

FÖRVALTNINGSUTSKOTTETS UTLÅTANDE 20/2011 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

Till kommunikationsutskottet

INLEDNING

Remiss

Riksdagen remitterade den 13 oktober 2011 en 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 (RP 45/2011 rd) till kommunikationsutskottet för beredning och bestämde samtidigt att förvaltningsutskottet ska lämna utlåtande i ärendet till kommunikationsutskottet.

Sakkunniga

Utskottet har hört

- lagstiftningsråd Anna-Riitta Wallin, justitieministeriet
- konsultativ tjänsteman Timo Kievari, kommunikationsministeriet
- IT-direktör Mikael Kiviniemi, finansministeriet
- direktör Timo Lehtimäki, Kommunikationsverket.

Dessutom har skriftligt utlåtande lämnats av

- skyddspolisen
- Finlands näringsliv.

PROPOSITIONEN

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 företags säkerheten 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 verkställig-

heten 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 myndighetersnas 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.

UTSKOTTETS ÖVERVÄGANDEN

Motivering

Allmänt

I propositionen förslås en lag om bedömningsorgan för informationssäkerhet och en lag om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation. Ytterligare föreslås vissa ändringar i lagen om kommunikationsförvaltning (625/2001) när det gäller Kommunikationsverkets uppgifter.

Utskottet anser att den föreslagna helheten av lagar och lagändringar är välkommen. Den föreslagna bedömnings- och utredningsverksamheten kan förväntas bidra till att kraven på informationssäkerhet implementeras och utnyttjas både i företag och statsförvaltningen, vilket skulle resultera i en nivåförhöjning av den nationella informationssäkerheten. Det här är förenligt med statsrådets principbeslut om informationssäkerhet och säkerhetsnätverk inom förvaltningen. Utskottet hänvisar till de synpunkter som redovisas nedan och förordar lagförslagen.

Lag om bedömningsorgan för informationssäkerhet

Genom lagen om bedömningsorgan för informationssäkerheten skapas ett system genom vilket företagen kan utveckla informationssäkerheten med hjälp av dels gemensamma kriterier, dels bedömningsorgan som står under myndighetstillsyn. I lagen ges bedömningsorganen en möjlighet att ansöka om godkännande av sin verksamhet hos Kommunikationsverket. Bedömningsorganet ska utvärdera informationssäker-

heten i ett företag i förhållande till på förhand fastställda säkerhetskriterier. Dessa kan vara fastställda i lag eller t.ex. standarder. Valet av vilka kriterier bedömningen görs mot avgörs av det företag som begär en bedömning. Kommunikationsverket övervakar bedömningsorganen.

Utskottet anser att lagförslaget är behövligt. Vår gällande lagstiftning saknar för närvarande bestämmelser om organ som utför bedömningar av informationssäkerhet. I lagen om konstaterande av tillförlitligheten hos tjänster för bedömning av överensstämmelse med kraven (920/2005) föreskrivs om ett nationellt ackrediteringssystem som har till syfte att säkerställa tillförlitligheten av tjänster för bedömning av överensstämmelse med kraven samt deras internationella godtagbarhet. I lagen om säkerhetsutredningar (177/2002) föreskrivs om säkerhetsutredningar av enskilda personer.

Utskottet anser att det föreslagna systemet förbättrar företagssäkerheten och företags möjligheter att skydda sig mot hot som riktas mot deras informationssystem. Lagförslaget förbättrar också de europeiska företagens konkurrenskraft. Lagstiftningen skulle ge företag möjligheter att bättre än för närvarande bereda sig t.ex. inför internationella upphandlingstävlingar som kräver en myndighetsutförd säkerhetsutredning med intyg. Företagens möjligheter att med hjälp av myndighetsövervakade bedömningsorgan bevisa nivån på den egna informationssäkerheten är av betydelse också t.ex. i samband med teknologiska utvecklingsprojekt där flera aktörer samarbetar och utbyter affärshemligheter.

Lag om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation

I förslaget till lag om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation föreslås att Kommunikationsverket ska bedöma myndigheternas informationssystem och datakommunikation och utfärda intyg över system som uppfyller kraven. 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. Dessutom kan finansministeriet be Kommunikationsverket göra en utredning om den allmänna nivån på informationssäkerheten i statsförvaltningsmyndigheternas informationssystem eller datakommunikation.

Lagförslaget har samband med verkställigheten 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.

Den gällande lagstiftningen innehåller inga bestämmelser om genom vilket förfarande myndigheterna skulle kunna få en tillförlitlig bedömning av säkerhetsnivån på sina informationssystem och datakommunikationsarrangemang. Lagförslaget kompletterar alltså på ett relevant sätt den gällande lagstiftningen. Lagen behövs också för att säkerställa 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.

Genom lagförslaget blir det möjligt för Kommunikationsverket att använda också extern expertis i utvärderingsuppdrag. Experten agerar då på uppdrag av Kommunikationsverket och för

dess räkning. I förslaget till 6 § föreskrivs om rätt för Kommunikationsverkets sakkunniga att få uppgifter. Rätten till information är inte obegränsad utan Kommunikationsverket och den som handlar på uppdrag av verket har endast rätt att få tillgång till uppgifter om informationssystem och datakommunikation 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 experts rätt till uppgifter begränsas dessutom av uppdragets innehåll.

Utskottet understyrker att såväl Kommunikationsverket som den expert som handlar på verkets uppdrag är bundna av den sekretess som framgår av lagen om offentlighet i myndigheternas verksamhet, nedan offentlighetslagen (621/1999). Enligt 23 § 2 mom. i offentlighetslagen gäller sekretessplikten även den som verkar på uppdrag av en myndighet eller som är anställd hos den som utför ett myndighetsuppdrag. Det är därmed klart att företag och personer som handlar i bedömningsuppgifter på uppdrag av Kommunikationsverket har sekretessplikt i fråga om sådana sekretessbelagda uppgifter som de fått vetskap om när de fullgjort sitt uppdrag. Enligt offentlighetslagen får den som utför ett uppdrag inte heller annars röja en myndighetshandlings sekretessbelagda innehåll utan det är alltid myndigheten själv som beslutar om lämnande av sådana uppgifter. Enligt 22 § 1 mom. i offentlighetslagen skapar sekretessplikten samtidigt en skyldighet att hemlighålla handlingar.

I 26 § 3 mom. i offentlighetslagen ingår allmänna bestämmelser om utlämning av sekretessbelagda uppgifter för skötseln av uppdrag. Enligt lagrummet får en myndighet lämna ut uppgifter ur en sekretessbelagd handling för något annat uppdrag bara om detta är nödvändigt för att uppdraget ska kunna skötas. Myndigheten ska dessutom på förhand försäkra sig om att uppgifterna kommer att hemlighållas och skyddas på behörigt sätt. Utskottet framhåller att bedömning av säkerhetsnivån på informationssystem och datakommunikationssystem inte kräver tillgång till de uppgifter som hanteras eller överförs och att bedömningen kan göras också i min-

dre delar som inte möjliggör en bedömning av nivå på informationssäkerheten som en helhet.

Kommunikationsverket handlar under tjänsteansvar när det fattar sina beslut om expertuppdrags omfattning och inriktning samt med beaktande av de ovan refererade lagbestämmelserna. De personer inom Kommunikationsverket som sköter sådana bedömningsuppgifter som det är fråga om här omfattas av den säkerhetsutredning som avses i lagen om säkerhetsutredningar. Enligt utskottets uppfattning kan i praktiken endast personer om vilka en säkerhetsutredning har gjorts utföra uppdrag.

Utskottet anser att man i de föreslagna lagarna på behörigt sätt har beaktat också synpunkter som gäller informationssystem och datakommunikationssystem som omfattas av de högsta säkerhetskraven. De föreslagna bestämmelserna är inte heller något hinder för att den myndighet som begär en bedömning ger uttryck för sin egen uppfattning om hur och med vilken typ av uppdrag experter kan användas vid utvärderingen. En myndighet kan också återkalla sin begäran om den anser att Kommunikationsverkets plan för hur bedömningen ska gå till inte är saklig.

Utlåtande

Utskottet föreslår

att kommunikationsutskottet beaktar det som sägs ovan.

Helsingfors den 10 november 2011

I den avgörande behandlingen deltog

ordf. Jussi Halla-aho /saf
vordf. Maarit Feldt-Ranta /sd
medl. Heikki Autto /saml
Rakel Hiltunen /sd
Reijo Hongisto /saf
Risto Kalliorinne /vänst
Mika Kari /sd
Elsi Katainen /cent

Timo V. Korhonen /cent
Antti Lindtman /sd
Tapani Mäkinen /saml
Markku Mäntymaa /saml
Osmo Soininvaara /gröna
Ulla-Maj Wideroos /sv
ers. Anne Holmlund /saml.

Sekreterare var

utskottsråd Minna-Liisa Rinne.