

SUOMEN SÄÄDÖSKOKOELMA

Julkaistu Helsingissä 28 päivänä joulukuuta 2011

1406/2011

Laki

viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista

Annettu Helsingissä 22 päivänä joulukuuta 2011

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Lain soveltamisala

Tässä laissa säädetään viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista.

Viestintäviraston tehtävistä yhteisöturvallisuusselvityksiä laadittaessa säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004).

2 §

Määritelmät

Tässä laissa tarkoitetaan:

1) *tietojärjestelmällä* tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä;

2) *tietoliikennejärjestelyllä* tiedonsiirtoverkosta, tiedonsiirtolaitteista, ohjelmistoista ja muista tietojenkäsittelystä koostuvista järjestelyistä muodostuvaa järjestelmää;

3) *viranomaisella* viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 4 §:n 1 momentin 1—7 kohdassa tarkoitettuja toimielimiä;

4) *valtionhallinnon viranomaisella* valtion hallintoviranomaisia ja muita valtion virastoja ja laitoksia sekä tuomioistuimia ja muita lainkäyttöviranomaisia.

3 §

Tietoturvallisuuden arviointipalvelujen käyttäminen

Valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnissa vain tässä laissa tarkoitettua menettelyä taikka sellaista arviointilaitosta, joka on saanut Viestintäviraston hyväksynnän tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) mukaan.

4 §

Viestintäviraston tehtävät

Viestintäviraston tehtävänä on viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden edistämiseksi ja varmistamiseksi:

1) arvioida viranomaisen pyynnöstä tämän määräämisvallassa olevan tai hankittavaksi suunnitteleman tietojärjestelmän tai tietoliikennejärjestelyjen tietoturvallisuuden vaatimustenmukaisuutta;

2) antaa tietojärjestelmälle tai tietoliikennejärjestelylle sen hyväksymistä osoittava todistus 8 §:ssä säädetyllä tavalla;

3) tehdä valtiovarainministeriön pyynnöstä selvityksiä valtionhallinnon viranomaisen

määräamisvallassa olevien tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta.

Edellä 1 momentin 1 ja 2 kohdassa tarkoitettua pyynnön voi viranomaisen toimeksiannosta tehdä myös se, joka tekee viranomaisen lukuun hankintoja taikka tuottaa tietojenkäsittely- tai tietoliikennepalveluja taikka hoitaa niiden järjestämiseen liittyviä palvelutehtäviä.

Viestintävirasto suorittaa tässä laissa tarkoitettua tehtävää käytettävissään olevien voimavarojen mukaisesti ottaen huomioon kansainvälisten tietoturvallisuusvelvoitteiden noudattaminen sekä pyydettyjen toimenpiteiden merkitys viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden yleiseen parantamiseen.

5 §

Selvitykset valtiovarainministeriön toimeksiannosta

Valtiovarainministeriö voi pyytää valtionhallinnon tietoturvallisuudesta annettujen säännösten täytäntöönpanon seuraamiseksi sekä niiden kehittämiseksi Viestintävirastoa laatimaan selvityksen valtionhallinnon viranomaisten tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta. Selvityksen piiriin tulevat tietojärjestelmät voidaan määritellä tietojärjestelmien käyttötarkoituksen, niihin talletettavien tietojen laadun tai muun vastaavan yleisen tekijän mukaan.

Viestintävirasto voi salassapitosäännösten estämättä sisällyttää valtiovarainministeriölle antamaansa arvioon sellaisia tietoja, jotka ovat välttämättömiä arvioinnin tarkoituksen toteuttamiseksi.

6 §

Viestintäviraston tiedonsaantioikeus ja oikeus päästä tiloihin ja tietojärjestelmiin

Viestintävirastolla ja sen toimeksiannosta toimivalla asiantuntijalla on oikeus sen estämättä, mitä tietojen salassapidosta säädetään, saada käyttöönsä Viestintäviraston arvioitava tai selvityksen kohteena olevaa tietojär-

jestelmää tai tietoliikennejärjestelyjä koskevat tiedot sekä oikeus siinä laajuudessa kuin se on tarpeen arvioinnin suorittamiseksi päästä tietojärjestelmään tai tiloihin, joissa siihen kuuluvia tietoja käsitellään.

Edellä 1 momentissa tarkoitettua tarkastusta ei saa suorittaa pysyväisluonteiseen asumiseen käytetyissä tiloissa.

7 §

Tietoturvallisuuden arviointiperusteet

Viestintävirasto voi käyttää viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointiperusteina:

1) lailla tai asetuksella säädettyjä viranomaisten toimintaa koskevia tietoturvallisuusvaatimuksia ja valtiovarainministeriön tietoturvallisuutta koskevia ohjeita;

2) kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitettua kansallisen turvallisuusviranomaisen antamia kansainvälisten tietoturvallisuusvelvoitteiden toteuttamista koskevia ohjeita;

3) Euroopan unionin tai muun kansainvälisen toimielimen antamia tietoturvallisuutta koskevia säännöksiä ja ohjeita;

4) julkaistuja ja yleisesti tai alueellisesti sovellettuja tietoturvallisuutta koskevia säännöksiä, määräyksiä tai ohjeita;

5) vahvistettuun standardiin sisältyviä tietoturvallisuutta koskevia vaatimuksia.

Viestintävirasto selvittää, täyttääkö tietojärjestelmä tai tietoliikennejärjestely ne tietoturvallisuutta koskevat vaatimukset, jotka on otettu arviointiperusteeksi. Arviointi voidaan tehdä myös osittaisena.

8 §

Todistuksen antaminen

Viestintävirasto voi pyydettyään antaa todistuksen tietoturvallisuutta koskevat vaatimukset täyttävästä tietojärjestelmästä tai tietoliikennejärjestelystä. Todistukseen merkitään käytetyt arviointiperusteet sekä tiedot arvioinnin laajuudesta sekä tarvittaessa todistuksen voimassaoloajasta.

Todistus voidaan antaa määräajaksi, jos siihen on erityinen syy.

9 §

Tietoturvallisuuden tason ylläpito ja seuranta

Sen, joka haluaa 8 §:ssä tarkoitetun todistuksen, on annettava sitoumus tietoturvasuustason säilyttämisestä. Todistuksen saaneen on ilmoitettava Viestintävirastolle sellaisista muutoksista, joilla on vaikutusta tietoturvasuustason, sekä sallittava Viestintävirastolle pääsy tietojärjestelmiin ja tietoliikennejärjestelyihin sen selvittämiseksi, täyttävätkö ne edelleen todistuksen mukaiset vaatimukset.

10 §

Todistuksen peruuttaminen

Viestintävirasto voi peruuttaa tämän lain nojalla annetun todistuksen, jos arvioinnin kohteena ollut tietojärjestelmä tai tietoliikennejärjestely ei enää täytä niitä vaatimuksia, jotka ovat olleet edellytyksenä todistuksen antamiselle.

Viestintäviraston on ennen 1 momentissa tarkoitettua ratkaisun tekemistä kuultava todistuksen saanut sekä varattava tälle tilaisuus korjata puute.

Viestintävirasto voi 1 momentissa tarkoitettussa päätöksessään määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta,

Helsingissä 22 päivänä joulukuuta 2011

Tasavallan Presidentti

TARJA HALONEN

jollei muutoksenhakuviranomainen toisin määrää.

11 §

Muutoksenhaku

Muutoksenhausta Viestintäviraston tämän lain nojalla tekemään päätökseen säädetään hallintolainkäyttölaissa (586/1996).

12 §

Maksut

Asian vireille saattajalta Viestintäviraston arvioinnista, todistuksen antamisesta ja selvityksestä perittävistä maksuista säädetään valtion maksuperustelaisissa (150/1992) ja sen nojalla.

13 §

Voimaantulo

Tämä laki tulee voimaan 1 päivänä kesäkuuta 2012.

Valtionhallinnon viranomaisten on saatettava ulkopuolisten arviointipalvelujen käyttö vastaamaan 3 §:n velvoitteita kolmen vuoden kuluessa lain voimaantulosta.

Ennen lain voimaantuloa voidaan ryhtyä lain täytäntöönpanon edellyttämiin toimenpiteisiin.

Oikeusministeri *Anna-Maja Henriksson*