FINLANDS FÖRFATTNINGSSAMLING

Utgiven i Helsingfors den 28 december 2011

1405/2011

Lag

om bedömningsorgan för informationssäkerhet

Utfärdad i Helsingfors den 22 december 2011

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 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.

RP 45/2011
KoUB 9/2011
RSv 59/2011

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 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 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 iaktta förvaltningslagen (434/2003), lagen om offentlighet i myndigheternas verksamhet (621/1999) och språklagen (423/2003).

14 §

Ikraftträdande

Denna lag träder i kraft den 1 juni 2012.

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

Helsingfors den 22 december 2011

Republikens President

TARJA HALONEN

Justitieminister *Anna-Maja Henriksson*

UTGIVARE: JUSTITIEMINISTERIET EDITA PRIMA AB / EDITA PUBLISHING AB ISSN 1456-9663 / 0787-3182 (tryckt)