

EDUSKUNNAN VASTAUS 59/2011 vp

Hallituksen esitys laeiksi tietoturvallisuuden arviointilaitoksista, viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista sekä viestintähallinnosta annetun lain 2 §:n muuttamisesta

Asia

Hallitus on antanut eduskunnalle esityksensä laeiksi tietoturvallisuuden arviointilaitoksista, viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista sekä viestintähallinnosta annetun lain 2 §:n muuttamisesta (HE 45/2011 vp).

Valiokuntakäsittely

Liikenne- ja viestintävaliokunta on antanut asiasta mietinnön (LiVM 9/2011 vp).

Päätös

Eduskunta on hyväksynyt seuraavat lait:

Laki

tietoturvallisuuden arviointilaitoksista

Eduskunnan päätöksen mukaisesti säädetään:

1 luku

Yleiset säännökset

1 §

Lain tarkoitus

Tässä laissa säädetään menettelystä, jonka avulla yritykset voivat osoittaa luotettavasti ulkopuolisille, että niiden toiminnassa on toteutettu määrätty tietoturvallisuuden taso.

2 §

Lain soveltamisala

Tätä lakia sovelletaan elinkeinonharjoittajiin ja palvelutehtäviä julkishallinnolle tarjoaviin yksiköihin, jotka toimeksiannosta arvioivat tietoturvaluustason (*tietoturvallisuuden arviointilaitos*) ja jotka haluavat toiminnalleen Viestintäviraston hyväksynnän. Lisäksi tätä lakia sovelletaan hyväksymismenettelyyn.

Viestintäviraston tehtävistä viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnissa sekä yhteisöturvallisuusselvitysten laadinnassa säädetään erikseen.

2 luku

Arviointilaitoksen hyväksyminen ja valvonta

3 §

Arviointilaitoksen hyväksymistä koskeva hakemus

Tietoturvallisuuden arviointilaitos voi hakea Viestintäviraston hyväksyntää toimintaansa varten.

Hakemukseen on liitettävä tiedot, jotka ovat tarpeen asian käsittelyä varten.

4 §

Hakemuksen käsittely

Viestintäviraston on ennen tietoturvallisuuden arviointilaitoksen hyväksymistä varattava suojelupoliisille tilaisuus lausua arviointilaitoksen vastuuhenkilöiden luotettavuudesta ja sen toimitilojen turvallisuudesta. Suojelupoliisi noudattaa lausuntoaan laatiessaan, mitä kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004) säädetään.

Viestintävirasto voi hakemusta käsitellessä hankkia lausuntoja sekä antaa hakemuksen ja siinä esitettyjen tietojen arvioimiseksi toimeksiannostaan suoritettavia tehtäviä ulkopuolisille asiantuntijoille.

5 §

Arviointilaitoksen hyväksyminen

Tietoturvallisuuden arviointilaitoksen hyväksymisen edellytyksenä on, että:

1) laitos on toiminnallisesti ja taloudellisesti riippumaton arvioinnin kohteesta;

2) laitoksen henkilökunnalla on hyvä tekninen ja ammatillinen koulutus sekä riittävän laaja-alainen kokemus toimintaan kuuluvissa tehtävissä;

3) laitoksella on toiminnan edellyttämät laitteet, välineet ja järjestelmät;

4) laitoksen vastuuhenkilöiden luotettavuus on varmistettu ja laitoksella on luotettavaksi arvioitu ja valvottu menetelmä, jonka avulla laitoksen toimitilojen ja tietojenkäsittelyn turvallisuus varmistetaan;

5) laitoksella on asianmukaiset ohjeet toimintaansa ja sen seuranta varten.

Edellä 1 momentin 1—3 kohdassa tarkoitettujen vaatimusten täyttäminen on osoitettava vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annetussa laissa (920/2005) säädetyn menettelyn avulla.

Viestintävirasto hyväksyy saamiensa ja laatimiensa selvitysten sekä suorittamiensa tarkastusten perusteella vaatimukset täyttävän laitoksen hyväksytyksi tietoturvallisuuden arviointilaitokseksi. Tällainen laitos voi markkinoinnissaan ja muussa viestinnässään käyttää Viestintäviraston hyväksymistä koskevaa ilmaisua edellyttäen, ettei hyväksymisen voimassaoloa koskeva määräaika ole päättynyt tai Viestintävirasto ole päättänyt peruuttaa hyväksynnän.

Arviointilaitos voidaan hyväksyä määräajaksi, jos siihen on erityinen syy. Hyväksymistä koskevaan päätökseen voidaan sisällyttää arviointilaitoksen pätevyysaluetta, valvontaa sekä sellaisia toimintaa koskevia rajoituksia ja ehtoja, jotka ovat tarpeen arviointilaitoksen tehtävien asianmukaisen hoidon varmistamiseksi.

6 §

Arviointilaitoksen hyväksymisen peruuttaminen

Jos hyväksytty tietoturvallisuuden arviointilaitos toimii olennaisesti tai jatkuvasti säännösten vastaisesti taikka jos se ei enää täytä hyväksymiselle asetettuja vaatimuksia, Viestintäviraston on kehoitettava arviointilaitosta korjaamaan puute määräajassa. Jos puutetta ei korjata määräajassa, Viestintävirasto voi peruuttaa hyväksymisen.

Viestintävirasto voi päätöksessään määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta, jollei muutoksenhakuviranomainen toisin määrää.

7 §

Viestintäviraston tarkastusoikeus

Viestintävirastolla ja sen toimeksiannosta toimivalla asiantuntijalla on oikeus tarkastaa hyväksyntää hakeneen tai hyväksytyn tietoturvallisuuden arviointilaitoksen tilat sekä sen käytössä olevat menetelmät. Tarkastusta ei saa suorittaa pysyväisluonteiseen asumiseen käytetyissä tiloissa.

8 §

Arviointilaitoksen tiedonanto- ja ilmoitusvelvollisuus

Hyväksytyn tietoturvallisuuden arviointilaitoksen on ilmoitettava Viestintävirastolle sellaisesta toimintaansa koskevasta muutoksesta, jolla on merkitystä laitosta koskevien velvoitteiden kannalta.

Viestintävirastolla on sen lisäksi, mitä 1 momentissa säädetään, oikeus pyynnöstä saada arviointilaitokselta ne tiedot, jotka ovat tarpeen sen valvomiseksi, että laitos täyttää toimintaansa koskevat vaatimukset.

3 luku

Tietoturvallisuuden arviointi

9 §

Arviointilaitoksen tehtävät

Hyväksytyn tietoturvallisuuden arviointilaitoksen on saamaansa tietoturvallisuuden arviointitehtävää suorittaessaan noudatettava huolellisuutta ja pidettävä huolta siitä, että arvioinnin aikana:

- 1) tarkastetaan arvioinnin kohteen toimitilat;
- 2) selvitetään, onko arvioinnin kohteen toiminnassa asianmukaisella tavalla toteutettu 10 §:ssä tarkoitetut tietoturvallisuutta koskevat vaatimukset, jotka on otettu selvityksen perustaksi (*tietoturvallisuuden arviointiperusteet*).

Arviointi voidaan tehdä myös osittaisena.

Hyväksytty tietoturvallisuuden arviointilaitos antaa selvitysten ja tarkastuksen perusteella todistuksen, jos arvioitavan kohteen toimitilat ja toiminta on selvityksen perustana olleiden arviointiperusteiden mukainen. Todistuksessa tulee yksilöidä arvioinnissa käytetyt tietoturvallisuuden arviointiperusteet ja arvioinnin laajuus.

10 §

Tietoturvallisuuden arviointiperusteet

Tietoturvallisuuden arviointiperusteina voidaan tässä laissa tarkoitetussa arvioinnissa käyttää arvioinnin kohteen valinnan mukaan:

- 1) lailla tai asetuksella säädettyjä viranomaisen toimintaa koskevia tietoturvallisuusvaatimuksia ja valtiovarainministeriön tietoturvallisuutta koskevia ohjeita;
- 2) kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitetun kansallisen turvallisuusviranomaisen antamia kansainvälisten tietoturvallisuusvelvoitteiden toteuttamista koskevia ohjeita;
- 3) Euroopan unionin tai muun kansainvälisen toimielimen antamia tietoturvallisuutta koskevia säännöksiä tai ohjeita;
- 4) julkaistuja ja yleisesti tai alueellisesti sovellettuja tietoturvallisuutta koskevia säännöksiä, määräyksiä tai ohjeita;
- 5) vahvistettuun standardiin sisältyviä tietoturvallisuutta koskevia vaatimuksia.

4 luku

Erinäiset säännökset

11 §

Maksut

Tietoturvallisuuden arviointilaitoksen hyväksymistä koskevan asian käsittelystä Viestintävirastossa perittävästä maksusta säädetään valtion maksuperustelaissa (150/1992) ja sen nojalla.

12 §

Muutoksenhaku

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

13 §

Hyvää hallintoa koskevien säännösten soveltaminen

Hyväksytyn tietoturvallisuuden arviointilaitoksen on tässä laissa tarkoitettuja tehtäviä hoi-

taessaan noudatettava hallintolakia (434/2003), viranomaisten toiminnan julkisuudesta annettua lakia (621/1999) sekä kielilakia (423/2003).

14 §

Voimaantulo

Tämä laki tulee voimaan päivänä kuuta 20 .

Ennen lain voimaantuloa voidaan ryhtyä lain täytäntöönpanon edellyttämiin toimenpiteisiin.

Laki

viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista

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).

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.

2 §

Määritelmät

Tässä laissa tarkoitetaan:

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

2) *tietoliikennejärjestelyllä* tiedonsiirtoverkosta, tiedonsiirtolaitteista, ohjelmistoista ja

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 hyväk-

synnän tietoturvallisuuden arviointilaitoksista annetun lain (/20) 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 vaatimuksenmukaisuutta;

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

3) tehdä valtiovarainministeriön pyynnöstä selvityksiä valtionhallinnon viranomaisen määräämisvallassa 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 tarkoitettuja tehtäviä käyttävissään 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 sel-

vityksen 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 arvioitavana tai selvityksen kohteena olevaa tietojärjestelmää tai tietoliikennejärjestelyä 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 viranomaisen 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 tietoturvaluutta koskevia säännöksiä ja ohjeita;

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

5) vahvistettuun standardiin sisältyviä tietoturvaluutta koskevia vaatimuksia.

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

8 §

Todistuksen antaminen

Viestintävirasto voi pyydettäessä antaa todistuksen tietoturvaluutta 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 §

Tietoturvaluuden tason ylläpito ja seuranta

Sen, joka haluaa 8 §:ssä tarkoitettun todistuksen, on annettava sitoumus tietoturvaluustason säilyttämisestä. Todistuksen saaneen on ilmoitettava Viestintävirastolle sellaisista muutoksista, joilla on vaikutusta tietoturvaluustason, 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 tarkoitettun ratkaisun tekemistä kuultava todistuksen saanutta sekä varattava tälle tilaisuus korjata puute.

Viestintävirasto voi 1 momentissa tarkoitettussa päätöksessään määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta, 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 maksuperustelaissa (150/1992) ja sen nojalla.

13 §

Voimaantulo

Tämä laki tulee voimaan päivänä kuuta 20 .

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

Ennen lain voimaantuloa voidaan ryhtyä lain täytäntöönpanon edellyttämiin toimenpiteisiin.

Laki

viestintähallinnosta annetun lain 2 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan viestintähallinnosta annetun lain (625/2001) 2 §:n 1 kohta, sellaisena kuin se on laissa 886/2010, seuraavasti:

2 §

Viestintäviraston tehtävät

Viestintäviraston tehtävänä on:

1) huolehtia viestintämarkkina-laissa (393/2003), radiotaajuuksista ja telelaitteista annetussa laissa (1015/2001), postilaissa (415/2011), televisio- ja radiotoiminnasta annetussa laissa (744/1998), valtion televisio- ja radorahastosta annetussa laissa (745/1998), sähköisen viestinnän tietosuojalaissa (516/2004), eräiden suojauksen purkujärjestelmien kieltämisestä annetussa laissa (1117/2001), vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetus-

sa laissa (617/2009), kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004), tietoturvallisuuden arviointilaitoksista annetussa laissa (/20) viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetussa laissa (/20) sekä verkkotunnuslaissa (228/2003) sille säädetyistä tehtävistä;

— — — — —
Tämä laki tulee voimaan päivänä kuuta 20 .

Ennen lain voimaantuloa voidaan ryhtyä lain täytäntöönpanon edellyttämiin toimenpiteisiin.

Helsingissä 29 päivänä marraskuuta 2011