

FINLANDS FÖRFATTNINGSSAMLING

Utgiven i Helsingfors den 28 december 2011

1406/2011

Lag

om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation

Utfärdad i Helsingfors den 22 december 2011

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 (1405/2011).

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 informa-

tionssystem 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 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.

Helsingfors den 22 december 2011

Republikens President

TARJA HALONEN

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 iaktas 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 1 juni 2012.

Statsförvaltningsmyndigheterna ska inom tre år från lagens ikraftträdande se till att anlita det av externa bedömningstjänster motsvarar skyldigheterna enligt 3 §.

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

Justitieminister *Anna-Maja Henriksson*