade personal och som av säkerhetsmyndigheten har utsetts till uppgiften och vars verksamhet styrs och övervakas av säkerhetsmyndigheten.

Bedömningsmyndigheterna ska till sin organisation och sitt beslutsfattande vara oberoende vid skötseln av bedömningsuppgifterna. Dessutom ska bedömningsmyndigheterna säkerställa att dess anställda eller personer som agerar för dess räkning har tillräcklig utbildning och erfarenhet med tanke på bedömningsuppgiftens art och omfattning.

4 §

Bedömningsmyndigheternas uppgifter

Bedömningsmyndigheterna har till uppgift att på begäran av en myndighet bedöma informationssäkerheten i och beredskapen hos myndighetens informationssystem och datakommunikation och tillhörande säkerhetskritiska lösningar.

Utöver vad som föreskrivs i 1 mom. ska Transport- och kommunikationsverket

1) på ansökan av en tillverkare av säkerhetskritiska lösningar som är etablerad i Finland göra en bedömning av huruvida en i Finland tillverkad säkerhetskritisk lösning och dess tillverkning överensstämmer med kraven på informationssäkerhet,

2) ge rådgivning om informationssäkerhetsåtgärder och bedömning av informationssäkerheten i fråga om informationssystem, datakommunikation och säkerhetskritiska lösningar, och

3) styra och övervaka verksamheten hos tillverkare av säkerhetskritiska lösningar som tillverkar lösningar för skydd mot informationsläckage via diffus strålning och som har fått ett beslut om godkännande som avses i 8 § 3 mom., och vid behov meddela beslut om krav på tillverkningsåtgärder eller på lösningen.

Transport- och kommunikationsverket ska sätta de uppgifter som i denna lag föreskrivs för verket i egenskap av bedömningsmyndighet i prioritetsordning och sköta uppgifterna i enlighet med de resurser som står till dess förfogande. Transport- och kommunikationsverket kan genom sitt beslut låta bli att utföra en bedömning som begärts av verket eller åta sig att utföra endast en partiell bedömning. Vid prioriteringen av uppgifterna och i beslutet ska hänsyn tas till

1) iakttagande av internationella förpliktelser som gäller informationssäkerhet,

2) myndigheternas bedömningsskyldigheter enligt 3 a och 3 b §,

3) informationens säkerhetsklass,

4) tillgången till annan oberoende bedömning än den bedömning som Transport- och kommunikationsverket utför,

5) främjande av utbudet av finländska säkerhetskritiska lösningar,

6) likabehandling av dem som begär och ansöker om bedömning, och

7) vilken allmän betydelse de begärda åtgärderna har när det gäller att allmänt förbättra informationssäkerheten i myndigheternas informationssystem och datakommunikation eller att skydda samhällets vitala funktioner.

En i 1 mom. avsedd begäran till Transport- och kommunikationsverket får på uppdrag av en myndighet också framställas av den som för myndighetens räkning sköter anskaffningar eller tillhandahåller databehandlings- eller datakommunikationstjänster eller sköter serviceuppgifter med anknytning till ordnandet av dem.

4 a §

Uppgifter för att bistå bedömningsmyndigheterna

Bedömningsmyndigheterna kan anlita utomstående sakkunniga som hjälp vid bedömningen, om det är nödvändigt på grund av bedömningens art, de tillgängliga resurserna eller tekniska skäl som hänför sig till bedömningen. De utomstående sakkunniga ska ha tillräcklig utbildning och erfarenhet med tanke på bedömningsuppgiftens art och omfattning. På utomstående

sakkunniga tillämpas bestämmelserna om straffrättsligt tjänsteansvar när de sköter uppgifter enligt denna paragraf. Bestämmelser om skadeståndsansvar finns i skadeståndslagen (412/1974).

Teknologiska forskningscentralen VTT Ab har till uppgift att på uppdrag av en bedömningsmyndighet bedöma säkerhetskritiska lösningar. På anställda vid Teknologiska forskningscentralen VTT Ab tillämpas vad som i 1 mom. föreskrivs om utomstående sakkunniga.

4 b §

Informationsutbyte och samarbete mellan bedömningsmyndigheterna

Bedömningsmyndigheterna ska samarbeta när det gäller skötseln av uppgifter enligt denna lag och trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter lämna varandra sådana uppgifter som är nödvändiga för detta ändamål.

Trots bestämmelserna i 3 d § 1 mom. och 4 § 1 och 2 mom. kan bedömningsmyndigheterna avtala om att sköta enskilda i denna lag avsedda uppgifter eller en del av uppgifterna för en annan bedömningsmyndighets räkning, om arrangemanget behövs för att uppgifterna ska kunna skötas på ett ändamålsenligt, ekonomiskt och snabbt sätt.

Transport- och kommunikationsverket svarar för styrningen av samarbetet mellan bedömningsmyndigheterna med syfte att skapa en enhetlig tillämpningspraxis.

5 §

Utredningar på uppdrag av finansministeriet

För att följa verkställigheten av bestämmelserna om informationssäkerhet inom statsförvaltningen och för att utveckla bestämmelserna kan finansministeriet be Transport- och kommunikationsverket göra utredningar om den allmänna nivån på informationssäkerheten i och beredskapen hos statsförvaltningsmyndigheternas informationssystem eller datakommunikation. De informationssystem som en utredning ska omfatta kan utses utgående från informationssystemens användningsändamål, arten av de uppgifter som registreras eller något annat motsvarande allmänt kriterium.

Den utredning som Transport- och kommunikationsverket lämnar till finansministeriet får oberoende av sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter innehålla de uppgifter som är nödvändiga för att utredningens syfte ska kunna uppnås.

6 §

Bedömningsmyndigheternas rätt att få uppgifter, inspektionsrätt och rätt att få tillträde till lokaler och informationssystem

Bedömningsmyndigheterna och i 4 a § avsedda utomstående sakkunniga som bistår bedömningsmyndigheterna har rätt att trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter få tillgång till uppgifter, handlingar, utrustning och program som hänför sig till informationssystem, datakommunikation eller säkerhetskritiska lösningar eller tillverkningen av dem och som är nödvändiga för att de ska kunna utföra sina uppgifter enligt denna lag och att i den utsträckning det är nödvändigt för att utföra uppgifterna få tillträde till informationssystem och datakommunikationer samt till lokaler där uppgifter som hör till föremålet för bedömningen behandlas samt att utföra behövliga administrativa och tekniska bedömningsåtgärder.

Transport- och kommunikationsverket har rätt att utföra inspektioner i lokalerna hos en tillverkare av lösningar för skydd mot informationsläckage via diffus strålning och hos dennes underleverantörer för att utreda om tillverkaren och dennes underleverantör iakttar de beslut som meddelats med stöd av denna lag. Den utsedda säkerhetsmyndigheten vid Huvudstaben har rätt att utföra sådana inspektioner som avses ovan, om den sköter en uppgift för Transport- och kommunikationsverkets räkning på det sätt som avses i 4 b § 2 mom. Vid inspektionerna kan Transport- och kommunikationsverket och den utsedda säkerhetsmyndigheten vid Huvudstaben biträdas av sådana utomstående sakkunniga som avses i 4 a §. På den rätt som Transport- och kommunikationsverket, den utsedda säkerhetsmyndigheten vid Huvudstaben och utomstående sakkunniga har att få tillträde till lokaler och få granska nödvändiga uppgifter och att utföra bedömningsåtgärder tillämpas vad som föreskrivs i 1 mom. Vid inspektioner ska 39 § i förvaltningslagen (434/2003) iakttas.

Inspektioner som avses i 1 och 2 mom. får inte utföras i utrymmen som används för permanent boende.

7 §

Bedömningsgrunder för informationssäkerhet och beredskap

Som bedömningsgrunder för informationssäkerheten i och beredskapen hos informationssystem och datakommunikation samt som bedömningsgrunder för informationssäkerheten i säkerhetskritiska lösningar och vid tillverkningen av dem kan användas

1) i lag eller förordning föreskrivna krav på informationssäkerhet, cybersäkerhet eller beredskap som gäller myndigheternas verksamhet samt myndigheternas anvisningar om tillämpningen av kraven,

2) Europeiska unionens, Nordatlantiska fördragsorganisationens eller något annat internationellt organs bestämmelser, föreskrifter och anvisningar om informationssäkerhet, cybersäkerhet eller beredskap samt myndigheternas anvisningar om tillämpningen av dem,

3) publicerade allmänt eller regionalt tillämpade bestämmelser, föreskrifter eller anvisningar om informationssäkerhet, cybersäkerhet eller beredskap,

4) krav som gäller informationssäkerhet, cybersäkerhet eller beredskap och som ingår i en fastställd standard.

Vid fastställandet av bedömningsgrunderna och föremålet för bedömningen ska de föreskrivna kraven på informationssäkerheten i och beredskapen hos informationssystemet och datakommunikationen och de krav som valts utifrån en riskbedömning beaktas. Bedömningsmyndigheterna fastställer bedömningsgrunderna för en bedömning de ska utföra efter att ha hört den som begär bedömningen.

Bedömningsmyndigheterna fastställer bedömningsgrunderna för en säkerhetskritisk lösning efter att ha hört tillverkaren av den säkerhetskritiska lösningen. Utöver vad som föreskrivs i 1 och 2 mom. ska informationens säkerhetsklass, säkerheten vid tillverkningen samt beredskapen att uppfylla internationella förpliktelser som gäller informationssäkerhet beaktas när bedömningsgrunderna för säkerhetskritiska lösningar fastställs.

7 a §

Utredningar som hänför sig till bedömningar av tillverkare av säkerhetskritiska lösningar

Transport- och kommunikationsverket ska vid en i 4 § 2 mom. 1 punkten avsedd bedömning av en säkerhetskritisk lösning och av dess tillverkning ansöka om en i säkerhetsutredningslagen avsedd säkerhetsutredning av företag i fråga om den tillverkare som ansöker om bedömningen. Godkännandet av en säkerhetskritisk lösning förutsätter att det i den säkerhetsutredning av

företag som gäller tillverkaren inte har framkommit något som utifrån en helhetsbedömning skulle äventyra tillverkningens säkerhet och tillförlitlighet i synnerhet med hänsyn till riskerna för utländsk påverkan.

Om en fastställd internationell standard används som en del av bedömningsgrunderna avseende tillverkningen av en säkerhetskritisk lösning, kan överensstämmelse med standarden påvisas på det sätt som anges i lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (920/2005).

8 §

Utfärdande av bedömningsrapport, beslut om godkännande och utlåtande om godkännande

I fråga om bedömningen av informationssäkerheten i och beredskapen hos ett informationssystem och hos datakommunikation ska det utarbetas en bedömningsrapport i vilken ska antecknas uppgifter om föremålet för bedömningen, vilka bedömningsgrunder som använts, bedömningens omfattning och de observationer som gjorts.

Utöver vad som föreskrivs i 1 mom. ska bedömningsmyndigheten på en i 3 c § avsedd begäran meddela ett beslut om godkännande eller ge ett utlåtande om godkännande i fråga om en myndighets informationssystem eller datakommunikation, om informationssystemet eller datakommunikationen uppfyller kraven. I beslutet eller utlåtandet ska det antecknas uppgifter om föremålet för bedömningen, vilka bedömningsgrunder som använts, bedömningens omfattning, resultaten av bedömningen och kvarstående risk samt vid behov uppgift om giltighetstiden.

Utöver vad som föreskrivs i 1 mom. ska Transport- och kommunikationsverket i fråga om en i 4 § 2 mom. 1 punkten avsedd ansökan om bedömning av informationssäkerheten i en säkerhetskritisk lösning och av informationssäkerheten vid dess tillverkning meddela ett beslut av vilket resultatet av bedömningen framgår. Av beslutet om godkännande ska giltighetstiden för godkännandet framgå, och i beslutet kan ingå sådana begränsningar och villkor som behövs för en säker användning av lösningen. I ett beslut om godkännande som gäller en tillverkare av en säkerhetskritisk lösning som tillverkar lösningar för skydd mot informationsläckage via diffus strålning kan ingå sådana villkor som behövs för att säkerställa att tillverkningen är tillförlitlig.

8 a §

Förteckning över godkända säkerhetskritiska lösningar och tillverkare

Transport- och kommunikationsverket för en offentlig förteckning över säkerhetskritiska lösningar och tillverkare av säkerhetskritiska lösningar som fått ett beslut om godkännande i enlighet med 8 § 3 mom. Av förteckningen ska framgå

1) namnet på den säkerhetskritiska lösningen, dess användningsändamål och version,
2) den informationssäkerhetsklass för vilken lösningen konstaterats ge ett tillräckligt skydd,
3) tillverkaren av den säkerhetskritiska lösningen,
4) godkännandets giltighet samt ändring eller upphörande av godkännandet, och
5) de villkor och begränsningar för en säker användning som hänför sig till godkännandet.

9 §

Upprätthållande och uppföljning av informationssäkerheten

Den som fått ett beslut eller utlåtande enligt 8 § ska upprätthålla informationssäkerheten i enlighet med utlåtandet eller beslutet. Den som fått ett beslut eller utlåtande ska underrätta

bedömningsmyndigheten om sådana ändringar som kan inverka på de krav som anges i beslutet eller utlåtandet.

10 §

Återkallande av beslut om godkännande eller utlåtande om godkännande

Bedömningsmyndigheten kan helt eller delvis återkalla ett utlåtande eller beslut som avses i 8 §, om det informationssystem, den datakommunikation eller den säkerhetskritiska lösning eller den tillverkare av en säkerhetskritisk lösning som bedömningen har gällt inte längre uppfyller de krav som har utgjort en förutsättning för meddelande av beslutet eller givande av utlåtandet.

Innan bedömningsmyndigheten i enlighet med 1 mom. återkallar ett utlåtande eller beslut ska myndigheten höra den som fått beslutet eller utlåtandet och ge denne tillfälle att avhjälpa bristen.

Bedömningsmyndigheten kan i det beslut om återkallande som avses i 1 mom. bestämma att beslutet ska iakttas även om det överklagas, om inte besvärsmyndigheten bestämmer något annat.

11 §

Ändringssökande

I fråga om sökande av ändring i beslut som bedömningsmyndigheten har meddelat med stöd av denna lag gäller vad som föreskrivs i lagen om rättegång i förvaltningsärenden (808/2019).

12 §

Avgifter

För bedömningsmyndighetens bedömning samt för en bedömningsrapport, ett utlåtande eller ett beslut och för rådgivning och utredning tas det hos den som inlett ärendet ut en avgift med iakttagande av vad som föreskrivs i lagen om grunderna för avgifter till staten (150/1992).

Denna lag träder i kraft den 2026 .

Statsförvaltningsmyndigheterna ska se till att bedömningen av informationssäkerheten i och beredskapen hos deras informationssystem och datakommunikation motsvarar det som föreskrivs i 3 a § inom fem år från ikraftträdandet av denna lag, dock så att bedömningen ska motsvara det som föreskrivs i 2 mom. 1 punkten i den paragrafen inom två år från ikraftträdandet och det som föreskrivs i 2 punkten inom tre år från ikraftträdandet.

Andra än statsförvaltningsmyndigheter ska se till att bedömningen av informationssäkerheten i och beredskapen hos deras informationssystem och datakommunikation motsvarar det som föreskrivs i 3 b § 1 mom. inom två år från ikraftträdandet av denna lag och det som föreskrivs i 2 mom. i den paragrafen inom tre år från ikraftträdandet.

Ett intyg över överensstämmelse med kraven på informationssäkerhet som har utfärdats i enlighet med de bestämmelser som gällde vid ikraftträdandet av denna lag motsvarar det beslut som avses i 8 § och är giltigt under den tid som anges i intyget.

2.

Lag

om ändring av lagen om bedömningsorgan för informationssäkerhet

I enlighet med riksdagens beslut

ändras i lagen om bedömningsorgan för informationssäkerhet (1405/2011) 1 kap., 3 § 1 mom., 4–8 §, rubriken för 3 kap., 9–13 och 13 a §, av dem 4 § sådan den lyder delvis ändrad i lag 727/2014 och 13 a § sådan den lyder i lag 727/2014, samt

fogas till lagen en ny 9 a § som följer:

1 kap.

Allmänna bestämmelser

1 §

Lagens syfte

Denna lag innehåller bestämmelser om ett förfarande genom vilket myndigheter kan skaffa en oberoende bedömning av informationssäkerheten och beredskapen och genom vilket företag tillförlitligt kan visa en utomstående att de i sin verksamhet har sörjt för en viss informationssäkerhetsnivå.

2 §

Lagens tillämpningsområde

Denna lag tillämpas på näringsidkare och på enheter som tillhandahåller serviceuppgifter för den offentliga förvaltningen och som på uppdrag bedömer nivån på informationssäkerheten eller på beredskapen hos informationssystem eller datakommunikation (*bedömningsorgan för informationssäkerhet*) och som vill att Transport- och kommunikationsverket ska godkänna deras verksamhet. Lagen tillämpas dessutom på godkännandeförfarandet.

I fråga om bedömningsmyndigheternas uppgifter vid bedömning av informationssäkerheten i och beredskapen hos myndigheternas informationssystem och datakommunikation samt vid uppgörande av säkerhetsutredningar av företag föreskrivs särskilt.

3 §

Ansökan om godkännande av bedömningsorgan

Bedömningsorgan för informationssäkerhet kan ansöka hos Transport- och kommunikationsverket om godkännande för sin verksamhet och för kompetensområdet för bedömningen.

— —

4 §

Behandlingen av ansökan

Innan ett bedömningsorgan för informationssäkerhet godkänns ska Transport- och kommunikationsverket ge skyddspolisen tillfälle att yttra sig om tillförlitligheten hos bedömningsorganets ansvariga personer och om säkerheten i bedömningsorganets lokaler. Om ansökan gäller kompetensområdet för bedömning av hanteringen av säkerhetsklassificerad information, ska Transport- och kommunikationsverket för att säkerställa företagets och dess ansvarspersoners tillförlitlighet och förmåga att sköta sina åtaganden ansöka om en i säkerhetsutredningslagen (726/2014) avsedd säkerhetsutredning av företaget i fråga. När skyddspolisen sammanställer sitt utlåtande eller gör utredningen ska den iaktta det som föreskrivs i säkerhetsutredningslagen.

När Transport- och kommunikationsverket behandlar en ansökan kan verket inhämta utlåtanden av myndigheterna samt anlita utomstående sakkunniga för biträdande uppgifter i anknytning till bedömningen av ansökan och av uppgifter som ingår i den. På utomstående sakkunniga tillämpas bestämmelserna om straffrättsligt tjänsteansvar när de sköter uppgifter enligt denna paragraf. Bestämmelser om skadeståndsansvar finns i skadeståndslagen (412/1974).

5 §

Godkännande av bedömningsorgan

För att ett bedömningsorgan för informationssäkerhet ska godkännas krävs det att

1) organet är funktionellt och ekonomiskt oberoende av den som bedömningen gäller,

2) organets personal har god teknisk och yrkesinriktad utbildning samt tillräckligt omfattande erfarenhet av de uppgifter som ingår i verksamheten,

3) organet har den utrustning, de hjälpmedel och de system som behövs i verksamheten,

4) det i den säkerhetsutredning av företag som gäller organet inte har framkommit någon sådan omständighet som utifrån en helhetsbedömning skulle äventyra företagets och dess ansvarspersoners tillförlitlighet och förmåga att sköta sina åtaganden i fråga om bedömningsuppgiften, eller att tillförlitligheten hos de ansvariga personerna inom organet har säkerställts och organet har en övervakad metod som bedömts som tillförlitlig och med vars hjälp säkerheten i organets lokaler och databehandling samt personalens tillförlitlighet säkerställs,

5) organet har ändamålsenliga anvisningar för sin verksamhet och uppföljningen av den.

Uppfyllandet av kraven i 1 mom. 1–3 punkten ska visas på det sätt som anges i lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (920/2005).

Trots vad som föreskrivs i 2 mom. kan Transport- och kommunikationsverket, när ett godkänt bedömningsorgan ansöker om godkännande för ett nytt kompetensområde, efter att ha hört de myndigheter som är centrala när det gäller godkännandet av kompetensen besluta att kraven anses vara uppfyllda.

Utifrån de utredningar som Transport- och kommunikationsverket har mottagit eller utfört och de inspektioner som verket har förrättat godkänner verket ett organ där kraven uppfylls som ett godkänt bedömningsorgan för informationssäkerhet. Ett sådant organ får i sin marknadsföring och sin övriga kommunikation använda ett uttryck för Transport- och kommunikationsverkets godkännande, förutsatt att godkännandets giltighetstid inte har löpt ut eller att Transport- och kommunikationsverket inte har beslutat att återkalla godkännandet.

Ett bedömningsorgan kan godkännas för viss tid, om det finns särskilda skäl till detta. I ett beslut om godkännande kan det ingå begränsningar och villkor som gäller bedömningsorganets kompetensområde, tillsyn och verksamhet och som behövs för att säkerställa att bedömningsorganet sköter sina uppgifter.

6 §

Återkallelse av godkännande av bedömningsorgan

Om ett godkänt bedömningsorgan för informationssäkerhet i väsentlig grad eller fortlöpande handlar i strid med bestämmelserna eller om det inte längre uppfyller kraven för godkännande, ska Transport- och kommunikationsverket uppmana bedömningsorganet att avhjälpa bristen inom utsatt tid. Om bristen inte avhjälps inom utsatt tid, kan Transport- och kommunikationsverket återkalla godkännandet av bedömningsorganet eller kompetensområdet.

Transport- och kommunikationsverket kan i sitt beslut bestämma att beslutet ska iakttas även om det överklagas, om inte besvärsmyndigheten bestämmer något annat.

7 §

Transport- och kommunikationsverkets rätt att få information och dess inspektionsrätt

Transport- och kommunikationsverket har rätt att inspektera lokalerna hos ett bedömningsorgan för informationssäkerhet som ansöker om godkännande eller som är godkänt och hos en i 9 a § avsedd underleverantör till bedömningsorganet samt att granska de metoder som bedömningsorganet använder. Vid inspektionerna kan Transport- och kommunikationsverket biträdas av sådana utomstående sakkunniga som avses i 4 § 2 mom. Inspektioner får inte utföras i utrymmen som används för boende av permanent natur.

Transport- och kommunikationsverket har trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter rätt att av skyddspolisen, den nationella ackrediteringsenheten, den myndighet som styr eller övervakar tillämpningen av bedömningsgrunden för kompetensområdet, bedömningsorganet samt dess underleverantörer och kunder på begäran få de uppgifter som är nödvändiga för tillsynen över att ett bedömningsorgan för informationssäkerhet uppfyller de krav som ställs på dess verksamhet.

8 §

Bedömningsorganens anmälningsskyldighet

Ett godkänt bedömningsorgan för informationssäkerhet ska underrätta Transport- och kommunikationsverket om sådana ändringar i sin verksamhet som är av betydelse med tanke på de skyldigheter som organet har.

3 kap.

Bedömning av informationssäkerhet och beredskap

9 §

Bedömningsorganens uppgifter

När ett godkänt bedömningsorgan för informationssäkerhet har fått i uppdrag att utföra en bedömning av informationssäkerheten och beredskapen ska det iaktta omsorg och se till att

1) lokalerna hos den som bedömningen gäller vid behov inspekteras,

2) det under bedömningen utreds om den som bedömningen gäller i sin verksamhet på behörigt sätt har uppfyllt de i 10 § angivna kraven som gäller för informationssäkerheten eller beredskapen och som ligger till grund för utredningen (*bedömningsgrunder för informationssäkerhet och beredskap*).

Bedömningen kan även vara partiell.

Ett godkänt bedömningsorgan för informationssäkerhet ska utarbeta en bedömningsrapport i vilken antecknas uppgifter om föremålet för bedömningen, vilka bedömningsgrunder som använts, bedömningens omfattning och de observationer som gjorts.

Ett godkänt bedömningsorgan för informationssäkerhet kan på begäran, eller, om det särskilt föreskrivs om det, på basis av utredningar och inspektioner utfärda ett intyg, om föremålet för bedömningen är förenligt med de bedömningsgrunder för informationssäkerhet och beredskap som legat till grund för utredningen. De grunder för bedömning av informationssäkerheten och beredskapen som använts vid bedömningen samt bedömningens omfattning och giltighetstid ska specificeras i intyget.

9 a §

Underleverantörer

Ett godkänt bedömningsorgan för informationssäkerhet får lägga ut en uppgift i anslutning till bedömningen på underentreprenad till ett annat bolag som hör till samma koncern eller till någon annan underleverantör endast om koncernbolaget eller underleverantören uppfyller förutsättningarna för godkännande av ett bedömningsorgan för informationssäkerhet och en utredning om underentreprenaden har lämnats till Transport- och kommunikationsverket och verket har konstaterat att förutsättningarna uppfylls.

Ett godkänt bedömningsorgan för informationssäkerhet får lägga ut uppgifter som hänför sig till bedömning av hanteringen av säkerhetsklassificerad information på underentreprenad eller anlita ett dotterbolag för uppgifterna endast om organet avtalat om saken med kunden.

10 §

Bedömningsgrunder för informationssäkerhet och beredskap

Som bedömningsgrunder för informationssäkerhet och beredskap kan, enligt beslut av den som bedömningen gäller och enligt bedömningsorganets godkända kompetensområde, vid bedömningar som avses i denna lag användas

1) i lag eller förordning föreskrivna krav på informationssäkerhet, cybersäkerhet eller beredskap som gäller myndigheternas verksamhet samt myndigheternas anvisningar om tillämpningen av kraven,

2) Europeiska unionens, Nordatlantiska fördragsorganisationens eller något annat internationellt organs bestämmelser, föreskrifter och anvisningar om informationssäkerhet, cybersäkerhet eller beredskap samt myndigheternas anvisningar om tillämpningen av dem,

3) publicerade allmänt eller regionalt tillämpade bestämmelser, föreskrifter eller anvisningar om informationssäkerhet, cybersäkerhet eller beredskap,

4) krav som gäller informationssäkerhet, cybersäkerhet eller beredskap och som ingår i en fastställd standard.

11 §

Avgifter

För behandlingen vid Transport- och kommunikationsverket av ärenden som gäller godkännande av och tillsyn över bedömningsorgan för informationssäkerhet tas det ut en avgift med iakttagande av vad som föreskrivs i lagen om grunderna för avgifter till staten (150/1992).

12 §

Ändringssökande

I fråga om sökande av ändring i beslut som Transport- och kommunikationsverket har meddelat med stöd av denna lag gäller vad som föreskrivs i lagen om rättegång i förvaltningsärenden (808/2019).

13 §

Tillämpning av bestämmelser om tjänsteansvar och god förvaltning

När ett godkänt bedömningsorgan för informationssäkerhet utför offentliga förvaltningsuppgifter som avses i denna lag ska det iaktta förvaltningslagen (434/2003), lagen om offentlighet i myndigheternas verksamhet (621/1999), språklagen (423/2003), samiska språklagen (1086/2003), dataskyddslagen (1050/2018) och lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003).

På ansvarspersoner och personer som är anställda vid ett godkänt bedömningsorgan för informationssäkerhet samt på personer som är anställda hos i 9 a § avsedda underleverantörer tillämpas bestämmelserna om straffrättsligt tjänsteansvar när de utför uppgifter enligt denna lag. Bestämmelser om skadeståndsansvar finns i skadeståndslagen.

13 a §

Registrering av uppgifter i registret över säkerhetsutredningar

Transport- och kommunikationsverket ska i det register över säkerhetsutredningar som avses i säkerhetsutredningslagen anteckna uppgifter om godkända bedömningsorgan för informationssäkerhet samt uppgifter som ingår i intyg som getts till bedömningsorganen. Återkallelsen av ett godkännande ska omedelbart antecknas i registret.

Ett godkänt bedömningsorgan för informationssäkerhet kan för anteckning i registret över säkerhetsutredningar och för vidarebefordran ur registret lämna Transport- och kommunikationsverket uppgifter om de organisationer som har varit föremål för bedömningsorganets bedömning och om innehållet i de intyg som bedömningsorganet har gett åt de organisationerna, om inte organisationerna har förbjudit detta. Före uppgifterna lämnas ska den som bedömningen gäller informeras om syftet med databehandlingen och vilken lagstiftning databehandlingen omfattas av.

Denna lag träder i kraft den 2026 .

Transport- och kommunikationsverket ska inom två år från ikraftträdandet av denna lag i enlighet med 4 § ansöka om en säkerhetsutredning av företag i fråga om ett sådant godkänt bedömningsorgan för informationssäkerhet för vilket ett kompetensområde för bedömning av hanteringen av säkerhetsklassificerad information har godkänts i enlighet med de bestämmelser som gällde vid ikraftträdandet.

3.

Lag

om ändring av 18 och 48 § i säkerhetsutredningslagen

I enlighet med riksdagens beslut

upphävs i säkerhetsutredningslagen (726/2014) 48 § 4 mom. 1 punkten, sådan den lyder i lag 347/2020, och

ändras 18 § 2 mom. som följer:

18 §

Överensstämmelse med säkerhetskraven som en allmän förutsättning

— —

Överensstämmelse med kraven enligt 1 mom. kan påvisas genom ett intyg utfärdat av ett godkänt bedömningsorgan som avses i lagen om bedömningsorgan för informationssäkerhet (1405/2011), genom ett beslut eller utlåtande som utfärdats i enlighet med lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011), genom en säkerhetsplan eller på något annat sätt som den behöriga myndighet som beslutar att säkerhetsutredning ska göras godkänner.

— —

_____

Denna lag träder i kraft den 2026.

_____

Helsingfors den 7 maj 2026

Statsminister

Petteri Orpo

Kommun- och regionminister Anna-Kaisa Ikonen

1.

Lag

om ändring av lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation

I enlighet med riksdagens beslut

upphävs i lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011) 8 b §, sådan den lyder i lag 728/2014,

ändras 1–8, 8 a och 9–12 §, av dem 1 § sådan den lyder delvis ändrad i lag 728/2014 och 8 a § sådan den lyder i lag 728/2014, samt

fogas till lagen nya 3 a–3 d, 4 a, 4 b och 7 a § som följer:

Gällande lydelse	*Föreslagen lydelse*
1 §	1 §
Lagens tillämpningsområde	*Lagens tillämpningsområde*
I denna lag finns bestämmelser om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation. Bestämmelser om Kommunikationsverkets uppgifter vid uppgörandet av säkerhetsutredningar av företag finns i säkerhetsutredningslagen (726/2014).	*Denna lag innehåller bestämmelser om bedömning av informationssäkerheten i och beredskapen hos myndigheternas informationssystem och datakommunikation. Denna lag innehåller dessutom bestämmelser om bedömning av informationssäkerheten i säkerhetskritiska lösningar och av informationssäkerheten vid tillverkningen av dem.* *Denna lag tillämpas på sådan bedömning av informationssäkerheten i fråga om för hanteringen av särskilt känsligt informationsmaterial avsedda informationssystem, datakommunikationer och säkerhetskritiska lösningar samt tillverkningen av säkerhetskritiska lösningar som förutsätts enligt i lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004) avsedda internationella förpliktelser som gäller informationssäkerhet, om inte något annat föreskrivs i den lagen eller följer av en i den lagen avsedd internationell förpliktelse som gäller informationssäkerhet.* *Bestämmelser om Transport- och kommunikationsverkets uppgifter vid utarbetandet av säkerhetsutredningar av*

Gällande lydelse	*Föreslagen lydelse*
	företag finns i säkerhetsutredningslagen (726/2014) och bestämmelser om verkets uppgifter i fråga om ärenden som gäller den informationssäkerhet i informationssystem och datakommunikation som krävs enligt internationella förpliktelser som gäller informationssäkerhet finns i lagen om internationella förpliktelser som gäller informationssäkerhet.
2 §	2 §
Definitioner	*Definitioner*
I denna lag avses med 1)*informationssystem* ett helhetsarrangemang som består av databehandlingsutrustning, programvara och annan databehandling, 2)*datakommunikation* ett system som utgörs av arrangemang omfattande ett dataöverföringsnät, dataöverföringsutrustning, programvara och andra databehandlingsarrangemang, 3)*myndighet* organ som avses i 4 § 1 mom. 1–7 punkten i lagen om offentlighet i myndigheternas verksamhet (621/1999) , 4)*statsförvaltningsmyndighet* statliga förvaltningsmyndigheter och andra statliga ämbetsverk och inrättningar samt domstolar och andra rättskipningsmyndigheter.	I denna lag avses med 1) *informationssystem* ett helhetsarrangemang som består av databehandlingsutrustning, programvara och annan databehandling, 2) *datakommunikation ett helhetsarrangemang som består av* dataöverföringsnät, dataöverföringsutrustning, programvara och *annan databehandling samt förfarandena i anslutning till dem,* 3) *myndighet myndigheter* som avses i 4 § 1 mom. i lagen om offentlighet i myndigheternas verksamhet (621/1999), 4) *statsförvaltningsmyndighet* statliga förvaltningsmyndigheter och andra statliga ämbetsverk och inrättningar samt domstolar och andra rättskipningsmyndigheter, 5) *informationssäkerhet skyddande av informationens tillgänglighet, integritet och konfidentialitet genom administrativa, funktionella och tekniska åtgärder,* *6) beredskap åtgärder för att sörja för att utnyttjandet av informationssystem och datakommunikation samt den verksamhet som baserar sig på dem fortsätter så störningsfritt som möjligt vid störningar under normala förhållanden samt under sådana undantagsförhållanden som avses i beredskapslagen (1552/2011),* *7) bedömningsorgan för informationssäkerhet sådana företag, sammanslutningar och myndigheter som avses i lagen om bedömningsorgan för informationssäkerhet (1405/2011) och som*

Gällande lydelse	*Föreslagen lydelse*
	Transport- och kommunikationsverket har godkänt i enlighet med den lagen, *8) säkerhetsklass säkerhetsklasser som avses i 18 § 1 mom. i lagen om informationshantering inom den offentliga förvaltningen (906/2019) och i den statsrådsförordning som utfärdats med stöd av 4 mom. i den paragrafen,* *9) säkerhetskritiska lösningar krypteringslösningar, lösningar för skydd mot informationsläckage via diffus strålning och andra informations- och kommunikationstekniska lösningar, produkter, implementeringar eller tjänster som skyddar säkerhetsklassificerad information i informationssystem och datakommunikation,* *10) tillverkare av en säkerhetskritisk lösning ett företag som ansvarar för utvecklingen, planeringen, tillverkningen, sammanställningen och underhållet av en säkerhetskritisk lösning.*
3 §	3 §
Anlitande av tjänster för bedömning av informationssäkerheten	*Förfaranden för bedömning av informationssäkerhet och beredskap*
Statsförvaltningsmyndigheterna får för bedömning av informationssäkerheten i sina informationssystem och sin datakommunikation bara använda sig av det förfarande som avses i denna lag eller av ett sådant bedömningsorgan som har godkänts av Kommunikationsverket enligt lagen om bedömningsorgan för informationssäkerhet (1405/2011).	*Förfaranden för bedömning av informationssäkerheten i och beredskapen hos informationssystem och datakommunikation är* *1) självbedömning som en myndighet genomför,* *2) bedömningar som en tjänsteleverantör utför på uppdrag av en myndighet,* *3) bedömningar som utförs av ett bedömningsorgan för informationssäkerhet, och* *4) bedömningar som utförs av en bedömningsmyndighet som avses i 3 d §.* *En myndighet kan utföra en bedömning genom ett förfarande enligt 1 mom. 2 punkten endast om det i det informationssystem eller den datakommunikation som är föremål för bedömningen behandlas uppgifter som är offentliga eller sekretessbelagda eller som högst hör till säkerhetsklass IV. Myndigheten ska då på förhand försäkra sig om*

Gällande lydelse

Föreslagen lydelse

tjänsteleverantörens tillförlitlighet i den omfattning som uppdraget förutsätter.

En myndighet kan utföra en bedömning genom ett förfarande enligt 1 mom. 3 punkten endast om det i det informationssystem eller den datakommunikation som är föremål för bedömningen behandlas uppgifter som högst hör till säkerhetsklass III.

3 a §

Bedömningsskyldigheter för statsförvaltningsmyndigheter

En statsförvaltningsmyndighet ska bedöma informationssäkerheten i och beredskapen hos sina informationssystem och sin datakommunikation med hjälp av de förfaranden som avses i 3 § 1 mom.

Statsförvaltningsmyndigheten ska välja bedömningsförfarande på basis av en riskbedömning av informationssystemet eller datakommunikationen, dock så att myndigheten ska

1) begära en bedömning av en bedömningsmyndighet i fråga om sådana informationssystem och sådan datakommunikation där uppgifter som hör till säkerhetsklass I eller II behandlas,

2) begära en bedömning av en bedömningsmyndighet eller skaffa en bedömning av ett bedömningsorgan för informationssäkerhet i fråga om sådana informationssystem och sådan datakommunikation där uppgifter som hör till säkerhetsklass III behandlas, om inte statsförvaltningsmyndigheten på basis av en riskbedömning av informationssystemet eller datakommunikationen beslutar att det är onödigt att begära eller skaffa en bedömning,

3) alltid åtminstone genomföra en självbedömning.

Vad som föreskrivs i 2 mom. tillämpas inte på verksamhet som bedrivs av skyddspolisen, riksdagens justitieombudsman eller justitiekanslern i statsrådet eller på domstolar, nämnder som inrättats för att handlägga besvärsärenden, republikens presidents kansli eller riksdagens ämbetsverk.

Gällande lydelse

Föreslagen lydelse

3 b §

Bedömningsskyldigheter för andra myndigheter än statsförvaltningsmyndigheter

Andra myndigheter än de som avses i 3 a § ska på det sätt som avses i 3 a § 2 mom. 1 punkten bedöma de av sina informationssystem eller den av sin datakommunikation där uppgifter som hör till säkerhetsklass I eller II behandlas.

Andra myndigheter än de som avses i 3 a § ska på det sätt som avses i 3 a § 2 mom. 2 punkten bedöma de av sina informationssystem eller den av sin datakommunikation där uppgifter som hör till säkerhetsklass III behandlas, om inte myndigheten på basis av en riskbedömning av informationssystemet eller datakommunikationen beslutar att det är onödigt att begära eller skaffa en bedömning, varvid myndigheten ska genomföra en självbedömning.

3 c §

Påvisande av att kraven uppfylls

En myndighet kan begära godkännande av en bedömningsmyndighet för sitt informationssystem eller sin datakommunikation för att visa att kraven på informationssäkerhet uppfylls

1) i situationer som avses i lagen om internationella förpliktelser som gäller informationssäkerhet eller som avses i internationella förpliktelser som gäller informationssäkerhet enligt den lagen,

2) om annat internationellt samarbete än sådant som avses i 1 punkten förutsätter det, eller

3) om det föreskrivs särskilt om påvisande av överensstämmelse med kraven.

3 d §

Bedömningsmyndigheter

Behörig bedömningsmyndighet är Transport- och kommunikationsverket. Om

Gällande lydelse	*Föreslagen lydelse*
	bedömningen gäller informationssäkerheten i och beredskapen hos Försvarsmaktens informationssystem eller datakommunikation eller tillhörande säkerhetskritiska lösningar, är behörig bedömningsmyndighet den utsedda säkerhetsmyndigheten vid Huvudstaben som avses i 4 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet. *De bedömningsuppgifter som hör till den utsedda säkerhetsmyndigheten vid Huvudstaben kan också skötas av en person som hör till Försvarsmaktens avlönade personal och som av säkerhetsmyndigheten har utsetts till uppgiften och vars verksamhet styrs och övervakas av säkerhetsmyndigheten.* *Bedömningsmyndigheterna ska till sin organisation och sitt beslutsfattande vara oberoende vid skötseln av bedömningsuppgifterna. Dessutom ska bedömningsmyndigheterna säkerställa att dess anställda eller personer som agerar för dess räkning har tillräcklig utbildning och erfarenhet med tanke på bedömningsuppgiftens art och omfattning.*
4 §	4 §
Kommunikationsverkets uppgifter	*Bedömningsmyndigheternas uppgifter*
Kommunikationsverket ska i syfte att främja och säkerställa informationssäkerheten i myndigheternas informationssystem och datakommunikation 1)på en myndighets begäran göra en bedömning av överensstämmelse med kraven på informationssäkerhet i fråga om informationssystem eller datakommunikation som myndigheten bestämmer över eller planerar att skaffa, 2)på det sätt som föreskrivs i 8 § utfärda ett intyg som visar att informationssystemet eller datakommunikationen har godkänts, 3)på finansministeriets begäran göra utredningar om den allmänna nivån på informationssäkerheten i informationssystem eller datakommunikation som en statsförvaltningsmyndighet bestämmer över. En begäran enligt 1 mom. 1 och 2 punkten får på uppdrag av en myndighet också framställas av den som för myndighetens	*Bedömningsmyndigheterna har till uppgift att på begäran av en myndighet bedöma informationssäkerheten i och beredskapen hos myndighetens informationssystem och datakommunikation och tillhörande säkerhetskritiska lösningar.* *Utöver vad som föreskrivs i 1 mom. ska Transport- och kommunikationsverket* *1) på ansökan av en tillverkare av säkerhetskritiska lösningar som är etablerad i Finland göra en bedömning av huruvida en i Finland tillverkad säkerhetskritisk lösning och dess tillverkning överensstämmer med kraven på informationssäkerhet,* *2) ge rådgivning om informationssäkerhetsåtgärder och bedömning av informationssäkerheten i fråga om informationssystem, datakommunikation och säkerhetskritiska lösningar, och* *3) styra och övervaka verksamheten hos tillverkare av säkerhetskritiska lösningar som*

Gällande lydelse

räkning sköter anskaffningar eller tillhandahåller databehandlings- eller datakommunikationstjänster eller sköter serviceuppgifter med anknytning till ordnandet av dem.

Kommunikationsverket utför de uppgifter som avses i denna lag inom ramen för de resurser som står till buds och med beaktande av uppfyllandet av internationella förpliktelser som gäller informationssäkerhet och de begärda åtgärdernas betydelse för en allmän förbättring av informationssäkerheten i myndigheternas informationssystem och datakommunikation.

Föreslagen lydelse

tillverkar lösningar för skydd mot informationsläckage via diffus strålning och som har fått ett beslut om godkännande som avses i 8 § 3 mom., och vid behov meddela beslut om krav på tillverkningsåtgärder eller på lösningen.

Transport- och kommunikationsverket ska sätta de uppgifter som i denna lag föreskrivs för verket i egenskap av bedömningsmyndighet i prioritetsordning och sköta uppgifterna i enlighet med de resurser som står till dess förfogande. Transport- och kommunikationsverket kan genom sitt beslut låta bli att utföra en bedömning som begärts av verket eller åta sig att utföra endast en partiell bedömning. Vid prioriteringen av uppgifterna och i beslutet ska hänsyn tas till

1) iakttagande av internationella förpliktelser som gäller informationssäkerhet,

2) myndigheternas bedömningsskyldigheter enligt 3 a och 3 b §,

3) informationens säkerhetsklass,

4) tillgången till annan oberoende bedömning än den bedömning som Transport- och kommunikationsverket utför,

5) främjande av utbudet av finländska säkerhetskritiska lösningar,

6) likabehandling av dem som begär och ansöker om bedömning, och

7) vilken allmän betydelse de begärda åtgärderna har när det gäller att allmänt förbättra informationssäkerheten i myndigheternas informationssystem och datakommunikation eller att skydda samhällets vitala funktioner.

En i 1 mom. avsedd begäran till Transport- och kommunikationsverket får på uppdrag av en myndighet också framställas av den som för myndighetens räkning sköter anskaffningar eller tillhandahåller databehandlings- eller datakommunikationstjänster eller sköter serviceuppgifter med anknytning till ordnandet av dem.

4 a §

Uppgifter för att bistå bedömningsmyndigheterna

Gällande lydelse	*Föreslagen lydelse*
	Bedömningsmyndigheterna kan anlita utomstående sakkunniga som hjälp vid bedömningen, om det är nödvändigt på grund av bedömningens art, de tillgängliga resurserna eller tekniska skäl som hänför sig till bedömningen. De utomstående sakkunniga ska ha tillräcklig utbildning och erfarenhet med tanke på bedömningsuppgiftens art och omfattning. På utomstående sakkunniga tillämpas bestämmelserna om straffrättsligt tjänsteansvar när de sköter uppgifter enligt denna paragraf. Bestämmelser om skadeståndsansvar finns i skadeståndslagen (412/1974). *Teknologiska forskningscentralen VTT Ab har till uppgift att på uppdrag av en bedömningsmyndighet bedöma säkerhetskritiska lösningar. På anställda vid Teknologiska forskningscentralen VTT Ab tillämpas vad som i 1 mom. föreskrivs om utomstående sakkunniga.*
	4 b §
	Informationsutbyte och samarbete mellan bedömningsmyndigheterna
	Bedömningsmyndigheterna ska samarbeta när det gäller skötseln av uppgifter enligt denna lag och trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter lämna varandra sådana uppgifter som är nödvändiga för detta ändamål. *Trots bestämmelserna i 3 d § 1 mom. och 4 § 1 och 2 mom. kan bedömningsmyndigheterna avtala om att sköta enskilda i denna lag avsedda uppgifter eller en del av uppgifterna för en annan bedömningsmyndighets räkning, om arrangemanget behövs för att uppgifterna ska kunna skötas på ett ändamålsenligt, ekonomiskt och snabbt sätt.* *Transport- och kommunikationsverket svarar för styrningen av samarbetet mellan bedömningsmyndigheterna med syfte att skapa en enhetlig tillämpningspraxis.*
5 §	5 §

Gällande lydelse

Utredningar på uppdrag av finansministeriet

För att följa verkställigheten av bestämmelserna om informationssäkerhet inom statsförvaltningen och för att utveckla dem kan finansministeriet be Kommunikationsverket göra en utredning om den allmänna nivån på informationssäkerheten i statsförvaltningsmyndigheternas informationssystem eller datakommunikation. De informationssystem som utredningen ska omfatta kan utses utgående från informationssystemens användningsändamål, arten av de uppgifter som registreras eller någon annan motsvarande allmän omständighet.
Den bedömning som Kommunikationsverket lämnar till finansministeriet får oberoende av sekretessbestämmelserna innehålla de uppgifter som är nödvändiga för att bedömningens syfte ska kunna uppnås.

6 §

Kommunikationsverkets rätt att få uppgifter och rätt att få tillträde till lokaler och informationssystem

Kommunikationsverket och sakkunniga som handlar på uppdrag av verket har oberoende av bestämmelserna om sekretessbelagda uppgifter rätt att få tillgång till uppgifterna om de informationssystem och den datakommunikation som Kommunikationsverket ska bedöma eller som är föremål för utredning samt, i den utsträckning det behövs för bedömningens utförande, att få tillträde till informationssystemet och till lokaler där uppgifter som ingår i systemet behandlas.
Inspektioner som avses i 1 mom. får inte utföras i utrymmen som används för permanent boende.

Föreslagen lydelse

Utredningar på uppdrag av finansministeriet

För att följa verkställigheten av bestämmelserna om informationssäkerhet inom statsförvaltningen och för att utveckla bestämmelserna kan finansministeriet be *Transport- och kommunikationsverket* göra utredningar om den allmänna nivån på informationssäkerheten i och beredskapen hos statsförvaltningsmyndigheternas informationssystem eller datakommunikation. De informationssystem som en utredning ska omfatta kan utses utgående från informationssystemens användningsändamål, arten av de uppgifter som registreras eller något annat motsvarande *allmänt kriterium.*
Den utredning som Transport- och kommunikationsverket lämnar till finansministeriet får oberoende av sekretessbestämmelserna *och andra begränsningar som gäller utlämnande av uppgifter* innehålla de uppgifter som är nödvändiga för att utredningens syfte ska kunna uppnås.

6 §

***Bedömningsmyndigheternas** rätt att få uppgifter, **inspektionsrätt** och rätt att få tillträde till lokaler och informationssystem*

Bedömningsmyndigheterna och i 4 a § avsedda utomstående sakkunniga som bistår bedömningsmyndigheterna har rätt att trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter få tillgång till uppgifter, handlingar, utrustning och program som hänför sig till informationssystem, datakommunikation eller säkerhetskritiska lösningar eller tillverkningen av dem och som är nödvändiga för att de ska kunna utföra sina uppgifter enligt denna lag och att i den utsträckning det är nödvändigt för att utföra uppgifterna få tillträde till informationssystem och datakommunikationer samt till lokaler där uppgifter som hör till föremålet för bedömningen behandlas samt att utföra

Gällande lydelse	*Föreslagen lydelse*
	behövliga administrativa och tekniska bedömningsåtgärder. *Transport- och kommunikationsverket har rätt att utföra inspektioner i lokalerna hos en tillverkare av lösningar för skydd mot informationsläckage via diffus strålning och hos dennes underleverantörer för att utreda om tillverkaren och dennes underleverantör iakttar de beslut som meddelats med stöd av denna lag. Den utsedda säkerhetsmyndigheten vid Huvudstaben har rätt att utföra sådana inspektioner som avses ovan, om den sköter en uppgift för Transport- och kommunikationsverkets räkning på det sätt som avses i 4 b § 2 mom. Vid inspektionerna kan Transport- och kommunikationsverket och den utsedda säkerhetsmyndigheten vid Huvudstaben biträdas av sådana utomstående sakkunniga som avses i 4 a §. På den rätt som Transport- och kommunikationsverket, den utsedda säkerhetsmyndigheten vid Huvudstaben och utomstående sakkunniga har att få tillträde till lokaler och få granska nödvändiga uppgifter och att utföra bedömningsåtgärder tillämpas vad som föreskrivs i 1 mom. Vid inspektioner ska 39 § i förvaltningslagen (434/2003) iakttas.* *Inspektioner som avses i 1 och 2 mom. får inte utföras i utrymmen som används för permanent boende.*
7 §	7 §
Bedömningsgrunder för informationssäkerhet	*Bedömningsgrunder för informationssäkerhet* ***och beredskap***
Som bedömningsgrunder för informationssäkerheten i myndigheternas informationssystem och datakommunikation kan Kommunikationsverket använda 1)i lag eller förordning föreskrivna krav på informationssäkerheten i myndigheternas verksamhet samt finansministeriets anvisningar om informationssäkerhet, 2)anvisningar om uppfyllande av internationella informationssäkerhetsförpliktelser som meddelats av den nationella säkerhetsmyndighet som avses i lagen om	Som bedömningsgrunder för informationssäkerheten i *och beredskapen hos* informationssystem och datakommunikation *samt som bedömningsgrunder för informationssäkerheten i säkerhetskritiska lösningar och vid tillverkningen av dem kan användas* 1) i lag eller förordning föreskrivna krav på informationssäkerhet, *cybersäkerhet eller beredskap som gäller myndigheternas verksamhet samt myndigheternas anvisningar om tillämpningen av kraven,*

Gällande lydelse

internationella förpliktelser som gäller informationssäkerhet,

3)Europeiska unionens eller något annat internationellt organs bestämmelser och anvisningar om informationssäkerhet,

4)publicerade allmänt eller regionalt tillämpade bestämmelser, föreskrifter eller anvisningar om informationssäkerhet,

5)informationssäkerhetskrav som ingår i en fastställd standard.

Kommunikationsverket utreder om informationssystemet eller datakommunikationen uppfyller de krav angående informationssäkerheten som utgör bedömningsgrunder. Bedömningen kan även vara partiell.

Föreslagen lydelse

2) *Europeiska unionens, Nordatlantiska fördragsorganisationens eller något annat internationellt organs bestämmelser, föreskrifter och anvisningar om informationssäkerhet, cybersäkerhet eller beredskap samt myndigheternas anvisningar om tillämpningen av dem,*

3) publicerade allmänt eller regionalt tillämpade bestämmelser, föreskrifter eller anvisningar om informationssäkerhet, cybersäkerhet eller beredskap,

4) krav som gäller informationssäkerhet, cybersäkerhet eller beredskap och som ingår i en fastställd standard.

Vid fastställandet av bedömningsgrunderna och föremålet för bedömningen ska de föreskrivna kraven på informationssäkerheten i och beredskapen hos informationssystemet och datakommunikationen och de krav som valts utifrån en riskbedömning beaktas. Bedömningsmyndigheterna fastställer bedömningsgrunderna för en bedömning de ska utföra efter att ha hört den som begär bedömningen.

Bedömningsmyndigheterna fastställer bedömningsgrunderna för en säkerhetskritisk lösning efter att ha hört tillverkaren av den säkerhetskritiska lösningen. Utöver vad som föreskrivs i 1 och 2 mom. ska informationens säkerhetsklass, säkerheten vid tillverkningen samt beredskapen att uppfylla internationella förpliktelser som gäller informationssäkerhet beaktas när bedömningsgrunderna för säkerhetskritiska lösningar fastställs.

7 a §

Utredningar som hänför sig till bedömningar av tillverkare av säkerhetskritiska lösningar

Transport- och kommunikationsverket ska vid en i 4 § 2 mom. 1 punkten avsedd bedömning av en säkerhetskritisk lösning och av dess tillverkning ansöka om en i säkerhetsutredningslagen avsedd säkerhetsutredning av företag i fråga om den tillverkare som ansöker om bedömningen. Godkännandet av en säkerhetskritisk lösning förutsätter att det i den säkerhetsutredning av företag som gäller tillverkaren inte har

Gällande lydelse	*Föreslagen lydelse*
	framkommit något som utifrån en helhetsbedömning skulle äventyra tillverkningens säkerhet och tillförlitlighet i synnerhet med hänsyn till riskerna för utländsk påverkan.
	Om en fastställd internationell standard används som en del av bedömningsgrunderna avseende tillverkningen av en säkerhetskritisk lösning, kan överensstämmelse med standarden påvisas på det sätt som anges i lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (920/2005).
8 §	8 §
Utfärdande av intyg	*Utfärdande av* ***bedömningsrapport, beslut om godkännande och utlåtande om godkännande***
Kommunikationsverket kan på begäran utfärda intyg över informationssystem eller datakommunikation som uppfyller kraven på informationssäkerhet. I intyget antecknas bedömningsgrunderna och uppgifter om bedömningens omfattning samt vid behov uppgift om intygets giltighetstid.	*I fråga om bedömningen av informationssäkerheten i och beredskapen hos ett informationssystem och hos datakommunikation ska det utarbetas en bedömningsrapport i vilken ska antecknas uppgifter om föremålet för bedömningen, vilka bedömningsgrunder som använts, bedömningens omfattning och de observationer som gjorts.*
Intyg kan utfärdas för viss tid, om det finns särskilda skäl till det.	*Utöver vad som föreskrivs i 1 mom. ska bedömningsmyndigheten på en i 3 c § avsedd begäran meddela ett beslut om godkännande eller ge ett utlåtande om godkännande i fråga om en myndighets informationssystem eller datakommunikation, om informationssystemet eller datakommunikationen uppfyller kraven. I beslutet eller utlåtandet ska det antecknas uppgifter om föremålet för bedömningen, vilka bedömningsgrunder som använts, bedömningens omfattning, resultaten av bedömningen och kvarstående risk samt vid behov uppgift om giltighetstiden.*
	Utöver vad som föreskrivs i 1 mom. ska Transport- och kommunikationsverket i fråga om en i 4 § 2 mom. 1 punkten avsedd ansökan om bedömning av informationssäkerheten i en säkerhetskritisk lösning och av informationssäkerheten vid dess tillverkning meddela ett beslut av vilket resultatet av bedömningen framgår. Av beslutet om

Gällande lydelse	*Föreslagen lydelse*
	godkännande ska giltighetstiden för godkännandet framgå, och i beslutet kan ingå sådana begränsningar och villkor som behövs för en säker användning av lösningen. I ett beslut om godkännande som gäller en tillverkare av en säkerhetskritisk lösning som tillverkar lösningar för skydd mot informationsläckage via diffus strålning kan ingå sådana villkor som behövs för att säkerställa att tillverkningen är tillförlitlig.
8 a §	8 a §
Myndighetens skyldighet att skaffa intyg	***Förteckning över godkända säkerhetskritiska lösningar och tillverkare***
Genom förordning av statsrådet får det föreskrivas att ett intyg som avses i 8 § ska skaffas i fråga om informationssystem eller datakommunikation som en statsförvaltningsmyndighet bestämmer över och där handlingar som hör till säkerhetsklass I eller II behandlas.	*Transport- och kommunikationsverket för en offentlig förteckning över säkerhetskritiska lösningar och tillverkare av säkerhetskritiska lösningar som fått ett beslut om godkännande i enlighet med 8 § 3 mom. Av förteckningen ska framgå* *1) namnet på den säkerhetskritiska lösningen, dess användningsändamål och version,* *2) den informationssäkerhetsklass för vilken lösningen konstaterats ge ett tillräckligt skydd,* *3) tillverkaren av den säkerhetskritiska lösningen,* *4) godkännandets giltighet samt ändring eller upphörande av godkännandet, och* *5) de villkor och begränsningar för en säker användning som hänför sig till godkännandet.*
8 b §	
Införande av uppgifter i registret över säkerhetsutredningar och avförande av anteckning	
Kommunikationsverket får föra in uppgifter enligt 8 § ur intyg som det utfärdat i det register över säkerhetsutredningar som avses i säkerhetsutredningslagen. Kommunikationsverket ska avföra en sådan anteckning inom sex månader efter det att den tid som angetts i intyget har löpt ut. En sådan anteckning avförs inom en månad efter det att	(upphävs)

Gällande lydelse	*Föreslagen lydelse*
ett avgörande om återkallelse av ett intyg har vunnit laga kraft.	
9 §	9 §
Upprätthållande och uppföljning av informationssäkerhetsnivån	*Upprätthållande och uppföljning av informationssäkerheten*
Den som önskar få ett intyg som avses i 8 § ska förbinda sig att upprätthålla informationssäkerhetsnivån. Den som fått ett intyg ska underrätta Kommunikationsverket om sådana ändringar som inverkar på informationssäkerhetsnivån och ge Kommunikationsverket tillträde till informationssystemen och datakommunikationen för utredande av om dessa alltjämt uppfyller de krav som anges i intyget.	*Den som fått ett beslut eller utlåtande enligt 8 § ska upprätthålla informationssäkerheten i enlighet med utlåtandet eller beslutet. Den som fått ett beslut eller utlåtande ska underrätta bedömningsmyndigheten om sådana ändringar som kan inverka på de krav som anges i beslutet eller utlåtandet.*
10 §	10 §
Återkallelse av intyg	*Återkallande av beslut om godkännande eller utlåtande om godkännande*
Kommunikationsverket kan återkalla ett intyg som utfärdats med stöd av denna lag, om det informationssystem eller den datakommunikation som bedömningen har gällt inte längre uppfyller de krav som har utgjort en förutsättning för utfärdande av intyget. Innan Kommunikationsverket träffar ett avgörande som avses i 1 mom. ska verket höra innehavaren av intyget och ge denne tillfälle att avhjälpa bristen. Kommunikationsverket kan i sitt beslut enligt 1 mom. bestämma att beslutet ska iakttas även om det överklagas, om inte besvärsmyndigheten bestämmer något annat.	*Bedömningsmyndigheten kan helt eller delvis återkalla ett utlåtande eller beslut som avses i 8 §, om det informationssystem, den datakommunikation eller den säkerhetskritiska lösning eller den tillverkare av en säkerhetskritisk lösning som bedömningen har gällt inte längre uppfyller de krav som har utgjort en förutsättning för meddelande av beslutet eller givande av utlåtandet.* Innan *bedömningsmyndigheten i enlighet med 1 mom. återkallar ett utlåtande eller beslut ska myndigheten höra den som fått beslutet eller utlåtandet* och ge denne tillfälle att avhjälpa bristen. *Bedömningsmyndigheten kan i det* beslut *om återkallande som avses i 1 mom. bestämma att beslutet ska iakttas även om det överklagas,* om inte besvärsmyndigheten bestämmer något annat.
11 §	11 §
Ändringssökande	*Ändringssökande*

Gällande lydelse

I fråga om sökande av ändring i beslut som Kommunikationsverket har meddelat med stöd av denna lag gäller vad som föreskrivs i förvaltningsprocesslagen (586/1996).

12 §

Avgifter

I fråga om avgifter för Kommunikationsverkets bedömning, utfärdande av intyg och utredning som tas ut hos den som inlett ärendet gäller vad som föreskrivs i lagen om grunderna för avgifter till staten (150/1992) och i bestämmelser som utfärdats med stöd av den lagen.

Föreslagen lydelse

I fråga om sökande av ändring i beslut som *bedömningsmyndigheten* har meddelat med stöd av denna lag gäller vad som föreskrivs i *lagen om rättegång i förvaltningsärenden (808/2019).*

12 §

Avgifter

För bedömningsmyndighetens bedömning samt för en bedömningsrapport, ett utlåtande eller ett beslut och för rådgivning och utredning tas det hos den som inlett ärendet ut en avgift med iakttagande av vad som föreskrivs i lagen om grunderna för avgifter till staten (150/1992).

Denna lag träder i kraft den 2026 .

Statsförvaltningsmyndigheterna ska se till att bedömningen av informationssäkerheten i och beredskapen hos deras informationssystem och datakommunikation motsvarar det som föreskrivs i 3 a § inom fem år från ikraftträdandet av denna lag, dock så att bedömningen ska motsvara det som föreskrivs i 2 mom. 1 punkten i den paragrafen inom två år från ikraftträdandet och det som föreskrivs i 2 punkten inom tre år från ikraftträdandet.

Andra än statsförvaltningsmyndigheter ska se till att bedömningen av informationssäkerheten i och beredskapen hos deras informationssystem och datakommunikation motsvarar det som föreskrivs i 3 b § 1 mom. inom två år från ikraftträdandet av denna lag och det som föreskrivs i 2 mom. i den paragrafen inom tre år från ikraftträdandet.

Ett intyg över överensstämmelse med kraven på informationssäkerhet som har utfärdats i enlighet med de bestämmelser som gällde vid ikraftträdandet av denna lag motsvarar det beslut som avses i 8 § och är giltigt under den tid som anges i intyget.

2.

Lag

om ändring av lagen om bedömningsorgan för informationssäkerhet

I enlighet med riksdagens beslut

ändras i lagen om bedömningsorgan för informationssäkerhet (1405/2011) 1 kap., 3 § 1 mom., 4–8 §, rubriken för 3 kap., 9–13 och 13 a §, av dem 4 § sådan den lyder delvis ändrad i lag 727/2014 och 13 a § sådan den lyder i lag 727/2014, samt

fogas till lagen en ny 9 a § som följer:

Gällande lydelse	*Föreslagen lydelse*
1 kap.	1 kap.
Allmänna bestämmelser	**Allmänna bestämmelser**
1 §	1 §
Lagens syfte	*Lagens syfte*
I denna lag finns bestämmelser om ett förfarande genom vilket företag tillförlitligt kan visa en utomstående att de i sin verksamhet har sörjt för en viss informationssäkerhetsnivå.	*Denna lag innehåller* bestämmelser om ett förfarande genom vilket *myndigheter kan skaffa en oberoende bedömning av informationssäkerheten och beredskapen och genom vilket företag tillförlitligt kan visa en utomstående att de i sin verksamhet har sörjt för en viss informationssäkerhetsnivå.*
2 §	2 §
Lagens tillämpningsområde	*Lagens tillämpningsområde*
Denna lag tillämpas på näringsidkare och på enheter som tillhandahåller serviceuppgifter för den offentliga förvaltningen och som på uppdrag bedömer informationssäkerhetens nivå (bedömningsorgan för informationssäkerhet) och vill att Kommunikationsverket ska godkänna deras verksamhet. Lagen tillämpas dessutom på godkännandeförfarandet. I fråga om Kommunikationsverkets uppgifter vid bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation samt vid uppgörande av säkerhetsutredningar	Denna lag tillämpas på näringsidkare och på enheter som tillhandahåller serviceuppgifter för den offentliga förvaltningen och som på uppdrag bedömer *nivån på* informationssäkerheten *eller på beredskapen hos informationssystem eller datakommunikation* (*bedömningsorgan för informationssäkerhet*) och som vill att Transport- och kommunikationsverket ska godkänna deras verksamhet. Lagen tillämpas dessutom på godkännandeförfarandet. I fråga om bedömningsmyndigheternas uppgifter vid bedömning av informationssäkerheten i och beredskapen hos myndigheternas informationssystem och

Gällande lydelse

som gäller sammanslutningar föreskrivs särskilt.

3 §

Ansökan om godkännande av bedömningsorgan

Bedömningsorgan för informationssäkerhet kan ansöka hos Kommunikationsverket om godkännande för sin verksamhet.

— — — — — — — — — — — — — —

4 §

Behandlingen av ansökan

Innan ett bedömningsorgan för informationssäkerhet godkänns ska Kommunikationsverket ge skyddspolisen tillfälle att yttra sig om tillförlitligheten hos bedömningsorganets ansvariga personer och om säkerheten i bedömningsorganets lokaler. När skyddspolisen sammanställer sitt utlåtande ska den iaktta det som föreskrivs i säkerhetsutredningslagen (726/2014).

När ansökan behandlas kan Kommunikationsverket inhämta utlåtanden och ge utomstående sakkunniga i uppdrag att utföra uppgifter som anknyter till bedömningen av ansökan och av uppgifter som ingår i den.

Föreslagen lydelse

datakommunikation samt vid uppgörande av säkerhetsutredningar av företag föreskrivs särskilt.

3 §

Ansökan om godkännande av bedömningsorgan

Bedömningsorgan för informationssäkerhet kan ansöka hos Transport- och kommunikationsverket om godkännande för sin verksamhet och för kompetensområdet för bedömningen.

— — — — — — — — — — — — — —

4 §

Behandlingen av ansökan

Innan ett bedömningsorgan för informationssäkerhet godkänns ska *Transport- och kommunikationsverket* ge skyddspolisen tillfälle att yttra sig om tillförlitligheten hos bedömningsorganets ansvariga personer och om säkerheten i bedömningsorganets lokaler. *Om ansökan gäller kompetensområdet för bedömning av hanteringen av säkerhetsklassificerad information, ska Transport- och kommunikationsverket för att säkerställa företagets och dess ansvarspersoners tillförlitlighet och förmåga att sköta sina åtaganden ansöka om en i säkerhetsutredningslagen (726/2014) avsedd säkerhetsutredning av företaget i fråga. När skyddspolisen sammanställer sitt utlåtande eller gör utredningen ska den iaktta det som föreskrivs i säkerhetsutredningslagen.*

När Transport- och kommunikationsverket behandlar en ansökan kan verket inhämta utlåtanden av myndigheterna samt anlita utomstående sakkunniga för biträdande uppgifter i anknytning till bedömningen av ansökan och av uppgifter som ingår i den. På utomstående sakkunniga tillämpas bestämmelserna om straffrättsligt tjänsteansvar när de sköter uppgifter enligt denna paragraf. Bestämmelser om

Gällande lydelse	*Föreslagen lydelse*
	skadeståndsansvar finns i skadeståndslagen (412/1974).
5 §	5 §
Godkännande av bedömningsorgan	*Godkännande av bedömningsorgan*
För att ett bedömningsorgan för informationssäkerhet ska godkännas krävs det att	För att ett bedömningsorgan för informationssäkerhet ska godkännas krävs det att
1)organet är funktionellt och ekonomiskt oberoende av den som bedömningen gäller,	1) organet är funktionellt och ekonomiskt oberoende av den som bedömningen gäller,
2)organets personal har god teknisk och yrkesinriktad utbildning samt tillräckligt omfattande erfarenhet av de uppgifter som ingår i verksamheten,	2) organets personal har god teknisk och yrkesinriktad utbildning samt tillräckligt omfattande erfarenhet av de uppgifter som ingår i verksamheten,
3)organet har den utrustning, de hjälpmedel och de system som behövs i verksamheten,	3) organet har den utrustning, de hjälpmedel och de system som behövs i verksamheten,
4)tillförlitligheten hos de ansvariga personerna inom organet har säkerställts och organet har en övervakad metod som bedömts som tillförlitlig och med vars hjälp säkerheten i organets lokaler och databehandling säkerställs,	4*) det i den säkerhetsutredning av företag som gäller organet inte har framkommit någon sådan omständighet som utifrån en helhetsbedömning skulle äventyra företagets och dess ansvarspersoners tillförlitlighet och förmåga att sköta sina åtaganden i fråga om bedömningsuppgiften, eller att tillförlitligheten hos de ansvariga personerna inom organet har säkerställts och organet har en övervakad metod som bedömts som tillförlitlig och med vars hjälp säkerheten i organets lokaler och databehandling samt personalens tillförlitlighet säkerställs,*
5)organet har ändamålsenliga anvisningar för sin verksamhet och uppföljningen av den.	5) organet har ändamålsenliga anvisningar för sin verksamhet och uppföljningen av den.
Uppfyllandet av kraven i 1 mom. 1–3 punkten ska visas på det sätt som anges i lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (920/2005).	Uppfyllandet av kraven i 1 mom. 1–3 punkten ska visas på det sätt som anges i lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (920/2005).
	Trots vad som föreskrivs i 2 mom. kan Transport- och kommunikationsverket, när ett godkänt bedömningsorgan ansöker om godkännande för ett nytt kompetensområde, efter att ha hört de myndigheter som är centrala när det gäller godkännandet av kompetensen besluta att kraven anses vara uppfyllda.
Utifrån de utredningar som Kommunikationsverket har mottagit eller utfört och de inspektioner som verket har förrättat godkänner verket ett organ där kraven uppfylls som ett godkänt bedömningsorgan för informationssäkerhet. Ett sådant organ får i sin marknadsföring och sin övriga kommunikation använda ett uttryck för Kommunikationsverkets godkännande, förutsatt att godkännandets giltighetstid inte har löpt ut eller att Kommunikationsverket inte har beslutat att återkalla godkännandet.	Utifrån de utredningar som *Transport- och kommunikationsverket* har mottagit eller utfört och de inspektioner som verket har förrättat godkänner verket ett organ där
Ett bedömningsorgan kan godkännas för viss tid, om det finns särskilda skäl till detta. I ett beslut om godkännande kan det ingå begränsningar och villkor som gäller bedömningsorganets kompetensområde, tillsyn och verksamhet och som behövs för att	

Gällande lydelse

säkerställa att bedömningsorganet sköter sina uppgifter.

6 §

Återkallelse av godkännande av bedömningsorgan

Om ett godkänt bedömningsorgan för informationssäkerhet i väsentlig grad eller fortlöpande handlar i strid med bestämmelserna eller om det inte längre uppfyller kraven för godkännande, ska Kommunikationsverket uppmana bedömningsorganet att avhjälpa bristen inom utsatt tid. Om bristen inte avhjälps inom utsatt tid, kan Kommunikationsverket återkalla godkännandet.

Kommunikationsverket kan i sitt beslut bestämma att beslutet ska iakttas även om det överklagas, om inte besvärsmyndigheten bestämmer något annat.

7 §

Kommunikationsverkets inspektionsrätt

Kommunikationsverket och sakkunniga som handlar på uppdrag av verket har rätt att inspektera lokaler som de bedömningsorgan för informationssäkerhet som ansökt om

Föreslagen lydelse

kraven uppfylls som ett godkänt bedömningsorgan för informationssäkerhet. Ett sådant organ får i sin marknadsföring och sin övriga kommunikation använda ett uttryck för *Transport- och kommunikationsverkets* godkännande, förutsatt att godkännandets giltighetstid inte har löpt ut eller att *Transport- och kommunikationsverket* inte har beslutat att återkalla godkännandet.

Ett bedömningsorgan kan godkännas för viss tid, om det finns särskilda skäl till detta. I ett beslut om godkännande kan det ingå begränsningar och villkor som gäller bedömningsorganets kompetensområde, tillsyn och verksamhet och som behövs för att säkerställa att bedömningsorganet sköter sina uppgifter.

6 §

Återkallelse av godkännande av bedömningsorgan

Om ett godkänt bedömningsorgan för informationssäkerhet i väsentlig grad eller fortlöpande handlar i strid med bestämmelserna eller om det inte längre uppfyller kraven för godkännande, ska *Transport- och kommunikationsverket* uppmana bedömningsorganet att avhjälpa bristen inom utsatt tid. Om bristen inte avhjälps inom utsatt tid, kan Transport- och kommunikationsverket återkalla godkännandet av bedömningsorganet eller kompetensområdet.

Transport- och kommunikationsverket kan i sitt beslut bestämma att beslutet ska iakttas även om det överklagas, om inte besvärsmyndigheten bestämmer något annat.

7 §

Transport- och kommunikationsverkets rätt att få information och dess inspektionsrätt

Transport- och kommunikationsverket har rätt att inspektera lokalerna hos ett bedömningsorgan för informationssäkerhet som *ansöker* om godkännande eller som *är godkänt och hos en i 9 a § avsedd*

Gällande lydelse

godkännande förfogar över, eller som godkända bedömningsorgan förfogar över, och de metoder som bedömningsorganen använder. Inspektion får inte utföras i utrymmen som används för permanent boende.

8 §

Bedömningsorganens upplysnings- och anmälningsskyldighet

Ett godkänt bedömningsorgan för informationssäkerhet ska underrätta Kommunikationsverket om sådana ändringar i sin verksamhet som har betydelse för de skyldigheter som organet har.

Utöver vad som föreskrivs i 1 mom. har Kommunikationsverket rätt att av bedömningsorganet på begäran få de upplysningar som behövs för tillsyn över att organet uppfyller kraven på dess verksamhet.

3 kap.

Bedömning av informationssäkerheten

9 §

Bedömningsorganens uppgifter

Föreslagen lydelse

underleverantör till bedömningsorganet samt att granska de metoder som bedömningsorganet använder. Vid inspektionerna kan Transport- och kommunikationsverket biträdas av sådana utomstående sakkunniga som avses i 4 § 2 mom. Inspektioner får inte utföras i utrymmen som används för boende av permanent natur.

Transport- och kommunikationsverket har trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av uppgifter rätt att av skyddspolisen, den nationella ackrediteringsenheten, den myndighet som styr eller övervakar tillämpningen av bedömningsgrunden för kompetensområdet, bedömningsorganet samt dess underleverantörer och kunder på begäran få de uppgifter som är nödvändiga för tillsynen över att ett bedömningsorgan för informationssäkerhet uppfyller de krav som ställs på dess verksamhet.

8 §

Bedömningsorganens anmälningsskyldighet

Ett godkänt bedömningsorgan för informationssäkerhet ska underrätta *Transport- och kommunikationsverket* om sådana ändringar i sin verksamhet som är av betydelse med tanke på de skyldigheter som organet har.

3 kap.

Bedömning av informationssäkerhet och beredskap

9 §

Bedömningsorganens uppgifter

När ett godkänt bedömningsorgan för informationssäkerhet har fått i uppdrag att utföra en bedömning av

Gällande lydelse

När ett godkänt bedömningsorgan för informationssäkerhet har fått i uppdrag att utföra en bedömning av informationssäkerheten ska det iaktta omsorg och se till att

1)lokalerna hos den som bedömningen gäller granskas under bedömningen,

2) det under bedömningen klarläggs om den som bedömningen gäller i sin verksamhet på behörigt sätt har uppfyllt de krav angående informationssäkerheten som anges i 10 § och som ligger till grund för utredningen (bedömningsgrunder för informationssäkerhet).

Bedömningen kan även vara partiell.

Det godkända bedömningsorganet för informationssäkerhet utfärdar på basis av utredningarna och granskningen ett intyg, om lokalerna och verksamheten hos den som bedömningen gäller är förenliga med de bedömningsgrunder som legat till grund för utredningen. De grunder för bedömning av informationssäkerheten som använts vid bedömningen och bedömningens omfattning ska specificeras i intyget.

Föreslagen lydelse

informationssäkerheten *och beredskapen* ska det iaktta omsorg och se till att

1) lokalerna hos den som bedömningen gäller *vid behov inspekteras,*

2) det under bedömningen *utreds* om den som bedömningen gäller i sin verksamhet på behörigt sätt har uppfyllt de *i 10 § angivna kraven som gäller för informationssäkerheten eller beredskapen och som ligger till grund för utredningen* (*bedömningsgrunder för informationssäkerhet och beredskap*).

Bedömningen kan även vara partiell.

Ett godkänt bedömningsorgan för informationssäkerhet ska utarbeta en bedömningsrapport i vilken antecknas uppgifter om föremålet för bedömningen, vilka bedömningsgrunder som använts, bedömningens omfattning och de observationer som gjorts.

Ett godkänt bedömningsorgan för informationssäkerhet kan på begäran, eller, om det särskilt föreskrivs om det, på basis av utredningar och inspektioner utfärda ett intyg, om föremålet för bedömningen är förenligt med de bedömningsgrunder för informationssäkerhet och beredskap som legat till grund för utredningen. De grunder för bedömning av informationssäkerheten och beredskapen som använts vid bedömningen samt bedömningens omfattning och giltighetstid ska specificeras i intyget.

9 a §

Underleverantörer

Ett godkänt bedömningsorgan för informationssäkerhet får lägga ut en uppgift i anslutning till bedömningen på underentreprenad till ett annat bolag som hör till samma koncern eller till någon annan underleverantör endast om koncernbolaget eller underleverantören uppfyller förutsättningarna för godkännande av ett bedömningsorgan för informationssäkerhet och en utredning om underentreprenaden har lämnats till Transport- och kommunikationsverket och verket har konstaterat att förutsättningarna uppfylls.

Gällande lydelse

10 §

Bedömningsgrunder för informationssäkerhet

Som bedömningsgrunder för informationssäkerhet kan, enligt beslut av den som bedömningen gäller, vid bedömningar som avses i denna lag användas

1)i lag eller förordning föreskrivna krav på informationssäkerheten i myndigheternas verksamhet samt finansministeriets anvisningar om informationssäkerhet,

2)anvisningar om uppfyllande av internationella informationssäkerhetsförpliktelser som meddelats av den nationella säkerhetsmyndighet som avses i lagen om internationella förpliktelser som gäller informationssäkerhet,

3)Europeiska unionens eller något annat internationellt organs bestämmelser eller anvisningar om informationssäkerhet,

4)publicerade allmänt eller regionalt tillämpade bestämmelser, föreskrifter eller anvisningar om informationssäkerhet,

5)informationssäkerhetskrav som ingår i en fastställd standard.

11 §

Avgifter

I fråga om avgiften för behandlingen av ärenden som gäller godkännande av bedömningsorgan för informationssäkerhet vid Kommunikationsverket gäller vad som föreskrivs i lagen om grunderna för avgifter

Föreslagen lydelse

Ett godkänt bedömningsorgan för informationssäkerhet får lägga ut uppgifter som hänför sig till bedömning av hanteringen av säkerhetsklassificerad information på underentreprenad eller anlita ett dotterbolag för uppgifterna endast om organet avtalat om saken med kunden.

10 §

Bedömningsgrunder för informationssäkerhet och beredskap

Som bedömningsgrunder för informationssäkerhet *och beredskap* kan, enligt beslut av den som bedömningen gäller *och enligt bedömningsorganets godkända kompetensområde*, vid bedömningar som avses i denna lag användas

1) i lag eller förordning föreskrivna krav på informationssäkerhet, *cybersäkerhet eller beredskap som gäller myndigheternas verksamhet samt myndigheternas anvisningar om tillämpningen av kraven,*

2) Europeiska unionens, Nordatlantiska fördragsorganisationens eller något annat internationellt organs bestämmelser, föreskrifter och anvisningar om informationssäkerhet, cybersäkerhet eller beredskap samt myndigheternas anvisningar om tillämpningen av dem,

3) publicerade allmänt eller regionalt tillämpade bestämmelser, föreskrifter eller anvisningar om informationssäkerhet, cybersäkerhet eller beredskap,

4) krav som gäller informationssäkerhet, cybersäkerhet eller beredskap och som ingår i en fastställd standard.

11 §

Avgifter

För behandlingen vid Transport- och kommunikationsverket av ärenden som gäller godkännande av och tillsyn över bedömningsorgan för informationssäkerhet tas det ut en avgift med iakttagande av vad som föreskrivs i lagen om grunderna för avgifter till staten (150/1992).

Gällande lydelse

till staten (150/1992) och i bestämmelser som utfärdats med stöd av den lagen.

12 §

Ändringssökande

I fråga om sökande av ändring i beslut som Kommunikationsverket meddelat med stöd av denna lag gäller vad som föreskrivs i förvaltningsprocesslagen (586/1996).

13 §

Tillämpning av bestämmelser om god förvaltning

När ett godkänt bedömningsorgan för informationssäkerhet utför uppgifter som avses i denna lag ska det iaktta förvaltningslagen (434/2003), lagen om offentlighet i myndigheternas verksamhet (621/1999) *och* språklagen (423/2003).

13 a §

Registrering av uppgifter i registret över säkerhetsutredningar

Kommunikationsverket ska i det register över säkerhetsutredningar som avses i säkerhetsutredningslagen anteckna uppgifter om godkända bedömningsorgan samt uppgifter som ingår i intyg som getts till bedömningsorgan. Återkallelsen av ett

Föreslagen lydelse

12 §

Ändringssökande

I fråga om sökande av ändring i beslut som *Transport- och kommunikationsverket har meddelat* med stöd av denna lag gäller vad som föreskrivs i lagen om rättegång i förvaltningsärenden (808/2019).

13 §

Tillämpning av bestämmelser om tjänsteansvar och god förvaltning

När ett godkänt bedömningsorgan för informationssäkerhet utför *offentliga förvaltningsuppgifter* som avses i denna lag ska det iaktta förvaltningslagen (434/2003), lagen om offentlighet i myndigheternas verksamhet (621/1999), språklagen (423/2003), samiska språklagen (1086/2003*), dataskyddslagen (1050/2018) och lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003)*.

På ansvarspersoner och personer som är anställda vid ett godkänt bedömningsorgan för informationssäkerhet samt på personer som är anställda hos i 9 a § avsedda underleverantörer tillämpas bestämmelserna om straffrättsligt tjänsteansvar när de utför uppgifter enligt denna lag. Bestämmelser om skadeståndsansvar finns i skadeståndslagen.

13 a §

Registrering av uppgifter i registret över säkerhetsutredningar

Transport- och kommunikationsverket ska i det register över säkerhetsutredningar som avses i säkerhetsutredningslagen anteckna uppgifter om godkända bedömningsorgan *för informationssäkerhet* samt uppgifter som ingår i intyg som getts till bedömningsorganen. Återkallelsen av ett godkännande ska omedelbart antecknas i registret.

Gällande lydelse

godkännande ska omedelbart antecknas i registret.

Ett godkänt bedömningsorgan kan för anteckning i registret över säkerhetsutredningar och för vidarebefordran ur registret lämna Kommunikationsverket uppgifter om dem som det har bedömt och om innehållet i det intyg som det har utfärdat, om inte den som bedömningen gäller har förbjudit detta. Före underrättelsen ska den som bedömningen gäller informeras om syftet med databehandlingen och den reglering som gäller den.

Föreslagen lydelse

Ett godkänt bedömningsorgan för *informationssäkerhet kan för anteckning* i registret över säkerhetsutredningar och för vidarebefordran ur registret lämna *Transport- och kommunikationsverket* uppgifter om de organisationer som har varit föremål för bedömningsorganets bedömning och om innehållet i de intyg som bedömningsorganet har gett åt de organisationerna, om inte organisationerna har förbjudit detta. Före uppgifterna lämnas ska den som bedömningen gäller informeras om syftet med databehandlingen och vilken lagstiftning databehandlingen omfattas av.

Denna lag träder i kraft den 2026 .

Transport- och kommunikationsverket ska inom två år från ikraftträdandet av denna lag i enlighet med 4 § ansöka om en säkerhetsutredning av företag i fråga om ett sådant godkänt bedömningsorgan för informationssäkerhet för vilket ett kompetensområde för bedömning av hanteringen av säkerhetsklassificerad information har godkänts i enlighet med de bestämmelser som gällde vid ikraftträdandet.

3.

Lag

om ändring av 18 och 48 § i säkerhetsutredningslagen

I enlighet med riksdagens beslut

upphävs i säkerhetsutredningslagen (726/2014) 48 § 4 mom. 1 punkten, sådan den lyder i lag 347/2020, och

ändras 18 § 2 mom. som följer:

Gällande lydelse	*Föreslagen lydelse*
18 §	18 §
Överensstämmelse med säkerhetskraven som en allmän förutsättning	*Överensstämmelse med säkerhetskraven som en allmän förutsättning*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Överensstämmelse med kraven enligt 1 mom. kan påvisas genom ett intyg utfärdat av ett godkänt bedömningsorgan som avses i lagen om bedömningsorgan för informationssäkerhet (1405/2011), genom ett intyg utfärdat i enlighet med lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011), genom en säkerhetsplan eller på något annat sätt som den behöriga myndighet som beslutar att säkerhetsutredning ska göras godkänner.	Överensstämmelse med kraven enligt 1 mom. kan påvisas genom ett intyg utfärdat av ett godkänt bedömningsorgan som avses i lagen om bedömningsorgan för informationssäkerhet (1405/2011), genom ett *beslut eller utlåtande som utfärdats* i enlighet med lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011), genom en säkerhetsplan eller på något annat sätt som den behöriga myndighet som beslutar att säkerhetsutredning ska göras godkänner.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
48 §	
Registret över säkerhetsutredningar och registrets ändamål samt registrering av uppgifter	
— — — — — — — — — — — — — — —	
Transport- och kommunikationsverket får registrera uppgifter om	
1)de intyg som det har utfärdat enligt lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation och de uppgifter som antecknats i intygen,	(upphävs)
— — — — — — — — — — — — — — —	

Gällande lydelse	*Föreslagen lydelse*
	_____
	Denna lag träder i kraft den 2026.
	_____