OIKEUSMINISTERIÖ
Lainsäädäntöneuvos
Anna-Riitta Wallin

MUISTIO
23.6.2010

Liite 1

ASETUS TIETOTURVALLISUUDESTA VALTIONHALLINNOSSA

1. Uudistuksen tausta ja tavoitteet ja pääasiallinen sisältö

Tietoturvallisuuden tarkoituksena valtionhallinnossa on varmistaa viranomaisen toiminnan jatkuvuus ja laatu sekä oikeusturvan toteutuminen. Voimassa oleva asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999) annettiin joulukuussa 1999 voimaan tulleen viranomaisten toiminnan julkisuudesta annetun lain (621/1999), jäljempänä julkisuuslaki, nojalla. Nykyinen sääntely ei vastaa tietoturvallisuuden kehittämistarpeita, jotka on määritelty valtioneuvoston vuonna 2009 antamassa periaatepäätöksessä valtionhallinnon tietoturvallisuuden kehittämisestä.

Hallituksen esitys eduskunnalle laiksi viranomaisten toiminnan julkisuudesta annetun lain sekä kuntalain 50 §:n muuttamisesta (HE 20/2005 vp) annettiin eduskunnalle kevätkaudella 2005. Lait (495–496/2005) tulivat voimaan 1 päivänä lokakuuta 2005. Uudistuksen avulla oli tarkoitus muun ohella määritellä aikaisempaa täsmällisimmistä asetuksenantovaltuuksista sekä antaa siten mahdollisuudet tietoturvallisuuden tehostamiseksi valtionhallinnossa.

Annettavaksi ehdotetun asetuksen tavoitteena on luoda edellytykset valtionhallinnon tietoturvallisuustyön kehittämiseksi sekä yhtenäisten menettelyjen luomiseksi salassa pidettäviä ja käytöltään rajoitettuja tietoaineistoja käsiteltäessä. Asetusta laadittaessa on otettu huomioon valtiovarainministeriössä laadittu suunnitelma erilaisten tietoturvallisuustasojen toteuttamisesta valtionhallinnossa. Sen avulla vahvistetaan valtiovarainministeriön kehittämisosaston informaatio-ohjaukseen jo perustuvaa kehittämistyötä ja tämän ohjauksen merkitystä.

Uudistus muun ohella vahvistaa hallinnon asiakkaiden ja sidosryhmien luottamusta hallintoon ja sen tietojenkäsittelyyn sekä luo asianmukaiset puitteet sähköisen asianhallinnan ja sähköisten palvelujen kehittämiselle. Yhtenäisten menettelytapojen syntyminen antaa mahdollisuuden saavuttaa tehokkuushyötyjä erilaisten luokituskäytäntöjen poistuessa sekä tehostaa valtiovarainministeriön tietoturvallisuutta koskevan ohjeiston merkitystä ja vaikuttavuutta.

Uudistuksen tarkoituksena on myös yhdenmukaistaa Suomea sitoviin kansainvälisiin sopimuksiin perustuvia ja kansallisia tietoturvallisuusvelvoitteita, erityisesti tietoaineistojen turvallisuusluokitusta. Euroopan unionin edustajien Suomeen tekemän turvallisuustarkastuksen johdosta vuonna 29.1.2008 annetussa tarkastuskertomuksessa kiirehdittiin nyt annettavaksi ehdotetun asetuksen antamista.

Uudistus toteutettaisiin antamalla kokonaan uusi asetus tietoturvallisuudesta valtionhallinnossa. Ehdotettu asetus sisältäisi viisi lukua (yleiset säännökset, yleiset tietoturvalli-

suusvaatimukset, asiakirjojen luokittelu, luokitellun asiakirjan käsittelyä koskevat vaatimukset sekä voimaantulo- ja siirtymäsäännökset).

2. Asetuksenantovaltuudet

Valtioneuvoston asetuksella voidaan 5 luvussa säädettyjen velvoitteiden toteuttamiseksi valtionhallinnossa säätää:

1) tietoaineistojen luokittelusta asianmukaisten tietoturvallisuustoimenpiteiden toteuttamiseksi (1 mom. 3 k),

2) velvollisuudesta tehdä turvallisuusluokkaa koskeva merkintä asiakirjoihin, joiden oikeudeton paljastuminen voi aiheuttaa vahinkoa maanpuolustukselle, valtion turvallisuudelle, kansainvälisille suhteille tai muille yleisille eduille 24 §:n 1 momentin 2 ja 7–10 kohdassa tarkoitetulla tavalla (1 mom. 4 k.); ja

3) eri turvallisuusluokkia koskevista tietoturvallisuusvaatimuksista mukaan lukien toimitilojen turvallisuutta koskevat vaatimukset sekä tietoturvallisuutta koskevien vaatimusten soveltamisesta salassa pidettäviin asiakirjoihin ja niihin sisältyviin tietoihin samoin kuin sellaisiin asiakirjoihin ja niihin sisältyviin tietoihin, joiden luovuttamista on muutoin lailla rajoitettu taikka joihin sisältyviä tietoja saa lain mukaan käyttää vain määrättyyn tarkoitukseen (1 mom. 5 k.).

Asetus perustuu pääosin mainittuihin julkisuuslain 36 §:n 1 momentin säännöksiin. On huomattava, että edellä mainittu 36 §:n 1 momentin 3 kohta antaa valtuuden säätää tietoturvallisuutta koskevista vaatimuksesta silloinkin, kun kysymys ei ole turvallisuusluokitelluista asiakirjoista.

Ehdotetun 4 §:n säännökset tietoturvallisuuden suunnittelun perusteista perustuvat osaltaan julkisuuslain 36 §:n 1 momentin 1 kohtaan, jonka mukaan asetuksella voidaan säätää viranomaisen velvollisuudesta selvittää ja arvioida hallussaan olevat tietoaineistot sekä niiden käsittelyprosessit hyvän tiedonhallintatavan toteuttamiseksi. Tietoturvallisuus on osa hyvää tiedonhallintatapaa ja suunnittelu on erottamaton elementti tietoturvallisuusvaatimuksia, joita koskevien säännösten antamisesta asetuksella säädetään julkisuuslain 36 §:n 1 mom. 5 kohdassa.

Asetus ei vaikuttaisi hallinnon ulkopuolisten asemaan, esim. oikeuteen saada tieto viranomaisen asiakirjasta.

Perustuslain 80 §:ssä tarkoitettuina oikeussääntöinä ei pidetä aineelliselta sisällöltään toimeenpanovallan alaan kuuluvia hallinnon sisäisiä ja lähtökohtaisesti vain viranomaista velvoittavia määräyksiä. Valtioneuvostolla on perustuslain 3 §:n 2 momenttiin ja 65 §:ään perustuva yleistoimivalta ohjata alaistaan hallintokoneistoa ja antaa tässä tarkoituksessa hallinnon sisäisiä määräyksiä, vaikka määräystenantovallasta ei olisikaan lailla erikseen säädetty. Myös valtioneuvoston asetukseen voidaan ottaa aineelliselta sisällöltään hallinnollisiksi luonnehdittavia määräyksiä, kunhan itse asetuksen antaminen perustuu laissa säädettyyn valtuutukseen (ks. Lainlaatijan perustuslakiopas, Oikeusministeriön julkaisu 2006:11, s. 43 - 45).

Ehdotetun asetuksen 5 §:ään ehdotetaan otettaviksi säännökset tietoturvallisuuden perustason toteuttamisesta. Ne vastaavat asiasisällöltään julkisuuslaissa tai henkilötietolaissa (532/1999) säädettyjä velvoitteita. Pykälään sisältyvissä säännöksissä ei ole kysymys oikeussäännöistä perustuslain 80 §:n tarkoittamassa mielessä. Ne on kuitenkin katsottu tarpeelliseksi sisällyttää asetusehdotukseen mahdollisimman tehokkaan täytäntöönpanon varmistamiseksi ja ottamalla huomioon, että täytäntöönpanoon osallistuu todennäköisesti laajasti muita kuin oikeudellisen koulutuksen saaneita.

3. Valmistelu

Asetus on valmisteltu samanaikaisesti ja samassa työryhmässä kuin ohjeet asetuksen täytäntöönpanosta, jotka valtiovarainministeriö antaa asetuksen tultua säädetyksi. Asetusluonnos ja luonnos annettaviksi ohjeiksi olivat vuonna 2007 ja vuonna 2008 laajoilla lausuntokierroksilla. Tämän lisäksi asetusluonnosta on käsitelty lukuisissa Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) järjestämissä koulutus- ja keskustelutilaisuuksissa ja johtoryhmän kokouksissa. Annettu palaute on otettu huomioon asetuksen valmistelussa.

Uudistusta käsiteltiin kansliapäällikkökokouksessa 2.6.2008.

Valtiovarainministeriön hallinnon kehittämisosasto toteutti keväällä 2010 kyselyn, jossa valtionhallinnon yksiköiltä tiedusteltiin arvioita annettaviksi suunniteltujen valtionhallinnon tietoturvallisuutta koskevan asetuksen ja sen täytäntöönpanoa koskevan ohjeen vaikutuksista toimintaansa. Vastaukset saatiin 10 ministeriöltä ja 10 keskeiseltä virastolta. Useissa vastauksissa toivotaan asetuksen saattamista nopeasti voimaan.

4. Yksityiskohtaiset perustelut

4.1. Asetuksen soveltamisala ja suhde muuhun lainsäädäntöön

Asetuksessa säädettäisiin valtionhallinnon viranomaisia koskevista yleisistä tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista käsittelyssä noudatettavista tietoturvallisuusvaatimuksista (1 §).

Valtionhallinnon viranomaisilla tarkoitettaisiin valtion hallintoviranomaisia ja muita valtion virastoja ja laitoksia sekä tuomioistuimia ja muita lainkäyttöviranomaisia (3 § 1 k). Asetusta sovellettaessa tietoturvallisuudella tarkoitetaan tietojen suojaamiseksi ja niiden eheyden ja käytettävyyden varmistamiseksi toteutettavia hallinnollisia, teknisiä ja muita toimenpiteitä ja järjestelyjä (3 § 2 k).

Asetus on kirjoitettu käyttämällä käsitettä asiakirja. Käsite vastaa julkisuuslain 5 §:n 1 momentin määrittelyä (3 § 3 k) ja on siten välineneutraali eli riippumaton siitä, minkälaiselle alustalle tai minkälaisin keinoin tieto on talletettu. Siten asiakirjoilla tarkoitetaan paitsi perinteisiä paperimuotoisia asiakirjoja, myös sähköisesti talletettuja tietoaineistoja riippumatta niiden formaatista.

Asiakirjojen luokittelua koskevat säännökset koskisivat ensisijaisesti vain salassa pidettäviä tietoaineistoja. Tietyissä tilanteissa säännöksiä voitaisiin soveltaa myös sellaisiin asiakirjoihin, joissa olevien tietojen käyttöön liittyy lailla säädettyjä rajoituksia (9 § 2 mom.).

Annettava asetus ei aiheuta muutosta viranomaisten asiakirjojen julkisuuteen ja salassapitoon, vaan nämä määräytyisivät julkisuuslain ja erityissäännösten perusteella (2 § 1 mom.). Asetuksen mukaan tehty luokittelumerkintä ei siten ratkaise asiakirjan salassapitoa eikä oikeuta viranomaista poikkeamaan julkisuuslain mukaisesta velvollisuudesta tapaus- ja asiakirjakohtaisesti arvioida asiakirjan julkisuus siitä tietoja pyydettäessä.

Kansainvälisiin tietoturvallisuusvelvoitteisiin sovellettaisiin edelleenkin kansainvälistä tietoturvallisuusvelvoitteista annettua lakia (588/2004) sekä Suomea sitovia sopimuksia ja muita säädöksiä (2 § 2 mom.).

4. 2. Yleiset tietoturvallisuusvaatimukset

Ehdotetussa 2 luvussa olisivat säännökset yleisistä tietoturvallisuusvaatimuksista. Luvun säännökset koskevat valtionhallinnon viranomaisia siinäkin tapauksessa, että ne eivät luokittele tietoaineistojaan.

Lukuun on sisällytetty säännökset tietoturvallisuuden suunnittelun perusteista (4 §) ja tietoturvallisuuden perustason toteuttamisesta (5 §) sekä tietoaineistojen elinkaaren, ts. eri käsittelyvaiheiden huomioon ottamisesta (6 §). Luvun lopussa olisi säännökset luokitteluperusteiden ja niitä vastaavien tietoturvallisuusvaatimusten noudattamisesta (6 §).

Tietoturvallisuuden suunnittelun tulisi perustua hyvän tiedonhallintatavan mukaisiin selvityksiin ja arvioihin sekä tietoaineistoihin kohdistuvien riskien ja tietoturvallisuustoimenpiteiden kustannusten arviointiin. Nämä tulisi ottaa suunnittelussa huomioon (4 §).

Tietoturvallisuuden perustason toteuttaminen valtionhallinnon viranomaisissa koostuu erilaisista toimenpiteistä ja järjestelyistä, joista säädettäisiin asetuksen 5 §:n 1 momentissa. Niistä konkreettisista toimenpiteistä, joita tietoturvallisuuden perustason toteuttaminen edellyttää, annetaan tarkempia määrittelyjä valtiovarainministeriön ohjeistuksessa. Yksityiskohtaisista ja kovin teknisluonteisista seikoista ei muutoinkaan olisi tarkoituksenmukaista säätää asetuksessa etenkin kun vaatimustaso todennäköisesti muuttuu ajan kuluessa.

Tietoturvallisuuden toteuttaminen perustuu toimintaan liittyvien tietoturvallisuusriskien kartoittamiseen (1 k). Viranomaisen käytössä tuli olla riittävä asiantuntemus tietoturvallisuuden varmistamiseksi. Tietoturvallisuuden hoitamista koskevat tehtävät ja vastuu sekä asiakirjojen käsittelyä koskevat tehtävät ja vastuut on määriteltävä (2 ja 3 k).

Yleisiin velvoitteisiin kuuluisi tietojen saannin ja käytettävyys turvaaminen eri tilanteissa ja menettelytapojen luomista poikkeuksellisten tilanteiden selvittämiseksi (4 k). Viranomaisen olisi varmistettava, että salassa pidettäviin tietoihin ja henkilörekisterien tietoihin pääsevät vain ne, jotka tarvitsevat tällaisia tietoja työtehtäviensä hoitamiseksi (ns. "need-to-know"-periaate; 5 k).

Tietojen laadun turvaaminen sekä muu luvaton tai asiaton käsittely tulisi estää käyttöoikeushallinnan, käytön valvonnan sekä tietoverkkojen, tietojärjestelmien ja tietopal-

velujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä ja muilla toimenpiteillä (6 k).

Asiakirjojen suojaaminen edellyttää huolehtimista toimitilaturvallisuudesta: asiakirjojen tietojenkäsittely- ja säilytystilojen tulisi olla riittävästi valvottuja ja suojattuja (7 k).

Henkilöstöturvallisuudesta voidaan huolehtia luotettavuudesta turvallisuusselvitysmenettelyn ja muiden lain perusteella käytettävissä olevien keinojen avulla (8 k). Henkilöstölle ja muille käsittelytehtäviä hoitaville tulee antaa ohjeet ja koulutusta (9 k) ja annettujen ohjeiden noudattamista tulee valvoa ja niiden muutostarpeita arvioida säännöllisesti (10 k).

Valtionhallinnon viranomaisen velvollisuudesta huolehtia tietojen suojaamisesta annettaessa salassa pidettäviä tietoja toimeksiantotehtävän suorittamista varten on voimassa, mitä viranomaisten toiminnan julkisuudesta annetun lain 26 §:n 2 momentissa säädetään (5 § 2 mom.). Henkilörekisteritietojen antamisesta toimeksiantotehtäviä varten säädetään puolestaan henkilötietolain 32 §:n 2 momentissa.

Tietoturvallisuustoimenpiteiden suunnittelussa ja toteutuksessa tulee ottaa huomioon käsittelyn eri vaiheet koko tiedon elinkaaren ajalta (6 §). Tietoturvallisuuden kannalta on tärkeää, että asiakirjojen käsittelyvaiheet eritellään ja arvioidaan niihin liittyvät uhkatekijät sekä toimenpiteiden tarve.

Kuten edellä on todettu, asetuksessa ei säädettäisi ehdotonta velvollisuutta luokitella asiakirjat. Jos asiakirjat tai osa niistä päätetään luokitella, asetuksen 7 §:n 1 momenttiin otettaviksi ehdotettujen säännösten mukaan valtionhallinnon viranomaisen on luokittelussa noudatettava asetuksen 3 luvussa säädettyjä perusteita. Tämä ilmentää asetuksen tavoitetta yhtenäisten luokitteluperusteiden luomisesta sekä sitä kautta viranomaisten välisen tietojenvaihdon yksinkertaistamisesta ja helpottamisesta sekä kustannustehokkuutta.

Valtionhallinnon viranomaisen olisi 7 §:n 2 momentin mukaan pidettävä huolta siitä, että sen laatimien tai saamien luokiteltujen asiakirjojen käsittelyssä noudatetaan 4 luvussa säädettyjä vaatimuksia. Näiltä osin asetus kuitenkin osoittaisi tietoturvallisuuden minimitason, sillä asetus ei estäisi sitä, että viranomainen soveltaa omassa toiminnassaan 4 luvussa säädettyä korkeampia tietoturvallisuusvaatimuksia. Asetuksessa edellytettyjä toimia tehokkaimpia tietoturvallisuusvaatimuksia ei kuitenkaan voitaisi vaatia tietoja muille viranomaisille luovutettaessa.

4.3. Asiakirjojen luokittelu

Asiakirjojen luokittelua koskevassa 3 luvussa määriteltäisiin luokituksen perusteet ja käsittelyvaatimuksia osoittavat suojaustasot sekä säädettäisiin luokitusmerkinnöistä ja niiden vastaavuudesta suhteessa kansainvälisiin tietoturvallisuusvelvoitteisiin.

Luokittelun perusteita koskevilla säännöksillä pyritään luomaan kullekin viranomaiselle parhaiten sopivat luokittelutavat: luokittelu voidaan kohdistaa myös rajoitettuna tiettyihin tietoaineistoihin tai tiettyihin tietoaineistojen käsittelyvaiheisiin sen mukaan, minkälainen tarve suojattavan edun kannalta kulloinkin on. Ehdotetuissa säännöksissä kiellettäisiin luokituksen ulottaminen sellaiseen asiakirjaan tai asiakirjan osiin, joissa käsit-

telyvaatimusten noudattaminen ei suojattavan edun vuoksi ole tarpeen (8 §). Ehdotetut säännökset olisivat omiaan lisäämään valtionhallinnon viranomaisten omaa päätäntävaltaa sopeuttaa siirtymisensä asteittain ehdotetun asetuksen mukaisiin luokiteltuja tietoaineistoja koskeviin tietoturvallisuusvaatimuksiin käytettävissä olevien resurssien puitteissa ja ne huomioon otettuina.

Asetuksen 9 §:ssä olisi säännökset salassa pidettävän asiakirjan käsittelyvaatimuksia osoittavista suojaustasoista. Nykyisen asetuksen mukaan tasoluokkia on pääsäännön mukaan kolme. Ehdotuksen mukaan suojaustasoluokkia olisi neljä. Näin luokitus vastaisi kansainvälistä käytäntöä. Mitä vahingollisempia seurauksia tietoaineiston luvattomasta paljastamisesta aiheutuisi, sitä tarkempia käsittelyvaatimuksia olisi noudatettava ja sitä korkeampaan suojaustasoluokkaan aineisto sijoitetaan.

Ehdotuksen mukaan korkein suojaustasoluokka olisi suojaustasoluokka I, johon kuuluvia asiakirjoja käsiteltäessä tulisi noudattaa kaikista tehokkaimpia tietoturvallisuustoimia. Tähän luokkaan voidaan luokitella kuuluvaksi asiakirjan, jos siihen sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetuille yleisille eduille. Kysymys olisi siten sellaisten yleisten etujen suojaamisesta, joita koskevat tiedot on säädetty salassa pidettäviksi. Myös suojaustasolle II luokiteltavissa olevassa asiakirjassa on tietoja, jotka on säädetty salassa pidettäviksi yleisen edun suojaamistarkoituksessa. Suojaustasoluokkaan III ja IV voi kuulua myös sellaisia asiakirjoja, jotka sisältävät yksityisten etujen suojaamiseksi salassa pidettäviksi säädettyjä tietoja.

Suojaustasojen määrittely tapahtuisi arvioimalla niitä vahinkoja, joita salassa pidettävän tiedon ilmaisemisesta voisi konkreettisesti seurata. Tämä varsin yleispiirteinen arviointi sisältää riskin sille, että luokittelu on joko yli- tai alimitoitettua tai että luokittelu poikkeaa eri viranomaisissa toisistaan. Määrittelyn yhtenäisyyteen onkin tarkoitus kiinnittää erityistä huomiota mm. uudistuksen täytäntöönpanokoulutuksesta.

Se, että asiakirja on säädetty salassa pidettäväksi, ei vielä yksistään määritä sitä, mihin suojausluokkaan asiakirja tulisi osoittaa kuuluvaksi. Kukin tietoaineisto ja sen paljastumisesta aiheutuvat seuraukset on arvioitava konkreettisesti ja ottaen huomioon suojattava etu kokonaisuutena. Vaikka esim. yksityisyyden suojan vuoksi tiettyjä asiakirjoja koskisikin ehdoton salassapitovelvoite, tästä ei seuraa, että kaikki salassa pidettävät henkilöä koskevat asiakirjat tai niiden tiedot kuuluisivat suojausluokkaan III. Salassapidon perusteena yksityisyyden suojaa koskevia salassapitosäännöksiä säädettäessä on ollut yleisellä tasolla tehty arvio tietojen julkisuudesta johtuvasta yksityisyyden suojan vaarantumisen riskistä (HE 30/1998 vp., s. 88). Suojaustasoluokittelussa sen sijaan on kysymys sen arvioimisesta, mitkä salassapitovelvollisuuden piiriin kuuluvista tiedoista ovat sellaisia, että ne konkreettisesti voivat vahingoittaa yksityisyyden suojaa oikeusjärjestyksen suojaamana oikeushyvänä.

Luokittelu voisi pääsäännön mukaan kohdistua vain salassa pidettäviksi säädettyihin asiakirjoihin (9 § 1 mom.). Muu kuin salassa pidettävä asiakirja voidaan luokitella ehdotetun 9 §:n 2 momentin mukaan ensinnäkin, jos asiakirjan luovuttaminen on lain mukaan viranomaisen harkinnassa. Tämä viittaa tilanteisiin, joissa asiakirja ei ole vielä tullut julkiseksi julkisuuslain 6 ja 7 §:n mukaisesti. Toiseksi luokittelu olisi mahdollista, jos asiakirjaan sisältyviä tietoja saa lain mukaan käyttää tai luovuttaa vain määrättyyn tarkoitukseen. Säännös olisi sovellettavissa esimerkiksi viranomaisten henkilörekiste-

reihin, joista tiedon luovuttaminen on yleensä mahdollista vain tiettyjä käyttötarkoituksia varten. Kummassakin edellä kuvatussa tilanteessa lisäedellytyksenä olisi, että tiedon oikeudeton paljastuminen voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä.

Luokitusmerkintöjen tekemisestä säädettäisiin asetuksen 10 ja 11 §:ssä. Suojaustasoa osoittavan merkinnän yhteyteen voitaisiin merkitä tieto asiakirjan salassapidosta ottaen huomioon, mitä viranomaisen toiminnan julkisuudesta annetun lain 25 §:ssä säädetään (10 § 1 mom.). Luokitusmerkintä voitaisiin tehdä asiakirjaan tai asiakirjaan liitettävään erilliseen asiakirjaan (10 § 3 mom.). Myös luokituksen muuttamisesta tai poistamisesta olisi tehtävä asianmukaiset merkinnät. Jos valtiohallinnon viranomainen on saanut toiselta valtionhallinnon viranomaiselta asiakirjan, johon on tehty suojaustasoa I, II tai III osoittava merkintä, luokitusmerkinnän muuttamisesta olisi ilmoitettava asiakirjan antaneelle viranomaiselle (10 § 4 mom.).

Luokittelumerkinnän yhteyteen tai sen sijasta asiakirjaan voitaisiin tehdä merkintä turvallisuusluokituksesta silloin, kun kysymys on keskeisten yleisten etujen suojaamisesta tai jos asiakirja liittyy kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseen (11 §). Turvallisuusluokituksen merkitsemistä koskevilla säännösehdotuksilla on pyritty toteuttamaan kansainvälisiä tietoturvallisuusvelvoitteita vastaava luokitustapa. Turvallisuusluokitus on tarkoitettu osoittamaan sitä, että kysymys on keskeisten yleisten etujen (maanpuolustus, kansainväliset suhteet, tietoturvallisuus) suojan kannalta erityisen merkityksellisistä tietoaineistoista. Kansainvälistä käytäntöä vastaavalla tavalla turvallisuusluokitus rajattaisiin vain näihin tietoaineistoihin. Merkinnän tekemisestä ruotsinkielisenä säädettäisiin 11 §:n 4 momentissa.

Asetuksen 12 §:ssä olisi säännökset turvallisuusluokituksen vastaavuudesta kansainvälisiä velvoitteita toteutettaessa. Säännösehdotukset vastaavat käytäntöä, joka on syntynyt Suomen tekemissä kahdenkeskisissä tietoturvallisuussopimuksissa.

4.4. Luokitellun asiakirjan käsittelyvaatimukset

Käsittelyvaatimusten laajuus olisi pääsäännön mukaan riippuvainen siitä, mihin suojaustasoluokkaan tietoaineisto kuuluu. Käsittelyvaatimuksia koskevien säännösten perustana on käytetty nykyisin valtiovarainministeriön ohjeisiin sisältyviä käsittelyvaatimuksia sekä kansainvälisiä määräyksiä ja käytäntöjä. Ehdotetut käsittelyvaatimukset ovat tarkoituksenmukaisuus- ja kustannussyistä jossain määrin lievemmät kuin EU:n neuvoston turvallisuussäännöissä.

Luokiteltujen tietoaineistojen käyttöoikeuden antamisessa tulisi noudattaa periaatetta, jonka mukaan salassa pidettäviä tietoja saa antaa vain niille, joilla työtehtäviensä vuoksi on tarve tiedonsaantiin (13 § 1 mom.).

Toimitilojen turvallisuudesta tulisi huolehtia ulkoisen suojauksen avulla sekä edellyttämällä, että tiloissa, joissa käsitellään kahteen korkeimpaan suojaustasoon kuuluvia aineistoja, voidaan tunnistaa siellä liikkuvat henkilöt (14 §). Säännöksissä velvoitetaan viranomaiset huolehtimaan vastaavasta suojasta silloinkin kun tietojenkäsittely tapahtuu viranomaisten toimitilojen ulkopuolella, esim. atk-alan palveluyrityksessä.

Luokiteltuja asiakirjoja saisi pääsäännön mukaan käsitellä vain viranomaisen toimitiloissa. Käsittely toimitilojen ulkopuolella edellyttäisi aina viranomaisen lupaa, toimeksiantoa tai ohjeita, joissa asetetaan edellytykset aineistojen käsittelylle (15 §). Jos esim. käsittelytehtävät on annettu palveluyritykselle, asia kirjataan toimeksiantoon tai sen liiteasiakirjoihin.

Sähköisen asiakirjan laatimista, tallettamista ja muokkaamista koskevilla säännöksillä (16 §) pyritään takaamaan se, että luokiteltuja tietoja käsitellään sähköisesti vain sellaisissa tietojärjestelmissä, joissa voidaan taata tarvittava suoja. Ehdotetuissa säännöksissä edellytetään, että viranomainen osoittaa, minkälaisiin tietojärjestelmiin eri suojausluokkiin kuuluvia tietoja saa tallettaa. Virkamies ei voisi siten itse ratkaista, miten ja mihin tällainen asiakirja talletetaan.

Tallettamisen edellytyksissä on viitattu tavanomaisesti sovellettavan korkean tai korotetun tietoturvallisuustason vaatimuksiin. Vaatimustason kiinnittämisellä tavanomaisesti sovellettavaan korkean tai korotetun tietoturvallisuuden tasoon on haluttu lisätä sääntelyn joustavuutta ja suhteellisuusperiaatteen huomioon ottamista. Säännöksissä ei siten edellytettäisi kaikkia niitä toimia, joita esim. teknisesti olisi mahdollista suorittaa, vaan sitä, että tietojenkäsittely kokonaisuudessaan on riittävällä tasolla suhteessa suojattaviin intresseihin. Valtionhallinnon viranomaiset voisivat saada malleja ehdotetun sääntelyn mukaisista konkreettisista toimista valtiovarainministeriön ohjeista ja malleista.

Viranomainen voi varmistaa järjestelmänsä tietoturvallisuustason myös käyttämällä hyväksi yksityisiä arviointilaitoksia sekä alan standardeja ja esim. kansainvälisten järjestöjen käyttämiä vaatimuksia. Suomessa ei tällä hetkellä ole viranomaista, joka arvioisi ja varmistaisi tietojärjestelmien tai tietoverkkojen tietoturvallisuutta. Tarkoituksena on, että tehtävä annetaan Viestintävirastolle, joka ensi vaiheessa hoitaisi mainittuja tehtäviä kansainvälisiä tietoturvallisuusvelvoitteita toteutettaessa (HE 53/2010 vp).

Suojaustasoon I – II kuuluvan asiakirjan saisi ehdotetun 1 momentin 1 kohdan mukaan tallettaa sähköisesti tietovälineelle tai muulle laitteelle, joka ei ole liitetty tietoverkkoon, jos asiakirja talletetaan vahvasti salattuna tai jos se on muutoin vahvasti suojattu. Tallettaminen olisi sallittua myös sellaiselle tietovälineelle, joka on liitetty sellaiseen viranomaisen tietoverkkoon, joka yhdistää asiakirjan tallettamiseen ja säilyttämiseen käytetyn laitteen samassa viranomaisen hallinnassa olevassa erityisvalvotussa tilassa oleviin muihin laitteisiin, jos laitteet yhdistävään tietoverkkoon ei ole luotu yhteyttä muista tietoverkoista ja asiakirjan käsittely on muutoin vahvasti suojattua.

Ehdotuksen mukaan suojaustasoon II kuuluva asiakirja voitaisiin tallettaa sähköisesti viranomaisen sellaiseen tietoverkkoon liitetylle tietovälineelle tai muulle laitteelle, jonka käyttö on rajoitettu. Lisäksi edellytettäisiin, että asiakirja talletetaan vahvasti salattuna tai se on muutoin vahvasti suojattu ja että viranomainen on muutoinkin varmistanut, että tietoverkko ja tietojenkäsittely kokonaisuudessaan täyttävät tavanomaisesti sovellettavan korkean tietoturvallisuustason vaatimukset (2 mom.) Suojaustasoon III kuuluva asiakirja voitaisiin tallettaa vastaavasti, jos tietoverkko ja tietojenkäsittely kokonaisuudessaan täyttävät tavanomaisesti sovellettavan korotetun tietoturvallisuustason vaatimukset (3 mom.). Sama koskee suojaustasoon IV kuuluvaa arkaluonteisia henkilötietoja tai biometrisiä tunnistetietoja sisältävää henkilörekisteriin talletettua asiakirjaa.

Korkeimpiin suojausluokkiin kuuluvat asiakirjat talletettaisiin yleensä vahvasti salattuina tai muutoin vahvasti suojattuina. Tällaisia asiakirjoja laadittaessa ja muokattaessa asiakirjan tekstit ovat kuitenkin selväkielisessä muodossa, mistä aiheutuu riski tietojen paljastumiselle. Laadittaessa suojaustasoon I – III kuuluvaa asiakirjaa sähköisessä muodossa ja sitä muokattaessa olisi pidettävä huolta, että hajasäteilystä aiheutuvia haittoja voidaan riittävästi vähentää (16 § 4 mom.). Jos laite on liitetty tietoverkkoon, tietoverkon on lisäksi täytettävä 1 momentin 2 kohdassa taikka 2 tai 3 momentissa säädetyt edellytykset sen mukaan, mihin suojaustasoluokkaan käsiteltävä aineisto kuuluu.

Ehdotettujen säännösten mukaan suojaustasoon I kuuluvaa asiakirjaa ei saisi kopioida ilman sen laatineen viranomaisen antamaa lupaa (17 §). Suojaustasoon I tai II kuuluvan asiakirjan kopiot on luetteloitava. Asiakirjan sähköisessä kopioinnissa tietovälineelle olisi ottava huomioon, mitä 16 §:ssä säädetään sähköisen asiakirjan tallettamisen edellytyksistä. Luokitellun asiakirjan kopioon on tehtävä sama merkintä kuin mikä on tehty alkuperäiseen asiakirjaan, jollei luokitus muutoin jo ilmene asiakirjan kopiosta. Valtionhallinnon viranomainen voi päättää, että suojaustasoa III tai IV edellyttävään asiakirjaan ei ole tarpeen tehdä merkintää, jos asiakirjaa ei luovuteta ulkopuolisille ja asiakirjaa viranomaisessa käsittelevillä on tieto asiakirjan käsittelyssä noudatettavista vaatimuksista.

Suojaustasoon I tai II kuuluva asiakirja olisi asetuksen mukaan pakattava asianmukaisesti sekä toimitettava henkilökohtaisesti tai muulla viranomaisen hyväksymällä turvallisella tavalla vastaanottajalle (18 §). Säännösehdotukset merkitsevät, että kahteen alimpaan suojaustasoon kuuluvat asiakirjat sen sijaan voitaisiin välittää viranomaisen päättämällä tavalla.

Asiakirjan siirtämistä tietoverkossa säänneltäisiin asetuksen 19 §:ssä. Ehdotuksen mukaan pääsääntönä olisi, että suojaustasoon I tai II kuuluvaa asiakirjaa ei saa siirtää tietoverkossa. Tästä olisi kuitenkin poikkeuksia. Mainittuihin suojaustasoihin kuuluvia asiakirjoja olisi mahdollista siirtää sellaisessa tietoverkossa, joka yhdistää asiakirjan tallettamiseen ja säilyttämiseen käytetyn laitteen samassa viranomaisen hallinnassa olevassa erityisvalvotussa tilassa oleviin muihin laitteisiin, jos laitteet yhdistävään verkkoon ei ole luotu yhteyttä muista tietoverkoista ja tietojen käsittely on muutoinkin vahvasti suojattua (1 mom.). Suojaustasoon II kuuluvan asiakirjan sähköinen siirtäminen olisi sallittua myös sellaisessa viranomaisen tietoverkossa, jonka käyttö on rajoitettu, jos tiedot välitetään vahvasti salattuina tai ne on muutoin vahvasti suojattu ja valtionhallinnon viranomainen on muutoinkin varmistanut, että tietoverkko ja tietojenkäsittely kokonaisuudessaan täyttävät tavanomaisesti sovellettavan korkean tietoturvallisuustason vaatimukset (2 mom.).

Suojaustasoon III kuuluvan asiakirjan siirtäminen tietoverkossa voidaan sallia ehdotetun 19 §:n 3 momentissa säädettävin edellytyksin. Edellytyksenä on muun ohella, että tietoverkko ja tietojenkäsittely kokonaisuudessaan täyttävät tavanomaisesti sovellettavan korotetun tietoturvallisuuden tason vaatimukset. Sama koskee suojaustasoon IV kuuluvan valtakunnalliseen henkilörekisteriin talletettujen arkaluonteisten henkilötietojen tai biometristen tunnistetietojen siirtämistä. Suojaustasoon IV kuuluvia muita asiakirjoja saisi siirtää valtionhallinnon viranomaisen päättämällä tavalla.

Asetuksen 20 §:ssä olisi säännökset käsittelyn kirjaamisesta. Ehdotuksen mukaan suojaustasoon I–III kuuluvien asiakirjojen sekä suojaustasoon IV kuuluvien arkaluonteisia

henkilötietoja tai biometrisiä tietoja sisältävien henkilörekisteriin talletettujen asiakirjojen käsittely tulee kirjata sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, manuaaliseen diaariin tai asiakirjaan. Käsittelyn kirjaaminen on keskeinen keino valvoa luokiteltujen asiakirjojen asianmukaista käsittelyä. Säännös ei edellytä, että jokainen esim. yksittäisen hallintoasian käsittelyyn kuuluvan asiakirjan käsittelytapahtuma kirjataan, jos asiakirjaa käsittelevät vain ne virkamiehet, jotka asianhallintajärjestelmässä on merkitty asian käsittelijöiksi.

Salassa pidettävien tietojen suojaamiseksi olisi huolehdittava asianmukaisesta arkistoinnista tai hävittämisestä (21 §). Luokiteltujen asiakirjojen arkistoinnissa noudatetaan arkistolakia ja sen nojalla annettuja säännöksiä ja määräyksiä sekä viranomaisen arkistolain mukaisesti laatimaa arkistonmuodostussuunnitelmaa. Tarpeettomaksi käyneen suojaustasoon I tai II kuuluvan asiakirjan kopio tulisi hävittää, jollei sitä palauteta asiakirjan laatineelle viranomaiselle. Hävittämisen saa suorittaa vain henkilö, jonka viranomainen on tähän tehtävään määrännyt. Asiakirjan valmisteluvaiheen versiot voi kuitenkin hävittää ne laatinut henkilö. Paperimuotoinen asiakirja on tuhottava suojaustasoa vastaavalla tavalla. Sähköisesti talletettu asiakirja on vastaavasti tuhottava työasemalta, tietojärjestelmästä tai tietovälineeltä sekä pidettävä huolta, että tietojärjestelmien käytön yhteydessä syntyneet väliaikaistiedostot poistetaan riittävän usein.

5. Voimaantulo

Asetuksen on tarkoitus tulla voimaan 1.10.2010 (22 §). Voimaantulon ajankohtaa määriteltäessä on otettu huomioon, että ennen asetuksen voimaantuloa on tarpeen antaa asetusta täydentävät valtiovarainministeriön ohjeet sekä järjestää koulutusta.

Asetuksella kumottaisiin viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta annetun asetuksen 2 ja 3 §.

Asiakirjoja, jotka on luokiteltu ennen ehdotetun asetuksen voimaantuloa, käsiteltäisiin asetuksessa säädettävien vaatimusten mukaisesti, jollei ole ilmeistä, että luokitukselle ei annettavan asetuksen mukaan enää ole perusteita (23 § 1 mom.).

Siirtymäsäännöksissä on otettu huomioon tarve muuttaa tai korjata ennen asetuksen voimaantuloa koskeva luokitusmerkintä (23 § 2 mom.). Ehdotuksen mukaan merkintöjä ei olisi tarpeen välttämättä muuttaa annettavan asetuksen 11 §:n 3 momentissa edellytetyllä tavalla, vaan vasta silloin, kun luokiteltu asiakirja luovutetaan ulkopuoliselle.

Viranomaisen tietojenkäsittely olisi saatettava vastaamaan 5 §:ssä säädettyjä perustason tietoturvallisuusvaatimuksia kolmen vuoden kuluessa asetuksen voimaantulosta (23 § 3 mom.).

Asetusehdotukseen ei sisälly ehdotonta tietoaineistojen luokittelupakkoa. Asetusehdotuksen siirtymäsäännöksien mukaan viranomaisen tietojenkäsittely olisi kuitenkin saatettava vastaamaan asetuksen 4 luvussa säädettäviä vaatimuksia viiden vuoden kuluessa siitä, kun viranomainen on päättänyt luokitella asiakirjansa (22 § 4 mom.). Siirtymäaika laskettaisiin siten kunkin viranomaisen kohdalla erikseen, mikä mahdollistaa tietoturvallisuustoimien ajoittamisen viranomaisten voimavarojen mukaisesti.

Valtionhallinnon viranomaisen tämän asetuksen voimaan tullessa käytössä olevien toimitilojen olisi täytettävä asetuksessa säädettävät vaatimukset tilojen turvallisuudelle viiden vuoden kuluessa asetuksen voimaantulosta. Uusien tilojen suunnittelu ja hankinta on usein pitkäjännitteistä toimintaa eikä tiloja koskevia muutoksia ole helppo tehdä. Tämän vuoksi siirtymäaika koskisi myös sellaisia toimitiloja, jotka on otettu käyttöön ennen kuin on kulunut kaksi vuotta asetuksen voimaantulosta (23 § 5 mom.).

6. Täytäntöönpano, sen kustannukset ja seuranta

Kuten edellisestä ilmenee, siirtymäsäännöksillä on osaltaan pyritty siihen, että viranomaiset voisivat sopeuttaa tietoturvallisuuden kehittämisen osana toimintaansa ja sen kehittämistä, mikä vähentää uusista velvoitteista aiheutuvia erityiskustannuksia. Samaan tavoitteeseen tähtäävät myös asetuksen 8 §:ään otettaviksi ehdotetut säännökset, joiden mukaan viranomaisen tietoaineistojen luokittelu voidaan suorittaa myös siten, että tietoturvallisuutta koskevat vaatimukset kohdistetaan vain sellaisiin asiakirjoihin tai sellaisiin asiakirjan käsittelyvaiheisiin, joissa erityistoimenpiteet ovat suojattavan edun vuoksi tarpeen. Kuten edellä on todettu, ehdotettu sääntely olisit omiaan lisäämään valtionhallinnon viranomaisten omaa päätäntävaltaa sopeuttaa siirtymisensä asteittain ehdotetun asetuksen mukaisiin luokiteltavia tietoaineistoja koskeviin tietoturvallisuusvaatimuksiin käytettävissä olevien resurssien puitteissa ja ne huomioon otettuina.

Valtiovarainministeriön hallinnon kehittämisosaston keväällä 2010 toteuttamaan kyselyyn annetuissa vastauksissa asetukseen suunniteltua siirtymäaikaa pidettiin realistisena. Kaikki vastanneet toteavat tietoturvallisuuden perustason saavuttamisen viimeistään vuonna 2013 ja asetuksen mukaisten luokiteltujen aineistojen käsittelyvaatimusten täyttämisen viimeistään vuonna 2015 olevan realistisia tavoitteita. Useimmilla hallinnonaloilla on jo käynnissä asetuksen toimeenpanon mukaisia toimenpiteitä ja suurimmassa osassa viranomaisia useimmat perustietoturvallisuustason vaatimukset näytetään jo nykyisin täytettävän.

Asetuksen ja ohjeiden täytäntöönpanon edellyttämät toimet vaihtelevat eri virastoissa. Esimerkkejä toimista ovat henkilöstön koulutus, tietojärjestelmiin tehtävät muutokset sekä mm. käyttöoikeushallinnan kehittäminen.

Teknisen tietoturvallisuuden toteuttamisesta aiheutuviin resurssi- ja kustannusvaikutuksiin vaikuttaa se, että valtaosa hallinnon yksiköistä tulee siirtymään Valtion IT-palvelukeskuksen asiakkaiksi. Käytännössä tämä tarkoittaa sitä, että pääosassa organisaatioita ei ole tarvetta enää kehittää omaa toimintaansa esim. korotetun tietoturvallisuuden tasolle organisaatioiden siirtyessä palvelukeskuksen asiakkaiksi.

Kyselyyn antamassaan vastauksessa liikenne- ja viestintäministeriö toteaa tietohallintokustannusten mahdollisesti lisääntyvän uudistuksen seurauksena viidestä kymmeneen prosenttiin (2 – 4 henkilötyövuotta), mutta ei aiheuttavan henkilön lisätarvetta. Vastaajista valtioneuvoston kanslia, ulkoasiainministeriö, puolustusministeriö, opetusministeriö, maa- ja metsätalousministeriö, ympäristöministeriö ja työ- ja elinkeinoministeriö eivät esitä kokonaiskustannuslaskelmia. Työ- ja elinkeinoministeriön vastauksessa suoria kustannusvaikutuksia perustason aikaansaamiseksi ei pidetä merkittävinä ja ministeriö esittää hallinnonalan varsin hyvän tilanteen tietoturvallisuustasojen toimeenpanos-

sa. Sosiaali- ja terveysministeriö esittää, että valtiovarainministeriö osoittaisi organisaatioille erilliset tietoturvallisuusmäärärahat tietoturvallisuustasojen saavuttamiseksi. Sisäasiainministeriö katsoo asetuksen toimeenpanon edellyttävän kohdennettua lisärahoitusta sitä erittelemättä.

Tiivistelmänä voidaan todeta, että tietoturvallisuuden perustasoon kuuluvien toimien toteuttamista kolmen vuoden sisällä asetuksen voimaantulosta ei yleisesti voida pitää valtion hallinnon viranomaisen erityisrahoitusta koskevana toimena. Näin etenkin, kun otetaan huomioon, että viranomaisten toiminnan julkisuudesta annetun lain hyvää tiedonhallintatapaa koskevat säännökset ja niihin kuuluva velvoite tietoturvallisuudesta huolehtimisesta on ollut voimassa jo yli kymmenen vuotta. Muut aiheutuvat kustannukset ovat kokonaan riippuvaisia viranomaisten omista ratkaisuista, jotka siten voidaan toteuttaa käytettävissä olevien resurssien puitteissa.

Valtiovarainministeriön toteuttaman viimeisimmän koko valtionhallintoa koskevan tietoturvallisuuskyselyn perusteella on havaittavissa, että suurimmassa osassa viranomaisia useimmat perustietoturvallisuustason nyt ehdotetun asetuksen mukaiset vaatimukset on jo toteutettu. Liitteenä 1 olevassa taulukossa esitetään esimerkkejä asetusehdotuksessa tarkoitetun yleisten tietoturvallisuusvaatimusten ja erityisesti tietoturvallisuuden perustason toteuttamisen tilanteesta valtion virastoissa. Tiedot perustuvat Valtionhallinnon tietoturvallisuuden johtoryhmän toimintakertomukseen vuodelta 2009 (VAHTI 1/2010).

Useat viranomaiset ilmoittivat valtiovarainministeriön hallinnon kehittämisosaston kevään 2009 toteutetussa ehdotettua uudistusta koskeneessa kyselyssä luokituksen käyttöönoton ja korotetun tietoturvallisuustason käyttöönoton aiheuttavan kustannuksia ja henkilötyön kohdentamistarpeita.

Ehdotetun asetuksen mukaisen luokittelun käyttöönoton kustannuksia vähentävät olennaisesti perustietoturvallisuustason toimeenpanon varsin hyvän lähtötilanteen lisäksi viranomaisten ehdotetun asetuksen mukaan joustavat mahdollisuudet luokituksen käyttöönotosta ja sen laajuudesta päättämisessä (7 ja 8 §), nykyisin jo käytännössä sovellutettujen toimenpiteiden vastaavuus kahdessa korkeimpaan suojaustasoon kuuluvien asiakirjojen suojaamisessa samoin kuin asetusehdotukseen otetut ja eri osapuolten kanssa yhteistyössä valmistellut suojaustasoja III ja IV koskevat vaatimukset.

Valtiovarainministeriö selvitti vuonna 2008 luokiteltavan aineiston jakautumista eri suojaustasoihin. Määrällisesti suurin osa kaikesta luokiteltavasta aineistosta on matalinta suojaustasoa IV, jonka käsittelyvaatimuksista on asetukseen ehdotettu otettaviksi vain rajoitetuissa tapauksia koskevia käsittelyä koskevia vaatimuksia ja jota voidaan mm. käsitellä selväkielisenä viranomaisen perustietoturvallisuustason tietojenkäsittelyympäristössä.

Selvityksen mukaan jotakuinkin kaikilla viranomaisilla on suojaustasoihin III ja IV kuuluvia tietoaineistoja. Toisaalta useilla viranomaisilla ei ole ollenkaan suojaustasoihin I – II kuuluvia aineistoja. Suojaustasoihin I ja II kuuluvien tietoaineistojen osuus kaikesta luokiteltavasta tietoaineistosta on muutama prosentti. Yksittäisillä viranomaisilla niiden toimialan vuoksi suojaustasoihin I ja II kuuluvien aineistojen yhteenlaskettu osuus voi kuitenkin olla jopa kolmannes luokiteltavista asiakirjoista (esim. puolustus- ja

ulkoasiainhallinto). Näiden viranomaisten luokituksen käyttöönottoa helpottaa ja sen kustannuksia vähentää asetuksessa ehdotettujen säännösten (7 ja 8 §) lisäksi käynnissä oleva turvallisen viranomaisten turvallisuusverkon toteuttaminen (ns. TUVE-hanke).

Erityisesti korkeimpiin suojaustasoihin kuuluvien valtionhallinnon viranomaisten tietoaineistojen käsittely edellyttää tietoteknisten salausratkaisujen käyttöä. Sähköisten menettelyjen käyttöönoton luokiteltavien tietoaineistojen käsittelyssä ja siirrossa arvioidaan edellyttävän viestinvälityksen salausratkaisuun perustuvien tekniikoiden käyttäjien lisäämistä valtionhallinnossa nykyisestä noin 30 000:sta noin 60 000 – 70 000 käyttäjään. Sähköisiin toimikortteihin perustuvan viestinvälityksen salauksen käytön lisäämisen voidaan arvioida maksavan valtionhallinnossa yhteensä noin 900 000 euroa seuraavien viiden vuoden aikana. Toimikorttien käytön lisääminen tukisi kuitenkin samalla myös luotettavan sähköisen tunnistamisen ja sähköisen allekirjoituksen leviämistä. Tästä koituvana hyötynä on otettava huomioon sähköisen asioinnin helpottuminen mm. viranomaisten välisessä tietojenvaihdossa, mikä luo mahdollisuuksia tietojenkäsittelyn ja tietojenvälityksen säästöihin.

Ehdotetun asetuksen mukaisen luokituksen käyttöönoton kustannukset ovat riippuvaisia viranomaisten omista päätöksistä (7 ja 8 §). Luokituksen käyttöönoton asiallisena ja viranomaisen toimintaan sopivana perustana olisivat normaali toiminnan- ja talouden suunnittelu sekä hallinnonalan taloudelliset kehykset.

Asetuksen täytäntöönpanon ohjausta on tarkoitus tehostaa valtiovarainministeriön antamilla ohjeilla. Ohjeissa määriteltäisiin mm. perustietoturvallisuustasoa koskevat vaatimukset sekä tietoaineistoja ja verkkoja koskevat tietoturvallisuusvaatimukset. Ohjeet on tarkoitus antaa asetuksen antamisen jälkeen ja ennen sen voimaantuloa. Ohjeiden lisäksi on tarkoitus järjestää uudistuksesta koulutusta erityisesti tietoturvallisuudesta ja hallinnosta vastaaville henkilöstöryhmille.

Valtiovarainministeriö seuraa asetuksen ja ohjeiden täytäntöönpanoa. Oikeusministeriö ja valtiovarainministeriö selvittävät yhteistyössä vuoden 2012 aikana, onko tarpeen säätää laissa nykyistä laajemmin asiakirjojen luokittelun pakollisuudesta tai onko tarvetta siirtymäaikoja koskeviin muutoksiin.

Liite 1:

Tietoturvallisuuden perustason vaatimusten toimeenpano 2009

Lähde: Valtionhallinnon tietoturvallisuuden johtoryhmän toimintakertomus vuodelta 2009 (VAHTI 1/2010).

Tietoturvallisuuden perustason vaatimusten toimeenpanon kohde	Toteuttaneiden valtion organisaatioiden prosenttiosuus
Organisaatiossa on sovittu käyttövaltuuksien hallintaperiaatteet	94
Tunnukset ja valtuudet hoidetaan käyttövaltuuksien hallintaperiaatteiden mukaisesti	92
Organisaatiossa on nimetty tietoturvallisuusvastaava	86
Vakavista tietoturvallisuuspoikkeamista raportoidaan johdolle	85
Keskeiset osa-alueet kattava tietoturvallisuusohjeisto	84
Tilat on eriytetty tietojen suojausluokkien mukaisesti	83
Tietoturvallisuuspoikkeamien käsittely on organisoitu/vastuutettu	74
Tietoverkon eri suojaustasoa vaativat osat on eriytetty	73
Valmiussuunnitelma	71
Tietoturvallisuuspolitiikka	70
Tietoturvallisuussuunnitelma	70
Toiminnan kattava tietoturvallisuusvalvonta ja poikkeamaraportointi	70
Tietoturvallisuusvastuut on kuvattu tehtäväkuvauksissa	67
Salauksen käyttö tiedostoissa, hakemistoissa ja kovalevyissä	63
Salauksen käyttö viestinvälityksessä	61
Säännöllinen tietoturvallisuusriskien arviointi	56
Turvallisuusselvitysmenettely	51
Jatkuvuussuunnitelma	38