SUOMEN SÄÄDÖSKOKOELMA

Julkaistu Helsingissä 28 päivänä joulukuuta 2011

1405/2011

Laki

tietoturvallisuuden arviointilaitoksista

Annettu Helsingissä 22 päivänä joulukuuta 2011

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 tietoturvallisuustason (*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 arviointilai-

HE 45/2011
LiVM 9/2011
EV 59/2011

toksen vastuuhenkilöiden luotettavuudesta ja sen toimitilojen turvallisuudesta. Suojelupoliisi noudattaa lausuntoaan laatiessaan, mitä kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004) säädetään.

Viestintävirasto voi hakemusta käsiteltäessä 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 seurantaa 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 kehotettava 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 viranomaisten 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 tietototurvallisuutta 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 hoitaessaan noudatettava hallintolakia (434/2003), viranomaisten toiminnan julkisuudesta annettua lakia (621/1999) sekä kielilakia (423/2003).

14 §

Voimaantulo

Tämä laki tulee voimaan 1 päivänä kesäkuuta 2012.

Ennen lain voimaantuloa voidaan ryhtyä lain täytäntöönpanon edellyttämiin toimenpiteisiin.

Helsingissä 22 päivänä joulukuuta 2011

Tasavallan Presidentti

TARJA HALONEN

Oikeusministeri *Anna-Maja Henriksson*

JULKAISIJA: OIKEUSMINISTERIÖ EDITA PRIMA OY / EDITA PUBLISHING OY ISSN 1455-8904 / 1237-3419 (painettu)