KOMMUNIKATIONSUTSKOTTETS BETÄNKANDE 9/2011 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

INLEDNING

Remiss

Riksdagen remitterade den 13 oktober 2011 en proposition 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.

Utlåtande

I enlighet med riksdagens beslut har förvaltningsutskottet lämnat utlåtande i ärendet. Utlåtandet (FvUU 20/2011 rd) återges efter betänkandet.

Sakkunniga

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

Dessutom har skriftligt utlåtande lämnats av
— Dataombudsmannens byrå
— Huvudstaben
— Försörjningsberedskapscentralen
— Inspecta Oy
— KPMG.

PROPOSITIONEN

I propositionen 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.

UTSKOTTETS ÖVERVÄGANDEN

Allmän motivering

Sammantaget sett anser utskottet propositionen vara behövlig och angelägen. Utskottet tillstyrker lagförslagen, men med följande kommentarer och ändringsförslag.

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.

Enligt kommunikationsutskottets uppfattning är förslagen motiverade. I dagens informationssamhälle måste såväl företag som myndigheter ha en hög nivå på informationssäkerheten för att kunna verka framgångsrikt. I propositionen föreslås det att företag och aktörer inom den offentliga sektorn ska få en möjlighet att utveckla och höja nivån på sin informationssäkerhet med hjälp av en extern bedömning som görs utifrån lagfästa bedömningskriterier.

Utskottet anser att propositionen förbättrar finländska företags konkurrenskraft och deras möjligheter att göra sig gällande i internationella anbudstävlingar. Propositionen skapar möjligheter för myndigheterna att bevisa sin egen säkerhetsnivå t.ex. med avseende på internationellt myndighetssamarbete. Tillförlitliga bedömningsförfaranden bidrar till att höja nivån på informationssäkerheten såväl i företag som inom den offentliga förvaltningen.

Kommunikationsutskottet omfattar förvaltningsutskottets uppfattning (FvUU 20/2011 rd) om att man i de föreslagna lagarna på behörigt sätt har beaktat också synpunkter som gäller informationssystem och datakommunikationssystem som omfattas av de högsta säkehetskraven.

Kommunikationsutskottet anser propositionen vara lämplig och uttalar sitt stöd för den. Utskottet föreslår trots det vissa ändringar i den föreslagna lagen.

Detaljmotivering

1. Lagförslag

9 §. Bedömningsorganens uppgifter. Utskottet uppmärksammar att lagförslag 1 nämner att bedömningen också kan vara partiell och alltså gälla endast t.ex. en viss funktion inom ett företag. Utskottet föreslår därför att till 9 § fogas ett nytt 2 mom. som uttryckligen säger att bedömningen kan vara partiell, om den som begär bedömningen så önskar. Det föreslagna 2 mom. blir därmed 3 mom.

Kommunikationsutskottet anser det viktigt att också en utomstående, och i synnerhet den som företaget lämnar intyget över bedömningen till, ska kunna avgöra den faktiska betydelsen för informationssäkerheten av en sådan bedömning som avses i lagförslaget. Utskottet föreslår därför en sådan komplettering i 9 § 3 mom. att det av intyget över bedömningen ska framgå inte bara bedömningsgrunderna utan också bedömningens omfattning. Det här är viktigt för att säkerställa att intyget ger en korrekt bild av bedömningen. I momentet föreslås dessutom en

korrigering av teknisk natur så att ordet informationssäkerhetsnivån ändras till informationssäkerheten.

10 §. Bedömningsgrunder för informationssäkerhet. Ett företag avgör själv om det vill utnyttja den service i form av bedömning av säkerhetsnivån som utförs av sådana bedömningsorgan som avses i propositionen. Företaget står också för kostnaderna för bedömningen. Det är därför också klart att företaget, eller någon annan som vill ha en extern och tillförlitlig bedömning, själv ska kunna välja vilka lagfästa bedömningskriterier som ska användas vid bedömningen. Utskottet menar att denna möjlighet att välja är nödvändig med tanke på att bedömningsbehoven och bedömningssituationerna varierar så starkt.

I propositionen föreslås flera bestämmelser som syftar till att säkerställa ett sakligt val av bedömningsgrunder. Enligt propositionen åläggs godkända bedömningsorgan i 9 § 1 mom. en skyldighet att iaktta omsorg i sin verksamhet. Dessutom ska organet när det utför i lagen avsedda uppdrag följa vissa bestämmelser som i regel gäller myndighetsverksamhet, t.ex. förvaltningslagens (434/2003) principer om service och rådgivning. Ett godkänt bedömningsorgan ska också främja öppenhet i sin verksamhet och i detta syfte publicera handböcker, statistik och andra publikationer samt informationsmaterial om sin service. Även om de företag som utnyttjar godkända bedömningsorgans tjänster i regel själva har sakkunskap om informationssäkerhet, bidrar de nämnda kraven och förfaringssätten i lagförslagen till att säkerställa att företagen utifrån tillräcklig och saklig information samt kompetens väljer vilka bedömningsgrunder som ska användas vid bedömningen. Utskottet finner det viktigt att också den myndighet som övervakar bedömningsorganen ser till att den valfrihet i fråga om bedömningsgrunderna som nu föreslås inte heller i praktiken leder till problem för bedömningsverksamheten eller dess tillförlitlighet.

Utskottet föreslår för klarhetens skull att det inledande stycket i 10 § ändras så att det av bestämmelsen klart framgår att bedömningsobjektet själv väljer vilka bedömningsgrunderna ska vara.

Utskottets förslag till beslut

Riksdagen

godkänner lagförslag 2 och 3 utan ändringar,

godkänner lagförslag 1 enligt propositionen men 9 och 10 § med följande ändringar ***(Utskottets ändringsförslag)****.*

Utskottets ändringsförslag

9 §

Bedömningsorganens uppgifter

(1 mom. som i RP)

Bedömningen kan även vara partiell. (Nytt 2 mom.)

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. *(2 mom. som i RP)*

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 säkerhetsmyndig-

het 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.

Helsingfors den 18 november 2011

I den avgörande behandlingen deltog

ordf. Arto Satonen /saml
vordf. Osmo Kokko /saf
medl. Mikko Alatalo /cent
Thomas Blomqvist /sv
Ari Jalonen /saf
Merja Kuusisto /sd
Suna Kymäläinen /sd
Johanna Ojala-Niemelä /sd
Raimo Piirainen /sd
Eila Tiainen /vänst
Ari Torniainen /cent
Oras Tynkkynen /gröna
Mirja Vehkaperä /cent.

Sekreterare var

utskottsråd Juha Perttula.