RP 45/2011 rd

Regeringens proposition till Riksdagen med förslag till lagar om bedömningsorgan för informationssäkerhet, bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation och ändring av 2 § i lagen om kommunikationsförvaltningen

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås att det stiftas en lag om bedömningsorgan för informationssäkerhet och en lag om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation. De uppgifter som följer av reformen åläggs Kommunikationsverket, vilket medför att lagen om kommunikationsförvaltningen behöver ändras.

Syftet med propositionen är att främja företagssäkerheten genom att upprätta tillsyn över organ som bedömer företagens informationssäkerhet. Kommunikationsverket föreslås ha hand om godkännandet av och tillsynen över bedömningsorganen.

Godkännandet av bedömningsorgan ger företagen tillfälle att visa nivån på informationssäkerheten i sin verksamhet med hjälp av extern och tillförlitlig bedömning. Syftet med propositionen är att bidra till att förenkla och effektivisera myndigheternas förfaranden vid verkställigheten av senare lagstiftning om utredning av företags och personers bakgrund.

Kommunikationsverket föreslås också få i uppdrag att sköta uppgifter som gäller bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation. Syftet med lagförslaget är att utveckla informationssäkerheten inom statsförvaltningen.

Propositionen hänför sig till budgetpropositionen för 2012 och avses bli behandlad i samband med den.

De föreslagna lagarna avses träda i kraft senast den 1 juni 2012.

295660

INNEHÅLL

ALLMÄN MOTIVERING

1 Nuläge

I lagstiftningen finns det för närvarande inte några bestämmelser om verksamheten inom organ som bedömer informationssäkerheten i företag. I lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (920/2005) föreskrivs det om ett nationellt ackrediteringssystem med syfte att säkerställa att de tjänster för bedömning av överensstämmelse med kraven som tillhandahålls är tillförlitliga och internationellt acceptabla. Med bedömning av överensstämmelse med kraven avses ackreditering, testning, kalibrering, certifiering, kontroll och därmed jämförbar verksamhet. Avsikten har varit att med hjälp av bestämmelserna säkerställa att det nationella ackrediteringsorganet, mätteknikcentralens ackrediteringsenhet (ackrediteringstjänsten FINAS) uppfyller de internationella och europeiska bedömningskriterierna för ackreditering.

Bedömningsorganen för informationssäkerhet kan anlita ackrediteringstjänsten FINAS, men deras verksamhet som helhet saknar tillsyn som utomstående utför. Företagssäkerhetens betydelse blir allt större, bland annat på grund av de internationella upphandlingsförfarandena och efter hand som företagens innovationsverksamhet och verksamhet i övrigt bildar nätverk. Det innebär att det ligger också i företagens intresse att tillsyn över bedömningsorganen utövas.

För närvarande finns det en handfull bedömningsorgan som skulle kunna ansöka hos Kommunikationsverket om det godkännande som föreslås.

I lagstiftningen finns det inte heller bestämmelser om något för myndigheterna lämpligt förfarande genom vilket myndigheterna skulle kunna skaffa sig en tillförlitlig bedömning av nivån på informationssäkerheten i de informationssystem och den datakommunikation som de använder. Detta måste betraktas som en brist med avseende på uppfyllandet och utvecklingen av kraven på informationssäkerheten inom statsförvaltningen.

Kommunikationsverket bedömer företags informationssystem och datakommunikation redan som ett led i uppgörandet av säkerhetsutredningar som gäller sammanslutningar. Bestämmelser om sådana säkerhetsutredningar finns i lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004).

2 Målsättning och de viktigaste förslagen

2.1 Målsättning

Propositionens allmänna mål är att bidra till att främja företagssäkerheten och utveckla informationssäkerheten i myndigheternas verksamhet.

Den föreslagna lagen om bedömningsorgan för informationssäkerhet hänför sig till en mera omfattande totalreform av lagstiftningen om utredning av företags och personer bakgrund. Förfarandet med godkännande av bedömningsorgan ger företagen möjligheter att bättre än nu förbereda sig på säkerhetsutredningar som avser dem. Så är propositionens funktionella mål också att förenkla och effektivisera myndighetsförfarandena vid bakgrundsutredningar.

2.2 De viktigaste förslagen

Enligt lagförslag nr 1 i propositionen ska det skapas ett system genom vilket företagen kan utveckla informationssäkerheten med hjälp av dels gemensamma kriterier, dels bedömningsorgan som står under myndighetstillsyn. Även om en myndighet ska göra upp säkerhetsutredningar som avser företag gör lagförslaget det möjligt för företagen att bättre än nu förbereda sig på medverkan i exempelvis sådana internationella upphandlingsförfaranden där det krävs en av en myndighet uppgjord säkerhetsutredning och ett intyg över den. Detta förbättrar de finska företagens konkurrenskraft vid internationella upphandlingar.

I propositionen föreslås det i lagförslag nr 2 att Kommunikationsverket ska kunna

bedöma myndigheternas informationssystem och datakommunikation och utfärda intyg över system som uppfyller kraven. Förslaget anknyter till genomförandet och utvecklingen av bestämmelserna om informationssäkerheten inom statsförvaltningen. Den föreslagna lagen har också en mera allmän betydelse, eftersom den myndighet som bedömer informationssäkerheten i myndigheternas informationssystem och datakommunikation är en del av arrangemang som tillämpas i olika länder och i många internationella överenskommelser och rättsakter.

3 Propositionens konsekvenser

3.1 Ekonomiska konsekvenser och konsekvenser för personal

Antalet säkerhetsutredningar som avser företag väntas stiga under de närmaste åren. Uppgörandet av sådana kan ta rikligt med tid och arbete i anspråk, framför allt om det företag som är föremål för utredningen inte självt har utrett nivån på sina informationssäkerhetsåtgärder tidigare. Det är meningen att utredningsförfarandet ska försnabbas tack vare lagförslag nr 1. På basis av lagförslaget kan företagen själva i förväg säkra nivån på sina informationssäkerhetsåtgärder genom att låta ett bedömningsorgan som står under myndighetstillsyn bedöma informationssäkerheten.

Kommunikationsverket ska enligt förslaget godkänna och ha tillsyn över bedömningsorganen för informationssäkerhet (lagförslag nr 1). Dessutom föreslås Kommunikationsverket bedöma motsvarade omständigheter i fråga om myndigheternas verksamhet (lagförslag nr 2).

Verksamheten förutsätter nödvändigtvis skyddsutrymmen och andra tekniska system. Kommunikationsverket har till sitt förfogande de utrymmen som behövs.

Det är meningen att en avgift ska tas ut för de uppgifter som Kommunikationsverket utför. De inkomster som avgifterna inbringar uppskattas motsvara kostnaderna för verksamheten, när verksamheten är i gång i full utsträckning. Under de fem första verksamhetsåren behövs för verksamheten dock ett årligt anslag om ca 450 000 euro. Anslaget täcker personalkostnader motsvarande tre årsverken och kostnaderna för underhåll av de lokaler som behövs för verksamheten, logistik och arrangemang som gäller datakommunikation och programvara. Kostnaderna har beaktats i budgetpropositionen för 2012 vid dimensioneringen av anslaget under Kommunikationsverkets omkostnadsmoment (31.40.01). De nya uppgifterna väntas kunna bli genomförda inom den årsverkesram som fastställts för Kommunikationsverket i statsförvaltningens produktivitetsprogram.

De bestämmelser om utveckling av företagssäkerheten som ingår i propositionen är ägnade att underlätta företagssamarbetet i olika utvecklingsprojekt som kan leda till innovationer och utveckling av nya produkter. Nyttan av detta är dock svår att uppskatta.

3.2 Konsekvenser för myndigheterna

Genomförandet av de reformer som föreslås i propositionen har ingen stor inverkan på Kommunikationsverkets organisation.

Enligt den föreslagna lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation ska Kommunikationsverket sköta bedömningsuppgiften. Förfarandet förbättrar myndigheternas möjligheter att säkerställa nivån på sin informationssäkerhet. När propositionen beretts har man utgått från att bedömningar av detta slag görs centralt i den mån det är möjligt, och så att nyttan av dem inom förvaltningen kommer mer än en enda myndighet till del.

Avsikten är att Kommunikationsverket, finansministeriet, kommunikationsministeriet och de övriga förvaltningsområdena ska bedriva ett nära samarbete för att åstadkomma effektivaste möjliga utveckling av informationssäkerheten i informationssystemen och datakommunikationen inom statsförvaltningen och ett ändamålsenligt förfarande vid bedömningen av dem. I detta samarbete är det möjligt att utnyttja och vidareutveckla det redan nu välfungerande och heltäckande arbete som utförs i ledningsgruppen för datasäkerheten inom statsförvaltningen (VAHTI) för att utveckla och styra informationssäkerheten inom förvaltningen och bedriva samarbete på detta område. Avsikten är dessutom att resul-

tatstyrningen vid Kommunikationsverket i fråga om de nya uppgifter som anges i lagförslaget ska ske som ett nära samarbete mellan finansministeriet och kommunikationsministeriet.

3.3 Konsekvenser för medborgarna

De föreslagna lagarna har inga direkta konsekvenser för medborgarnas ställning.

3.4 Konsekvenser för företagsverksamheten

Den föreslagna lagen om bedömningsorgan för informationssäkerhet (lagförslag nr 1) erbjuder företagen möjligheter att få en tillförlitlig bedömning av nivån på de egna informationssäkerhetsåtgärderna och att därmed förbereda sig för projekt där uppfyllandet av krav på informationssäkerheten är ett villkor för projektdeltagande.

Det är meningen att bedömningsorganen ska kunna ansöka hos Kommunikationsverket om godkännande. Möjligheten gäller sannolikt den handfull företag som nu är verksamma. Eftersom det dessutom kommer att vara frivilligt för företagen att ansöka om godkännande kan det inte anses att förslaget innebär en betydande administrativ börda för företagssektorn.

4 Beredningen av propositionen

4.1 Beredningsskeden och beredningsmaterial

Justitieministeriet tillsatte den 1 oktober 2008 en arbetsgrupp med uppgift att bereda ett förslag till revidering av lagen om säkerhetsutredningar (177/2002). Arbetsgruppens förslag skulle ha formen av en regeringsproposition. Statsrådets kansli, utrikesministeriet, justitieministeriet, inrikesministeriet, försvarsministeriet, finansministeriet, social- och hälsovårdsministeriet, arbets- och näringsministeriet, skyddspolisen, huvudstaben och dataombudsmannens byrå var företrädda i arbetsgruppen. I arbetsgruppen ingick också en för arbetsgivarparten gemensam representant från Näringslivets centralförbund och en för löntagarorganisationerna gemensam representant från Akava ry.

Företrädare för kommunikationsministeriet, Finanssialan Keskusliitto - Finansbranschens Centralförbund ry och Finlands Kommunförbund samt en expert på företagssäkerhet från Näringslivets centralförbund deltog i arbetsgruppen som sakkunniga. Under arbetets gång hörde arbetsgruppen företrädare för riksdagens centralkansli, Centralhandelskammaren, Företagarna i Finland rf, Försörjningsberedskapscentralen, Rättsregistercentralen, Inspecta Sertifiointi Oy, Suomen Vartioliikkeitten Liitto ry samt Suomen Turvaurakoitsijaliitto - Finlands Säkerhetsentreprenörsförbund ry. I arbetsgruppens arbete deltog också sakkunniga inom säkerhetsbranschen från Kommunikationsverket, den nationella säkerhetsmyndigheten och försvarsministeriet.

Arbetsgruppen föreslog i sitt betänkande (Justitieministeriets betänkanden och utlåtanden 8/2011) att de lagförslag som ingår i denna proposition skulle föreläggas riksdagen som ett led i totalreformen. Utifrån diskussioner mellan ministerierna och Kommunikationsverket gick man i syfte att säkerställa kostnadsbesparingar in för att lagförslagen överlämnas till riksdagen före den mera omfattande proposition som gäller totalreformen.

4.2 Remissyttranden och hur de har beaktats

Sammanlagt 32 myndigheter och intresseföreträdare som är centrala i sammanhanget ombads ge utlåtande om det betänkande som den av justitieministeriet tillsatta arbetsgruppen för beredning av en totalreform av lagstiftningen om bakgrundsutredningar avlåtit. Ministerierna ombads inhämta utlåtanden hos den underställda förvaltningen som ansågs vara behövliga.

Relativt få ställningstaganden till de lagar som föreslås i denna proposition framfördes. De remissorgan som inkom med allmänna bedömningar ansåg att lagförslagen är behövliga. Försörjningsberedskapscentralen konstaterade visserligen att den lag som utgör lagförslag nr 1 behövs bara om avsikten

är att hindra oönskade fenomen inom branschen.

De mera detaljerade ställningstagandena var till övervägande del av framför allt lagtekniskt slag eller formulerade som frågor. I en del utlåtanden bedömdes arten och betydelsen av förfarandet för godkännande av bedömningsorgan. I statens revisionsverks utlåtande skärskådades frågor med anknytning till de sakkunniga som Kommunikationsverket anlitar. Riksdagens justitieombudsman ansåg att bedömningsorganen bör iaktta också språklagen (423/2003) vid skötseln av en offentlig förvaltningsuppgift.

Huvudstaben ansåg att bestämmelsen om Kommunikationsverkets rätt att få uppgifter (lagförslag nr 2, 6 §) är mycket viktig för att försvarsmaktens särbehov med anknytning till försvarsintressen ska beaktas i samband med ärenden om bedömning av informationssäkerheten i informationssystem och datakommunikation. Jämsides med allmänna nationella arrangemang bör försvarsmakten också i fortsättningen till behövliga delar kunna auditera sina egna kritiska informationssystem. Inrikesministeriet önskade att det skulle tas in i bestämmelserna att auditeringar som redan utförts inom statsförvaltningen inte behöver upprepas i onödan. Ministeriet ägnade också allmän uppmärksamhet åt kostnaderna för informationssäkerheten.

De synpunkter som förts fram i remissyttrandena har beaktats vid ärendets fortsatta beredning.

5 Samband med andra propositioner

Propositionen hänför sig till budgetpropositionen för 2012 och avses bli behandlad i samband med den.

De föreslagna lagarna gagnar en så kostnadseffektiv verkställighet som möjligt av den totalreform av lagstiftningen om utredning av företags och personers bakgrund som är under beredning.

DETALJMOTIVERING

1 Lagförslag

1.1 Lagen om bedömningsorgan för informationssäkerhet

1 kap. **Allmänna bestämmelser**

1 §. *Lagens syfte.* I den föreslagna lagen föreskrivs om ett förfarande genom vilket företag tillförlitligt kan visa en utomstående att de i sin verksamhet har sörjt för en viss informationssäkerhetsnivå.

Bedömningsorganet bedömer företagets informationssäkerhet i förhållande till i förväg fastställda krav på informationssäkerheten. Kraven kan ingå i en lag eller förordning eller fastställas till exempel i en standard. I 10 § finns bestämmelser om de kriterier som ska användas.

Lagen syfte fylls genom att bedömningsorganen ges möjlighet att ansöka om godkännande för sin verksamhet hos Kommunikationsverket. Enligt förslaget ska bedömningsverksamheten inte vara tillstånds- eller anmälningspliktig verksamhet. Ansökan om godkännande ska i stället vara en möjlighet för bedömningsorganen, inte en skyldighet (2 § 1 mom., 3 § 1 mom.).

Bedömningsorganen och den omständigheten att deras verksamhet är tillförlitlig är viktiga för företagen när de själva utvecklar informationssäkerheten i sin organisation. Med bedömningsorganens hjälp kan företagen också konsekvent förbereda sig för situationer där nivån på deras informationssäkerhet är ett absolut villkor för framgång i upphandlingsförfaranden, såsom internationella och nationella upphandlingar eller samarbetsprojekt inom försvars- och säkerhetssektorn.

2 §. *Lagens tillämpningsområde.* Lagen avses enligt 1 mom. bli tillämpad på näringsidkare och på enheter som tillhandahåller serviceuppgifter för den offentliga förvaltningen som på uppdrag bedömer informationssäkerhetens nivå (bedömningsorgan för informationssäkerhet) och vill att Kommunikationsverket ska godkänna deras verksamhet, samt på godkännandeförfarandet.

Meningen har varit att det i lagen inte ska avgränsas vilka slag av verksamhetsenheter som kan vara sådana bedömningsorgan som avses i lagen. Bedömningsorganen kan vara dels privata näringsidkare, dels – oberoende av organisationsformen – sådana verksamhetsenheter som tillhandahåller den offentliga förvaltningen bedömningstjänster. Även om den föreslagna lagens primära syfte är att främja företagssäkerheten kan det godkännande som avses i den alltså sökas också av bedömningsorgan vars kundkrets i första hand består av exempelvis myndigheter och andra aktörer inom den offentliga förvaltningen.

Av momentets ordalydelse framgår att lagen inte är avsedd att inverka på verksamhet som bedrivs av sådana bedömningsorgan för informationssäkerhet som inte har ansökt om godkännande hos Kommunikationsverket.

Enligt *2 mom.* föreskrivs särskilt om Kommunikationsverkets uppgifter vid bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation samt vid uppgörande av säkerhetsutredningar som gäller sammanslutningar. Med detta avses lagen i lagförslag nr 2 och lagen om internationella förpliktelser som gäller informationssäkerheten.

2 kap. **Godkännande av och tillsyn över bedömningsorgan**

3 §. *Ansökan om godkännande av bedömningsorgan.* Enligt *1 mom.* kan bedömningsorgan för informationssäkerhet ansöka hos Kommunikationsverket om godkännande för sin verksamhet.

Bestämmelsens ordalydelse ger vid handen att det inte är obligatoriskt att ansöka om godkännande. Enligt den föreslagna lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation kan myndigheterna emellertid anlita förutom Kommunikationsverket bara sådana bedömningsorgan som verket har godkänt (lagförslag nr 2, 3 §). Avsaknad

av godkännande kan antagligen också inverka på bedömningsorganets ställning på marknaden.

De uppgifter som behövs för behandling av ärendet ska fogas till ansökan.

4 §. *Behandlingen av ansökan.* Enligt *1 mom.* ska Kommunikationsverket innan ett bedömningsorgan för informationssäkerhet godkänns ge skyddspolisen tillfälle att yttra sig om tillförlitligheten hos bedömningsorganets ansvariga personer och om säkerheten i bedömningsorganets lokaler. Detta hänför sig till de föreslagna kraven för godkännande av bedömningsorgan, enligt vilka tillförlitligheten hos bedömningsorganets ansvariga personer och säkerheten i bedömningsorganets lokaler ska ha säkerställts.

När skyddspolisen sammanställer sitt utlåtande ska den iaktta det som bestäms i lagen om internationella förpliktelser som gäller informationssäkerheten. Med detta hänvisas det till den nämnda lagens bestämmelser om säkerhetsutredningar som gäller sammanslutningar och utredningar som gäller personsäkerhet. I samband med totalreformen av lagstiftningen om utredning av företags och personers bakgrund överförs regleringen av utredningar som avser företagssäkerhet i sin helhet till en allmän lag som är tillämplig nationellt.

När ansökan behandlas kan Kommunikationsverket enligt *2 mom.* inhämta utlåtanden och ge utomstående sakkunniga i uppdrag att utföra uppgifter som anknyter till bedömningen av ansökan och av uppgifter som ingår i den. Dessa sakkunniga beslutar inte om angelägenheter som rör bedömningsorganen utan sammanställer under Kommunikationsverkets styrning och tillsyn utredningar med avseende på beslutsfattandet. På personer tillämpas sekretessbestämmelserna i lagen om offentlighet i myndigheternas verksamhet (621/1999) direkt. Med beaktande av den ovan beskrivna ställningen som sakkunnig finns det inte behov av att i lagförslaget ta in någon särskild bestämmelse om sakkunniga där det hänvisas till allmänna förvaltningsrättsliga bestämmelser.

5 §. *Godkännande av bedömningsorgan.* I *1 mom.* bestäms det om kraven för godkännande av bedömningsorgan för informationssäkerhet. Organet ska vara funktionellt och ekonomiskt oberoende av den som bedömningen gäller (*1 punkten*). Detta är väsentligt för att det ska vara möjligt att lita på bedömningen och dess opartiskhet.

Enligt *2 punkten* ska organets personal ha god teknisk och yrkesinriktad utbildning samt tillräckligt omfattande erfarenhet av de uppgifter som ingår i verksamheten, och organet ska ha den utrustning, de hjälpmedel och de system som behövs i verksamheten (*3 punkten*). Tillförlitligheten hos de ansvariga personerna inom organet ska ha säkerställts och organet ska dessutom ha en övervakad metod som bedömts som tillförlitlig och med vars hjälp säkerheten i organets lokaler och databehandling säkerställs, samt ändamålsenliga anvisningar för verksamheten och uppföljning av den (*4 och 5 punkten*).

I *2 mom.* finns en särskild bestämmelse enligt vilken uppfyllandet av kraven i 1 mom. 1—3 punkten ska visas genom det förfarande som det bestäms om i lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven, och i den utsträckning som förfarandet möjliggör. Det innebär i praktiken att de nämnda omständigheterna ska ha klarlagts inom ackrediteringstjänsten FINAS i samarbete med Kommunikationsverket.

Ett organ som uppfyller kraven godkänns enligt *3 mom.* av Kommunikationsverket utifrån de utredningar som verket har mottagit eller utfört och de inspektioner som verket har förrättat som ett godkänt bedömningsorgan som avses i denna lag. Ett sådant organ får i sin marknadsföring och sin övriga kommunikation använda ett uttryck för godkännandet, om inte godkännandets giltighetstid har löpt ut eller om inte Kommunikationsverket har beslutat att återkalla godkännandet.

Enligt *4 mom.* kan godkännandet beviljas för viss tid, om det finns särskilda skäl till detta, och i ett beslut om godkännande kan det ingå begränsningar och villkor som gäller organets kompetensområde, tillsyn och verksamhet och som behövs för att säkerställa att uppgifterna sköts på behörigt sätt. Ett särskilt skäl kan hänföra sig exempelvis till avgränsning av bedömningsorganets kompetensområde, något som blir onödigt efter att bedömningsorganet har utvecklat sin verksamhet.

6 §. *Återkallelse av godkännande av bedömningsorgan.* Om ett godkänt bedömningsorgan för informationssäkerhet handlar i strid med bestämmelserna eller inte längre uppfyller kraven för godkännande, ska Kommunikationsverket enligt förslaget uppmana bedömningsorganet att avhjälpa bristen inom utsatt tid. Om bristen inte avhjälps inom utsatt tid, kan Kommunikationsverket återkalla godkännandet.

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

7 §. *Kommunikationsverkets inspektionsrätt.* Kommunikationsverket och en sakkunnig som handlar på uppdrag av verket ska enligt *1 mom.* ha rätt att inspektera organets lokaler och de metoder som bedömningsorganet för informationssäkerhet använder. Eftersom det inte är nödvändigt att utsträcka de inspektioner som avses i den föreslagna bestämmelsen till hemfridsskyddade utrymmen eller förutsättningarna för sådana inspektioner inte uppfylls har det i bestämmelsen ansetts vara skäl att uttryckligen ange att sådana utrymmen inte ska omfattas av inspektionsrätten.

8 §. *Bedömningsorganens upplysnings- och anmälningsskyldighet.* Syftet med paragrafen är att trygga Kommunikationsverkets möjlighet att få de upplysningar som behövs för skötseln av verkets tillsynsuppgifter. Bestämmelser om de uppgifter som behövs för behandling av ansökan föreslås i 3 § 2 mom.

I *1 mom.* föreslås en bestämmelse om skyldigheten för godkända bedömningsorgan att underrätta Kommunikationsverket om sådana ändringar i sin verksamhet som har betydelse för uppfyllandet av de krav som ställs på organet.

I *2 mom.* åläggs bedömningsorganet att lämna till Kommunikationsverket de upplysningar som behövs för tillsyn över att organet uppfyller kraven på dess verksamhet.

3 kap. Bedömning av informationssäkerheten

9 §. *Bedömningsorganents uppgifter.* Ett godkänt bedömningsorgan för informationssäkerhet ska enligt *1 mom.* iaktta omsorg när det utför en bedömningsuppgift. Avsikten med denna skrivning är att betona organets skyldighet att iaktta lämpliga förfaranden och att även i övrigt bedriva saklig verksamhet.

Ett godkänt bedömningsorgan ska enligt *1 punkten* se till att granska de lokaler där den som bedömningen gäller verkar. Intyg över bedömningen kan därmed inte utfärdas utan att lokalerna har granskats på tillbörligt sätt.

Enligt *2 punkten* ska det vid bedömningen klarläggas om den som bedömningen gäller i sin verksamhet på behörigt sätt har uppfyllt de övriga krav angående informationssäkerheten som anges i 10 § och ligger till grund för utredningen (bedömningsgrunder för informationssäkerhet).

Det godkända bedömningsorganet ska enligt *2 mom.* på basis av utredningarna och granskningen utfärda ett intyg, om lokalerna och verksamheten hos den som bedömningen gäller bedriver är förenlig med de krav på informationssäkerheten som legat till grund för bedömningen. De kriterier som använts vid bedömningen ska specificeras i intyget. Detta är viktigt för säkerställande av att intyget på behörigt sätt beskriver den informationssäkerhetsnivå som den som bedömningen gäller iakttar i sin verksamhet.

10 §. *Bedömningsgrunder för informationssäkerhet.* Vid de bedömningar som avses i den föreslagna lagen är det enligt förslaget möjligt att använda olika krav som gäller informationssäkerheten. Det har varit meningen att de kriterier som används när företagens informationssäkerhetsåtgärder bedöms kan vara olika eftersom också företagets behov kan skilja sig åt i olika situationer.

Enligt förslaget är det för det första möjligt att använda i lag eller förordning föreskrivna krav på informationssäkerheten i myndigheternas verksamhet samt finansministeriets anvisningar om informationssäkerhet (*1 punkten*). Med detta hänvisas särskilt till statsrådets förordning om informationssäkerheten inom statsförvaltningen (681/2010) och finansministeriets anvisning om genomförande av den (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010).

Som grund är det möjligt att använda också anvisningar om uppfyllande av internationella informationssäkerhetsförpliktelser som meddelats av den nationella säkerhetsmyndighet (NSA) som avses i lagen om internationella förpliktelser som gäller informationssäkerhet (*2 punkten*). I praktiken innebär detta att det som kravnivå är möjligt att använda den nationella kriteriesamlingen för säkerhetsauditering (KATAKRI), som i enlighet med en av den nationella säkerhetsmyndigheten meddelad anvisning tillämpas vid skötseln av internationella informationssäkerhetsförpliktelser.

Som bedömningsgrund är det enligt förslaget möjligt att använda Europeiska unionens eller något annat internationellt organs bestämmelser och anvisningar om informationssäkerhet (*3 punkten*). Uppnåendet av den informationssäkerhetsnivå som unionen fastställt kan vara av betydelse exempelvis i Europeiska unionens projekt som finska företag vill medverka i.

Som basnivå för informationssäkerheten är det enligt förslaget möjligt att använda publicerade allmänt eller regionalt tillämpade bestämmelser, föreskrifter eller anvisningar om informationssäkerheten (*4 punkten*) eller informationssäkerhetskrav som ingår i en fastställd standard (*5 punkten*).

4 kap. **Särskilda bestämmelser**

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

Lagen om grunderna för avgifter till staten avses inte bli tillämpad på godkända bedömningsorgan. Dessa beslutar i stället själva vilka avgifter de tar ut för bedömningen.

12 §. *Ändringssökande.* I fråga om sökande av ändring i beslut som Kommunikationsverket meddelat med stöd av den föreslagna lagen 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 den föreslagna lagen ska det enligt förslaget iaktta förvaltningslagen (434/2003), lagen om offentlighet i myndigheternas verksamhet och språklagen (423/2003).

För undvikande av tolkningsproblem ska tillämpningen av de nämnda författningarna enligt förslaget inte vara bunden till skötsel av en offentlig förvaltningsuppgift, utan författningarna ska tillämpas på skötseln av alla uppgifter som är förenliga med den föreslagna lagen. Till straff för brott mot tystnadsplikt samt förbudet att utnyttja uppgifter enligt lagen om offentlighet i myndigheternas verksamhet döms enligt 40 kap. 5 § i strafflagen, om gärningen inte är straffbar enligt 38 kap. 1 eller 2 § i strafflagen eller om strängare straff för gärningen inte föreskrivs någon annanstans i lag (lagen om offentlighet i myndigheternas verksamhet, 35 §).

14 §. *Ikraftträdande.* Det är meningen att lagen ska kunna sättas i kraft senast den 1 juni 2012. Åtgärder som krävs för verkställigheten av lagen får enligt lagförslaget vidtas innan lagen träder i kraft.

1.2 Lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation

1 §. *Lagens tillämpningsområde.* Den föreslagna lagen innehåller bestämmelser om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (*1 mom.*). Med lagens hjälp skapas det för myndigheterna möjligheter att av en extern särskild myndighet få en bedömning av nivån på informationssäkerheten hos informationssystem och datakommunikation som de bestämmer över.

Lagen behövs för säkerställande av att myndigheterna kan få en extern bedömning också när de behandlar informationsmaterial som omfattas av högsta krav på informationssäkerhet och vars behandling och överföring det är problematiskt att ge privata bedömningsorgan i uppdrag att bedöma.

Kommunikationsverket är den särskilda myndighet som avses i lagförslaget. Kommunikationsverket har redan i lagförslaget avsedda uppgifter i angelägenheter som hän-

för sig till internationella informationssäkerhetsförpliktelser. Det föreslagna 2 mom. innehåller en hänvisning till lagstiftningen om detta.

2 §. *Definitioner.* Paragrafen föreslås innehålla definitioner som är centrala med avseende på lagens tillämpning.

Enligt *1 punkten* avses med informationssystem ett helhetsarrangemang som består av databehandlingsutrustning, program och annan databehandling. Avsikten har varit att definitionen ska vara så heltäckande som möjligt.

Enligt *2 punkten* avses med datakommunikation ett system som utgörs av arrangemang omfattande ett dataöverföringsnät, dataöverföringsutrustning, programvara och andra databehandlingsarrangemang. Avsikten är att också denna definition ska vara bred för att lämpa sig för situationer som är olika och föränderliga.

I *3 punkten* definieras begreppet myndighet. Enligt definitionen avses med myndighet organ som avses i 4 § 1 mom. 1—7 punkten i lagen om offentlighet i myndigheternas verksamhet. Det innebär att myndighetsbegreppet inte omfattar arbetsgrupper och motsvarande som har tillsatts för att självständigt utföra en uppgift.

Den definition av begreppet statsförvaltningsmyndighet som föreslås i *4 punkten* motsvarar bestämmelserna i förordningen om informationssäkerheten inom statsförvaltningen. Detta är ändamålsenligt med beaktande av lagens syfte att främja informationssäkerheten inom statsförvaltningen. Definitionen innebär också att det på uppdrag av finansministeriet inte är möjligt att göra en utredning om exempelvis informationssäkerheten hos inrättningar som lyder under riksdagen. Sådana inrättningar kan däremot själva begära att en bedömning görs.

3 §. *Anlitande av tjänster för bedömning av informationssäkerheten.* Paragrafen föreslås uppta en bestämmelse med vars hjälp det säkerställs att statsförvaltningsmyndigheterna anlitar bara tillförlitliga externa tjänster för bedömning av informationssäkerheten. Bestämmelsen behövs för att informationssäkerheten inom statsförvaltningen ska utvecklas på ett enhetligt sätt och utan kostnader vars grund är osaklig.

Enligt förslaget ska statsförvaltningsmyndigheterna för bedömning av informationssäkerheten få använda bara det förfarande som avses i den föreslagna lagen eller anlita bara bedömningsorgan som har godkänts av Kommunikationsverket enligt den föreslagna lagen om bedömningsorgan (lagförslag nr 1).

Bestämmelsen föreslås bli avgränsad att gälla bara statsförvaltningsmyndigheterna, som också förordningen om informationssäkerheten inom statsförvaltningen tillämpas på.

4 §. *Kommunikationsverkets uppgifter.* Enligt *1 mom.* ska Kommunikationsverket i syfte att främja och säkerställa informationssäkerheten i myndigheternas informationssystem och datakommunikation utföra de uppgifter som specificeras i momentet. Det är skäl att lägga märke till att Kommunikationsverkets uppgifter inte inkluderar vare sig bedömning av om den information som registreras i informationssystemen är lagenlig eller andra frågor som anknyter till bedömning av informationssystemets innehåll. I uppgifterna är det fråga enbart om att bedöma om informationssystemen och datakommunikationen har de tekniska egenskaper som förutsätts av dem.

Enligt förslaget ska Kommunikationsverket 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 (*1 punkten*).

Det kan anses att en myndighet bestämmer över ett informationssystem, om informationssystemet är tillgängligt för myndigheten exempelvis med stöd av ett licensavtal och om myndigheten med stöd av bestämmelser har rätt att besluta om användningen av informationssystemet, utlämnandet av uppgifter ur det och annan databehandling. Förslaget innebär att bedömningen kan gälla också ett sådant informationssystem som myndigheten planerar att skaffa.

Den skyldighet som avses i punkten är inte ovillkorlig, såsom närmare framgår av 3 mom. Förslaget innebär också att Kommunikationsverket inte är tillsynsmyndighet utan gör bedömningen på myndighetens begäran.

I internationell praxis och olika länders lagstiftning kan det förutsättas att en oberoende instans har utfärdat ett intyg över att informationssystemet eller datakommunikationen uppfyller en viss kravnivå för informationssäkerhetens del. Enligt *2 punkten* ska Kommunikationsverket på begäran utfärda ett intyg som visar att informationssystemet eller datakommunikationen har godkänts.

Bland Kommunikationsverkets uppgifter ingår enligt förslaget att på finansministeriets begäran göra utredningar om den allmänna nivån på informationssäkerheten i informationssystem eller datakommunikation som en statsförvaltningsmyndighet bestämmer över (*3 punkten*). Detta hänför sig till behovet av att få allmän information om verkställigheten av lagstiftningen om informationssäkerhet.

I lagen har man på grund av effektivitets- och produktivitetskrav också 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. Därför får enligt *2 mom.* en begäran om bedömning av informationssäkerheten i ett informationssystem eller datakommunikation eller en begäran om erhållande av ett intyg över informationssäkerheten framställas också av någon som tillhandahåller sådana databehandlings- eller datakommunikationstjänster som anlitas allmänt av olika statsförvaltningsmyndigheter. Det faller sig naturligt att en tillhandahållare av tjänster sköter denna uppgift på så sätt att myndigheten känner till och godkänner att förfarandet inleds. Därför förutsätts det i bestämmelsen att görandet av en bedömning förutsätter ett uppdrag som den berörda myndigheten gett.

I *3 mom.* föreslås en bestämmelse med vars hjälp skötseln av Kommunikationsverkets uppgifter kan ställas i relation till de resurser som verket har till sitt förfogande. Enligt förslaget ska en bedömning av ett informationssystem eller datakommunikation som begärts av en myndighet som avses i 1 mom. eller av någon i 2 mom. avsedd tillhandahållare av databehandlings- eller datakommunikationstjänster utföras inom ramen för de resurser som står till buds.

5 §. *Utredningar på uppdrag av finansministeriet.* Det föreslås att *1 mom.* ska uppta en bestämmelse om det förfarande genom vilket finansministeriet kan få upplysningar om nivån på informationssäkerheten inom statsförvaltningen för att följa verkställigheten av lagstiftningen om den och allmänt utveckla informationssäkerheten.

Enligt förslaget kan finansministeriet ge Kommunikationsverket i uppdrag att på begäran av finansministeriet göra utredningar om den allmänna nivån på informationssäkerheten i informationssystem eller datakommunikation som en statsförvaltningsmyndighet bestämmer över.

De informationssystem som ska omfattas av utredningen kan utses utifrån deras användningsändamål, arten av de uppgifter som registreras i dem eller någon annan motsvarande allmän omständighet. Det är alltså inte fråga om att bedöma eller ha tillsyn över ett informationssystem som en viss, i förväg fastställd myndighet upprätthåller eller om att bedöma eller ha tillsyn över myndighetens åtgärder.

Vid bedömningen utreds det inte heller vilka uppgifter som registrerats i informationssystemet eller grunderna för att registrera dem.

Det föreslagna *2 mom.* innehåller en bestämmelse som berättigar finansministeriet att oberoende av sekretessbestämmelserna få upplysningar om slutresultaten av bedömningar som ministeriet har begärt. Upplysningarna bör dock begränsas till dem som är allra nödvändigast med avseende på bedömningens syfte.

Bestämmelsen behövs av tydlighetsskäl därför att det i 24 § 1 mom. 7 punkten i lagen om offentlighet i myndigheternas verksamhet föreskrivs att handlingar som gäller skyddsarrangemang för data- och kommunikationssystem och genomförandet av arrangemangen är sekretessbelagda, om det inte är uppenbart att utlämnandet av uppgifter ur en sådan handling inte äventyrar genomförandet av syftet med skyddsarrangemangen. Det är meningen att upplysningarna i regel ska ges på en sådan exakthetsnivå att lämnandet av upplysningar inte äventyrar genomförandet av syftet med skyddsarrangemangen.

6 §. *Kommunikationsverkets rätt att få uppgifter och rätt att få tillträde till lokaler och informationssystem.* Enligt *1 mom.* ska Kommunikationsverket oberoende av bestämmelserna om sekretessbelagda uppgifter ha rätt att få tillgång till uppgifter om informationssystem och datakommunikation som verket ska bedöma eller som är föremål för utredning samt, i den utsträckning det är nödvändigt för bedömningens utförande, att få tillträde till informationssystemet och till lokaler där uppgifter som ingår i systemet behandlas.

En sådan inspektion som avses i den föreslagna bestämmelsen är inte avsedd att omfatta hemfridsskyddade utrymmen. I den föreslagna bestämmelsen har det ansetts vara skäl att uttryckligen utesluta sådana utrymmen ur inspektionsrätten.

De föreslagna rättigheterna gäller också sakkunniga som Kommunikationsverket anlitar vid bedömningen.

7 §. *Bedömningsgrunder för informationssäkerhet.* I *1 mom.* definieras hurdana krav för fastställande av informationssäkerhetens nivå som kan användas när informationssäkerheten i myndigheternas informationssystem och datakommunikation bedöms. De krav som avses bli använda som bedömningsgrunder är desamma som bedömningsorgan som utför bedömningar av informationssäkerheten kan använda enligt lagförslag nr 1. Till denna del hänvisas det till det som konstateras i detaljmotiveringen till 10 § i det nämnda lagförslaget.

Enligt *2 mom.* ska Kommunikationsverket utreda om informationssystemet eller datakommunikationen uppfyller de krav angående informationssäkerheten som utgör bedömningsgrunder.

8 §. *Utfärdande av intyg.* Enligt *1 mom.* kan Kommunikationsverket på begäran utifrån en bedömning som verket har gjort utfärda intyg över informationssäkerheten i ett informationssystem eller datakommunikation.

I intyget ska enligt förslaget antecknas bedömningsgrunderna och uppgifter om bedömningens omfattning. Också giltighetstiden kan vid behov nämnas i intyget. Med detta refereras framför allt till intyg som utfärdats för viss tid.

Enligt *2 mom.* kan intyg utfärdas för viss tid, om det finns särskilda skäl till det.

9 §. *Upprätthållande och uppföljning av informationssäkerhetsnivån.* Informationssäkerhetsnivån kan förändras efter bedömningen. Därför är det befogat att den som önskar få ett intyg förbinder sig att framdeles sörja för informationssäkerhetsnivån. Den som fått ett intyg ska enligt förslaget också underrätta Kommunikationsverket om sådana ändringar som inverkar på informationssäkerhetsnivån. Likaså ska Kommunikationsverket ges tillträde till informationssystemen och datakommunikationen för säkerställande av att dessa alltjämt uppfyller de krav som anges i intyget.

10 §. *Återkallelse av intyg.* Kommunikationsverket kan på det sätt som det föreskrivs om i *1 mom.* återkalla ett intyg som verket har utfärdat, om det informationssystem eller den datakommunikation som bedömningen har gällt inte längre uppfyller de krav som har utgjort en förutsättning för utfärdande av intyget.

Enligt *2 mom.* ska Kommunikationsverket innan det träffar ett avgörande om återkallelse höra innehavaren av intyget och ge denne tillfälle att avhjälpa bristen. En tillräcklig tidsfrist för avhjälpande av bristen ska reserveras.

Enligt *3 mom.* kan Kommunikationsverket i sitt beslut om återkallelse av intyg bestämma att beslutet ska iakttas även om det överklagas, om inte besvärsmyndigheten bestämmer något annat.

11 §. *Ändringssökande.* Beslut om återkallelse av intyg som Kommunikationsverket har meddelat får enligt paragrafen överklagas genom besvär så som föreskrivs i förvaltningsprocesslagen.

12 §. *Avgifter.* Enligt förslaget ska det för Kommunikationsverkets bedömning, utfärdande av intyg och utredning tas ut en avgift av den som inlett ärendet enligt vad som föreskrivs i lagen om grunderna för avgifter till staten och i bestämmelser som utfärdats med stöd av den lagen.

13 §. *Ikraftträdande.* Lagen avses bli satt i kraft senast den 1 juni 2012. Skyldigheten enligt 3 § att anlita tjänster för bedömning av informationssäkerheten ska enligt den före-

slagna bestämmelsen vara fullgjord inom tre år från lagens ikraftträdande.

Åtgärder som krävs för verkställigheten av lagen får enligt förslaget vidtas innan lagen träder i kraft.

1.3 Lagen om kommunikationsförvaltningen

2 §. *Kommunikationsverkets uppgifter.* På grund av de nya uppgifter som föreslås för Kommunikationsverket i propositionen föreslås det att förteckningen i 1 § över uppgifter som ålagts verket i olika lagar kompletteras med hänvisningar till den föreslagna lagen om bedömningsorgan för informationssäkerhet och den föreslagna lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation.

2 Förhållande till grundlagen samt lagstiftningsordning

Enligt 18 § i grundlagen har var och en i enlighet med lag rätt att skaffa sig sin försörjning genom arbete, yrke eller näring som han eller hon valt fritt. Den föreslagna lagen om bedömningsorgan för informationssäkerhet ger företag som bedriver bedömningsverksamhet möjlighet att ansöka om godkännande hos Kommunikationsverket. Lagen föreslås dock inte innehålla bestämmelser om att bedömningsverksamheten ska vara en tillstånds- eller anmälningspliktig näring. Bedömningar ska därmed också i fortsättningen kunna göras utan att bedömningsverksamheten har godkänts av Kommunikationsverket.

Om myndighetens godkännande återkallas kan det i praktiken, trots det som sägs ovan, medföra en situation där bedömningsorganets förutsättningar att fortsätta sin verksamhet kan försvagas betydligt på grund av att godkännandet återkallats. Därför kan återkallelse av intyget vara av betydelse för den i 18 § i grundlagen tryggade näringsfriheten. I samband med regleringar av näringsverksamhet har grundlagsutskottets vedertagna tolkning varit att återkallelse av tillstånd är ett myndighetsingrepp i individens rättsliga ställning som har större konsekvenser än om ansökan hade avslagits. Med avseende på proportionalitetsaspekten har utskottet därför ansett det nödvändigt att binda möjligheten att återkalla tillstånd till allvarliga eller väsentliga förseelser eller försummelser och till att eventuella anmärkningar eller varningar som riktats mot tillståndshavaren inte har resulterat i att bristerna i verksamheten har avhjälpts (GrUU 8/2006 rd, s. 3/II, och de utlåtanden som det hänvisas till där).

De föreslagna förutsättningarna för återkallelse av godkännandet av bedömningsorgan ingår i lagförslaget (lagförslag nr 1, 8 §) och har sammanställts med beaktande av grundlagsutskottets ovan refererade utlåtandepraxis. Ändring i ett beslut om återkallelse av godkännande som Kommunikationsverket har meddelat får sökas genom besvär.

I de föreslagna lagarna ges Kommunikationsverket rätt att få tillträde till företagslokaler och till myndigheters lokaler. Det är inte vare sig avsikten eller nödvändigt att utsträcka den inspektion som avses i de föreslagna bestämmelserna till hemfridsskyddade utrymmen. Av tydlighetsskäl och i syfte att beakta grundlagsbestämmelserna om hemfrid utesluts sådana utrymmen uttryckligen ur inspektionsrätten i de föreslagna bestämmelserna (GrUU 2/2002 rd, GrUU 18/2006 rd). Eftersom grundlagen har en annan definition på vad som omfattas av hemfridsskyddet än till exempel strafflagen (SL 24:11), har begränsningen i enlighet med grundlagsutskottets ställningstaganden formulerats att avse utrymmen som används för permanent boende.

Med stöd av vad som anförts ovan kan lagförslagen behandlas i vanlig lagstiftningsordning.

3 Ikraftträdande

Lagarna föreslås träda i kraft senast den 1 juni 2012.

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

Lagförslag

1.

Lag

om bedömningsorgan för informationssäkerhet

I enlighet med riksdagens beslut föreskrivs:

1 kap.

Allmänna bestämmelser

1 §

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.

2 §

Lagens tillämpningsområde

Denna lag tillämpas på näringsidkare och på enheter som tillhandahåller serviceuppgifter för den offentliga förvaltningen 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 som gäller sammanslutningar föreskrivs särskilt.

2 kap.

Godkännande av och tillsyn över bedömningsorgan

3 §

Ansökan om godkännande av bedömningsorgan

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

De uppgifter som behövs för behandling av ärendet ska fogas till ansökan.

4 §

Behandlingen av ansökan

Innan ett bedömningsorgan för informationssäkerhet godkänns ska Kommunikationsverket ge skyddspolisen tillfälle att yttra sig om tillförlitligheten hos bedömningsor-

ganets ansvariga personer och om säkerheten i bedömningsorganets lokaler. När skyddspolisen sammanställer sitt utlåtande ska den iaktta det som föreskrivs i lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004).

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.

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) 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,

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).

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.

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 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 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

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 ligger till grund för utredningen (*bedömningsgrunder för informationssäkerhet*).

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 informationssäkerhetsnivån som använts vid bedömningen ska specificeras i intyget.

10 §

Bedömningsgrunder för informationssäkerhet

Som bedömningsgrunder för informationssäkerhet kan 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.

4 kap.

Särskilda bestämmelser

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 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).

14 §

Ikraftträdande

Denna lag träder i kraft den 20 .

Åtgärder som krävs för verkställigheten av denna lag får vidtas innan lagen träder i kraft.

2.

Lag

om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation

I enlighet med riksdagens beslut föreskrivs:

1 §

Lagens tillämpningsområde

I denna lag finns bestämmelser om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation.

Bestämmelser om Kommunikationsverkets uppgifter vid uppgörandet av säkerhetsutredningar som gäller sammanslutningar finns i lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004).

2 §

Definitioner

I denna lag avses med

1) *informationssystem* ett helhetsarrangemang som består av databehandlingsutrustning, program 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.

3 §

Anlitande av tjänster för bedömning av informationssäkerheten

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 (/20).

4 §

Kommunikationsverkets 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 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.

5 §

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 är nödvändigt 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.

7 §

Bedömningsgrunder för informationssäkerhet

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 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 vara också partiell.

8 §

Utfärdande av intyg

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.

Intyg kan utfärdas för viss tid, om det finns särskilda skäl till det.

9 §

Upprätthållande och uppföljning av informationssäkerhetsnivån

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.

10 §

Återkallelse av intyg

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.

11 §

Ändringssökande

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 av 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.

13 §

Ikraftträdande

Denna lag träder i kraft den 20 . Statsförvaltningsmyndigheterna ska inom tre år från lagens ikraftträdande se till att anlitandet av externa bedömningstjänster motsvarar skyldigheterna enligt 3 §.

Åtgärder som krävs för verkställigheten av denna lag får vidtas innan lagen träder i kraft.

3.

Lag

om ändring av 2 § i lagen om kommunikationsförvaltningen

I enlighet med riksdagens beslut

ändras i lagen om kommunikationsförvaltningen (625/2001) 2 § 1 punkten, sådan den lyder i lag 886/2010, som följer:

2 §

Kommunikationsverkets uppgifter

Kommunikationsverket har till uppgift att

1) sköta de uppgifter som enligt kommunikationsmarknadslagen (393/2003), lagen om radiofrekvenser och teleutrustningar (1015/2001), postlagen (415/2011), lagen om televisions- och radioverksamhet (744/1998), lagen om statens televisions- och radiofond (745/1998), lagen om dataskydd vid elektronisk kommunikation (516/2004), lagen om förbud mot vissa avkodningssystem (1117/2001), lagen om stark autentisering och elektroniska signaturer (617/2009), lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004), lagen om bedömningsorgan för informationssäkerhet (/20), lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (/20) samt lagen om domännamn (228/2003) ankommer på Kommunikationsverket,

— — — — — — — — — — — — — —

———

Denna lag träder i kraft den 20 .

Åtgärder som krävs för verkställigheten av denna lag får vidtas innan lagen träder i kraft.

———

Helsingfors den 5 oktober 2011

Republikens President

TARJA HALONEN

Justitieminister *Anna-Maja Henriksson*

Bilaga
Parallelltext

3.

Lag

om ändring av 2 § i lagen om kommunikationsförvaltningen

I enlighet med riksdagens beslut
ändras i lagen om kommunikationsförvaltningen (625/2001) 2 § 1 punkten, sådan den lyder i lag 886/2010, som följer:

Gällande lydelse	*Föreslagna lydelse*
2 §	2 §
Kommunikationsverkets uppgifter	*Kommunikationsverkets uppgifter*
Kommunikationsverket har till uppgift att 1) sköta de uppgifter som enligt kommunikationsmarknadslagen (393/2003), lagen om radiofrekvenser och teleutrustningar (1015/2001), lagen om posttjänster (313/2001), lagen om televisions- och radioverksamhet (744/1998), lagen om statens televisions- och radiofond (745/1998), lagen om dataskydd vid elektronisk kommunikation (516/2004), lagen om förbud mot vissa avkodningssystem (1117/2001), lagen om stark autentisering och elektroniska signaturer (617/2009), lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004) samt lagen om domännamn (228/2003) ankommer på Kommunikationsverket,	Kommunikationsverket har till uppgift att 1) sköta de uppgifter som enligt kommunikationsmarknadslagen (393/2003), lagen om radiofrekvenser och teleutrustningar (1015/2001), postlagen (415/2011), lagen om televisions- och radioverksamhet (744/1998), lagen om statens televisions- och radiofond (745/1998), lagen om dataskydd vid elektronisk kommunikation (516/2004), lagen om förbud mot vissa avkodningssystem (1117/2001), lagen om stark autentisering och elektroniska signaturer (617/2009), lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004)*, lagen om bedömningsorgan för informationssäkerhet (/20), lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (/20)* samt lagen om domännamn (228/2003) ankommer på Kommunikationsverket,
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

———

Denna lag träder i kraft den 20 .
Åtgärder som krävs för verkställigheten av denna lag får vidtas innan lagen träder i kraft.