

RIKSDAGENS SVAR 59/2011 rd

Regeringens 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

Ärende

Regeringen har till riksdagen överlämnat sin 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).

Beredning i utskott

Kommunikationsutskottet har i ärendet lämnat sitt betänkande (KoUB 9/2011 rd).

Beslut

Riksdagen har antagit följande lagar:

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 sört 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 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 bedömningsorganets 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 ut-

satt tid. Om bristen inte avhjälpas 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 iakttas 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.

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.

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 iakttä 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.

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, 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.

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 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.

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 även vara 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 om-

fattning 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 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.

13 §

Ikraftträdande

Denna lag träder i kraft den 20 Statsförvaltningsmyndigheterna ska inom tre år från lagens ikraftträdande se till att anlita av externa bedömningstjänster motsvarar skyldigheterna enligt 3 §. Åtgärder som krävs för verkställigheten av denna lag får vidtas innan lagen träder i kraft.

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 29 november 2011
