VALTIOVARAINMINISTERIÖ

14.02.2019

lainsäädäntöneuvos Sami Kivivasara

Vastineen täydennys hallituksen esityksestä 284/2018 vp laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi saaduista asiantuntijalausunnoista

Eduskunnan hallintovaliokunta on pyytänyt valtiovarainministeriöltä vastinetta saamistaan asiantuntijalausunnoista. Seuraavassa vastineen täydennys hallintovaliokuntaan 8.2.2019 toimitettuun vastineeseen.

1 Turvallisuusluokittelu ja suojaustasoluokituksesta luopuminen sekä asiakirjojen merkinnät

1.1 Turvallisuusluokittelua koskevan asetuksen välttämättömyys

UM (NSA), LVM, Traficom ja PLM esittävät lausunnoissaan, että Suomea sitovien kansainvälisten tietoturvallisuusvelvoitteiden näkökulmasta on välttämätöntä, että turvallisuusluokittelua, turvallisuusluokiteltaviin asiakirjoihin tehtäviä merkintöjä ja niiden käsittelyä koskeva asetus tulee voimaan samaan aikaan tiedonhallintalain kanssa.

Vastine

Asetuksen valmistelu on varsin pitkällä ja VM on viime viikolla aloittanut asetuksen viimeistelyn turvallisuusluokittelun kannalta tärkeimpien toimijoiden (UM, PLM, VNK, SM, Supo, VRK, Traficom) kanssa. Asetusluonnoksesta pyydetään lausuntoja.

Asetus on tarkoitus saattaa voimaan samaan aikaan ehdotettujen lakien kanssa ja valmistelussa huolehditaan siitä, ettei Suomea sitovien kansainvälisten tietoturvallisuusvelvoitteiden noudattaminen vaarannu asetuksen turvallisuusluokittelua taikka luokiteltujen tietojen käsittelyä koskevien uusien säännösten johdosta.

Valtiovarainministeriö katsoo, etteivät mainitut huomautukset anna aihetta muuttaa lakiehdotusta.

1.2 Turvallisuusluokiteltavat asiakirjat

KHO esittää, että sääntely vaikuttaa epäloogiselta, koska julkisuuslain 24 §:n 1 momentin 2 kohdassa tarkoitetut asiakirjat/tiedot olisivat luokiteltavia, mutta eivät saman momentin 1 kohdassa tarkoitetut ulkopolitiikan ydinalueelle kuuluvat asiakirjat/tiedot. Erityisesti KHO nostaa esille, että momentin vahinkoedellytyslauseke on tulkinnanvarainen.

Vastine

Voimassa olevan tietoturvallisuusasetuksen mukaan turvallisuusluokittelu voi kohdistua julkisuuslain 24 §:n 1 momentin 2 ja 7–10 kohdissa tarkoitettuihin asiakirjoihin. Tätä on julkisuuslain muuttamista koskevassa hallituksen esityksessä (HE 20/2005) perusteltu sillä, että turvallisuusluokitus olisi näin saatettu vastaamaan kansainvälistä käytäntöä.

Turvallisuusluokiteltavien asiakirjojen joukko voidaan määritellä kansallisesti ja pääsääntöisesti tietoturvallisuussopimusten soveltamisalat on sovittu laajoiksi eli ne koskevat kaikkea turvallisuusluokiteltua tietoja, jota sopimuspuolet vaihtavat keskenään.

Esityksessä ehdotetaan luokittelumahdollisuutta laajennettavaksi koskemaan myös 24 §:n 1 momentin 5 ja 11 kohdissa tarkoitettuja asiakirjoja. Valmistelun kuluessa ei ole esitetty, että tarvetta olisi luokitella julkisuuslain 24 §:n 1 momentin 1 kohdassa tarkoitettuja asiakirjoja.

Turvallisuusluokittelumahdollisuuden laajentaminen koskemaan julkisuuslain 24 §:n 1 momentin 5 ja 11 kohdissa tarkoitettuja tietoja johtuu osittain käytännössä ilmenneistä tarpeista, osittain siitä, että ehdotetun sääntelyn mukaan jatkossa muita kuin turvallisuusluokiteltuja asiakirjoja ei enää luokiteltaisi eri suojaustasoille, vaan niitä voitaisiin käsitellä toteuttamalla lain mukaiset tietoturvallisuusvaatimukset riskienhallinnan perusteella.

KHO ei ole esittänyt, millä tavalla vahinkoedellytyslauseke on tulkinnanvarainen.

Valtiovarainministeriö katsoo, etteivät mainitut huomautukset anna aihetta muuttaa lakiehdotusta.

1.3 Turvallisuusluokittelu pakollisuus

UM (NSA) ja Traficom ovat esittäneet lausunnoissaan, että turvallisuusluokittelumahdollisuuden laajentaminen koskemaan myös julkisuuslain 24 §:n 1 momentin 5 ja 11 kohdissa tarkoitettuja asiakirjoja eli muun muassa poliisin taktisia ja teknisiä menetelmiä koskevia asiakirjoja sekä asiakirjoja, jotka sisältävät tietoja raha- ja valuuttapoliittisista päätöksistä, saattaa hankaloittaa kansainvälistä yhteistyötä silloin, kun on tarve nopeaan sähköiseen tiedonsiirtoon ja tarve turvallisuusluokittelulle on hyvin lyhytaikainen. Tietoturvallisuussopimuksissa asetetaan tiettyjä vaatimuksia sähköiselle tiedonsiirrolle ja rajat ylittävä sähköinen tiedonsiirto edellyttää pääsääntöisesti kummankin maan toimivaltaisten viranomaisten hyväksyntää. Tällaisia toimivaltaisten viranomaisten hyväksymiä kanavia on vielä käytössä hyvin vähän, joten nopea tiedonsiirto saattaisi muodostua ongelmalliseksi, jos turvallisuusluokittelu on kaikissa tilanteissa pakollista.

Wallin ja osin KHO ovat myös suhtautuneet turvallisuusluokittelun pakollisuuteen varauksellisesti ja Wallin on todennut mm, että kun mahdollisuus luokitella erilaiset salassa pidettävät asiakirjat nykyiseen tapaan suojaustasoluokkiin poistettaisiin, viranomaisille voi syntyä tarve yleisten turvallisuusetujen suojaamista koskevien salassapitosäännösten laajentavaan tulkintaan. Tietoturvallisuusluokituksen (suojaustaso- ja turvallisuusluokittelu) käytössä voi ongelmana jo muutoinkin olla asiakirjojen ”yliluokittelu”. Vaikutus julkisuusperiaatteen toteutumiselle voi vaikeutua ja johtaa muutoksenhaun lisääntymiseen tiedonsaantia koskevien ratkaisujen johdosta.

KHO on myös esittänyt, että jää epäselväksi, voiko ja tuleeko viranomaisen luottaa siihen, että asiakirjan sille toimittanut valtionhallinnon viranomainen on ylipäätään arvioinut luokittelua ja myös luokitellut asiakirjan oikein, vai onko niin, että asiakirjan saaneen viranomaisen tulee joka tapauksessa arvioida kaikkien sille toimitettujen asiakirjojen luokittelutarve itse laatimiensa asiakirjojen lisäksi.

Lisäksi KHO on huomauttanut, että siirtymäsäännöksessä ei viitata lainkaan ehdotetun lain 18 §:ään. Tämä tarkoittaisi KHO:n mukaan jo olemassa olevien asiakirjojen tarkistamistyötä kaikille viranomaisille, eikä tätä ole huomioitu vaikutustenarvioinnissa.

Vastine

Tietojen luokittelu suojaustasoille ja turvallisuusluokittelu ovat nykyisin julkisuuslain ja tietoturvallisuusasetuksen mukaan harkinnanvaraista (ellei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu). Turvallisuusluokittelun pakollisuuteen on tietoturvallisuussäännösten valmistelun vaiheissa esitetty sekä puoltavia että varauksellisia näkemyksiä.

Lain säännöstä tarkentavan asetuksen valmistelun yhteydessä on pohdittu mahdollisuutta säätää sähköistä siirtämistä koskevasta poikkeuksesta, jonka mukaan asiakirjojen siirtämisessä voitaisiin yksittäistapauksessa käyttää muitakin kuin kyseiselle turvallisuusluokalle tarkoitettuja salausmenetelmiä tai ne voitaisiin siirtää ilman salausmenetelmiä, jos mahdollinen viivästyminen aiheuttaisi ilmeisesti suuremman vahingon kuin turvallisuusluokitellun aineiston mahdollisen paljastumisen aiheuttama vahinko. Tämä ei kuitenkaan voine olla peruste sille, että turvallisuusluokiteltuja tietoja pääsääntöisesti siirretään muilla kuin kyseiselle turvallisuusluokalle tarkoitetuilla salausmenetelmillä. Tällaisen poikkeuksen säätämisellä ei toisaalta kuitenkaan voitaisi poiketa kansainvälisten sopimusten velvoitteista. Tehdyn lisäselvityksen perusteella näyttää siltä, että kansainvälisten tietoturvallisuussopimusten säännöksistä johtuu suoraan se, että tiettyyn turvallisuusluokkaan luokitellut asiakirjat on käsiteltävä tietyin näissä sopimuksissa tarkoitetuin turvallisuustoimenpitein varmistettuna. Näitä varmistuksia ei voida kuitenkaan aina käytännössä toteuttaa, jolloin yksittäisissä, nopeaa tiedonsiirtoa edellyttävissä tilanteissa ei sopimusvelvoitteiden mukaisesti voitaisi tietoja siirtää riittävien tietoturvallisuusmenetelmien mukaisesti. Mikäli kansainvälisiin tietoturvallisuusvelvoitteisiin liittyvistä syistä olisi tarpeen säätää velvoitteesta poikkeusperuste, pitäisi se säätää laissa ja se pitäisi kohdistua suoraan luokitteluun ja sitä koskevan merkinnän tekemiseen. Tällainen poikkeus voitaisiin kohdentaa suppeasti kansainvälisistä tietoturvallisuusvelvoitteista ja niiden toteuttamiseen johtuviin syihin.

Valtiovarainministeriön tekemissä lisäselvityksissä esimerkkinä edellä mainitusta ongelmatiikasta on tullut esiin nimenomaan poliisitoimintaan liittyvien tietojen vaihto. Tietoturvallisuussopimuksissa on sovittu turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta. Pääsääntöisesti tietoturvallisuussopimusten soveltamisalat on sovittu laajoiksi eli ne koskevat kaikkea turvallisuusluokiteltua tietoja, jota sopimuspuolet vaihtavat keskenään. Näin ei kuitenkaan poliisitoimintaa koskevan tiedon osalta ole kattavasti. Esimerkiksi Sveitsin kanssa tehdyn tietoturvallisuussopimuksen (SopS 89/2014) 10 artiklassa polisiin turvallisuusluokiteltu tieto on Sveitsin aloitteesta suljettu nimenomaisesti sopimuksen ulkopuolelle ”This Agreement does not apply to the exchange of Classified Infomation between the intellingence services and the law enforcement agencies (e.g. the police) of the two Parties”. Suurimmassa osassa tietoturvallisuussopimuksia poliisitoimintaan liittyvä tieto on mainittu, mutta edellä mainitun sopimuksen esitöihin on kirjattu: ”Sopimusta ei sovelleta sellaisiin osapuolten välillä vaihdettaviin tietoihin, joita ei ole turvallisuusluokiteltu. Esimerkiksi poliisin tutkinta- ja tiedustelutietoihin ei Suomessa pääosin tehdä turvallisuusluokitusmerkintää.” Tiettyihin ongelmallisiin tilanteisiin, joissa on käytetty muita kuin tietoturvallisuussopimuksissa hyväksyttyjä menettelyjä, Suomi on vastannut siten, että tietoturvallisuussopimus ei sovellu, koska turvallisuusluokitusmerkintää ei ole tehty. Valtiovarainministeriö ei kuitenkaan ole saanut täyttä selvyyttä siitä, kuinka paljon tällaisia tilanteita on ja millä kehittämistoimilla tällaisten tilanteiden syntyminen voitaisiin jatkossa täysin välttää.

Valtiovarainministeriön katsoo, että turvallisuusluokittelun ja sitä koskevan merkinnän säätäminen velvoittavana olisi ehdotetulla tavalla perusteltua sen tavoitteen saavuttamiseksi, että lain säännöksillä yhtenäistettäisiin menettelyjä sekä osaltaan varmistettaisiin salassapidettävien tietojen asianmukaista ja turvallista käsittelyä mm. viranomaisyhteistyössä. Yhtenäisellä toimintatavalla parannettaisiin viranomaisten keskinäistä tiedonvaihtoa ja luottamusta tiedon oikeaan käsittelyyn. Harkinnanvaraista merkintää koskevan säännöksen ei voida katsoa riittävästi toteuttavan tätä, vaikka se sinänsä ohjaakin viranomaisten toimintaa, missä tilanteissa ja millä edellytyksillä merkintä saadaan tehdä.

Valtiovarainministeriö katsoo kuitenkin, että vielä tässä vaiheessa voisi asiakokonaisuuteen liittyvien epävarmuuksien ja kansainvälisen yhteistyön sujuvuuden vuoksi olla tarkoituksenmukaista säätää turvallisuusluokittelu harkinnanvaraiseksi. Tärkeää olisi kuitenkin, että lausunnoissa esiin tuodut ilmeisesti satunnaisiin tarpeisiin liittyvät käytännön tietojärjestelmäratkaisuihin tai toimintaprosesseihin liittyvät haasteet ratkaistaisiin näitä toimintoja kehittämällä, jolloin myös sääntely voitaisiin toteuttaa kattavasti velvoittavana.

Harkinnanvaraisuuden myötä, sääntelyä ei ole tarpeen kohdistaa ainoastaan valtionhallinnon viranomaisiin, mistä johtuisi seurannaismuutoksia ehdotetun tiedonhallintalain 18 §:ään.

Turvallisuusluokittelun muuttaminen harkinnanvaraiseksi tarkoittaisi käytännössä myös sitä, että asiakirjan saanut valtionhallinnon viranomainen voisi turvallisuusluokitella sille toimitetun asiakirjan, vaikkei asiakirjan sille toimittanut valtionhallinnon viranomainen olisi luokitellut asiakirjaa. On tosin otettava huomioon, että erilaiset merkinnät eivät sinänsä tee asiakirjasta salassa pidettävää, vaan asiakirjan salassapito on aina arvioitava erilliskysymyksenä. Tähän liittyy myös julkisuuslain 15 §:ssä säädetty kysymys asiakirjan antamisesta päättävästä viranomaisesta.

Turvallisuusluokittelun harkinnanvaraisuus poistaisi myös KHO:n esille nostaman tarpeen siirtymäsäännöksestä ehdotetun tiedonhallintalain 18 §:n suhteen. Mikäli valiokunta päätyy mietinnössään esittämään lain hyväksymistä hallituksen esityksen mukaisesti, on turvallisuusluokan merkitsemisestä koskevaan velvoitteeseen syytä säätä siirtymäaika. Tämä sen vuoksi, jottei velvoite koskisi KHO:n lausunnossaan esiin nostamalla tavalla kaikkia jo lain voimaan tullessa viranomaisen hallussa olevia asiakirjoja. Lain siirtymäsäännöspykälään voitaisiin lisätä esimerkiksi seuraavan kaltainen säännös:

Tämän lain 18 §:n 1 momenttia sovelletaan lain voimaantulon jälkeen säännöksessä tarkoitetuille viranomaisille saapuviin ja viranomaisen laatimiin uusin asiakirjoihin. Ennen lain voimaantuloa saapuneisiin tai laadittuihin asiakirjoihin voidaan tehdä turvallisuusluokkaa koskeva merkintä.

Turvallisuusluokittelua koskevilla säännöksillä ei puututa salassapitosäännöksiin, jotka edelleen ilmenevät julkisuuslain 24 §:stä tai mahdollisesta muusta lainsäädännöstä taikka kansainvälisestä tietoturvallisuusvelvoitteesta. Näin ollen valtiovarainministeriö ei näe, että turvallisuusluokittelua koskevalla sääntelyllä vaarannettaisiin julkisuusperiaatteen toteutuminen.

1.4 Turvallisuusluokan IV asiakirjojen käsittely

UM (NSA), Traficom ja LVM ovat esittäneet, että ehdotetun tiedonhallintalain 4 luvun tietoturvallisuusvaatimukset eivät kaikilta osin vastaa alimpaan turvallisuusluokkaan kuuluvan kansainvälisen turvallisuusluokitellun tiedon käsittelyvaatimuksia (esim. RESTRAINT UE /EU RESTRICTED), mikä tulee ottaa huomioon asetuksen valmistelussa.

Vastine

Lausunto johtuu ehdotetun tiedonhallintalain 18 §:n 4 momentin yksityiskohtaisissa perusteluissa todetusta tarkoituksesta asetuksen tasolla mahdollistaa alimman turvallisuusluokan asiakirjojen käsittely noudattaen ehdotetussa laissa säädettäviä tiedonhallinnan perusvaatimuksia.

Tarvetta turvallisuusluokan IV lisävaatimuksille on jossain määrin tuotu esille tietoturvasäännösten valmistelun kuluessa. Toisaalta näitä lisävaatimuksia suhteessa tietoturvallisuuden perusvaatimuksiin ei ole pystytty konkretisoimaan.

Asetuksen valmistelussa tullaan ottamaan huomioon kansainväliset tietoturvallisuusvelvoitteet ja se, ettei Suomea sitovien kansainvälisten tietoturvallisuusvelvoitteiden noudattaminen vaarannu asetuksen turvallisuusluokittelua taikka luokiteltujen tietojen käsittelyä koskevien uusien säännösten johdosta.

Valtiovarainministeriö katsoo, etteivät mainitut huomautukset anna aihetta muuttaa lakiehdotusta.

1.5 Turvallisuusluokittelua koskeva asetuksenantovaltuus

Wallinin mukaan perusteluista tai ehdotetusta 18 §:stä ei ilmene nykyisen lainsäädännön tapaan tietoturvallisuusluokituksen tarkoitusta ilmentäviä syitä (ks. esim. julkisuuslain 25 §:n 3 momentti ja 36 §:n 3 – 5 kohta). Tämä vaikuttaa lakiehdotuksen 4 momentin ja siinä säädettäväksi ehdotetun asetuksenantovaltuuden riittävyyteen ja toimivuuteen. Lakia valmistelleilla olisi ollut käytettävissä valmis malli valtuutussäännöksen kirjoittamistavasta julkisuuslain 36 §:n 1 momentin 3 – 5 kohdissa.

Vastine

Valtiovarainministeriö katsoo, että turvallisuusluokkaa koskevan säännöksen yhteyteen sijoitettuna esitetty asetuksenantovaltuus on sinänsä riittävän täsmällinen ja tarkkarajainen. Turvallisuusluokituksen merkitystä ilmentäviä seikkoja voitaisiin kuitenkin täsmentää 18 §:n 1 momentissa. Lisäksi asetuksenantovaltuutta on muutettava, mikäli turvallisuusluokittelu ja sitä koskevan merkinnän tekeminen muutetaan valiokuntakäsittelyssä harkinnanvaraiseksi.

1.6 Turvallisuusluokittelua koskevan sääntelyn siirtäminen tiedonhallintalakiin

Wallinin mukaan julkisuuslain 15 §:n 3 momentin ehdotettu viittaussäännös esitetyllä tavalla muotoiltuna voi aiheuttaa tulkintaongelmia sen suhteen, mikä merkitys asiakirjaan tehdyillä merkinnöillä on suhteessa asiakirjan julkisuuden määräytymiseen. Voimassa olevassa lainsäädännössä selkeän yksiselitteinen lähtökohta ja pääsääntö on, että merkinnät eivät sellaisenaan julkisuuslain mukaista tiedonsaantipyyntöä käsiteltäessä luo tai merkitse salassapitovelvollisuutta; ne toimivat ja välittävät tiedon asiakirjapyyntöä käsittelevälle eräänlaisena varoituksena. Kun lisäksi otetaan huomioon ehdotetun 25 §:n 2 momentin muotoilu, vaarana on, että turvallisuusluokitusta osoittavaa merkintää voitaisiin vastakohtaisuuspäätelmän vuoksi pitää rajoituksena tiedon antamiselle asiakirjasta. Siksi näyttäisikin välttämättömältä, että 15 §:ssä ei viitattaisi suoraan tiedonhallintaa julkishallinnossa koskevaan lakiin, vaan että turvallisuusluokituksesta säädettäisiin nykyiseen tapaan lain 25 §:ssä, johon sisällytettäisiin sopivalla tavalla viittaus tiedonhallintaa julkishallinnossa koskevaan lakiin.

Vastine

Esitetyllä säännösmuutoksella ei muuteta sitä lähtökohtaa, että tietoturvamerkinnät eivät luo tai merkitse salassapitovelvollisuutta. Tällaista ei esityksessä ehdoteta. Valtiovarainministeriön käsityksen mukaan myöskään mahdollista tulkintaongelman syntymistä suhteessa julkisuuden määräytymiseen ei pelkästään sillä, että säännös on joko julkisuuslaissa tai esitetyssä tiedonhallintalaissa voida katsoa syntyvän. Lausuntokommentista jää muutoinkin epäselväksi, mitä siinä esitetään sääntelyratkaisuksi.

Valtiovarainministeriö katsoo, etteivät mainitut huomautukset anna aihetta muuttaa lakiehdotusta.

1.7 Julkisuuslain 25 §:n mukaiset merkinnät

Wallinin lausunnossa on esitetty, että salassapitomerkinnän merkitsemistavasta säätäminen julkisuuslain 25 §:n 2 momentissa ei vaikuta olevan välttämätöntä julkisuuslain luonne yleislakina ja merkintöjen oikeudellinen merkitys huomioon ottaen. Merkintöjen yhdenmukaisuudessa ei ole myöskään osoitettu olevan erityisiä ongelmia käytännössä.

Lisäksi Wallin on todennut, että harkinnanvaraisesti julkisten asiakirjojen kysymyksessä ollen on myös syytä ottaa huomioon, että asiakirja voi olla harkinnanvaraisesti julkinen vain ennen sen lopullista valmistumista. Siten kysymys on usein varsin lyhyestä ajasta ja merkinnän tekeminen olisi usein paitsi tarpeetonta, myös epätarkoituksenmukaista. Merkinnästä säätäminen voi välillisesi vaikuttaa julkisuusperiaatteen soveltamiseen ja väärin tulkittuna käytännössä johtaa tiedonsaannin vaikeutumiseen. Edellä kuvattujen syiden vuoksi katsoisin, että ehdotettu 25 §:n 3 momentti olisi asianmukaisinta jättää säätämättä.

Traficom on todennut, ettei ehdotuksesta ei käy selkeästi ilmi, olisiko merkintä HARKINNANVARAISESTI ANNETTAVA organisaation sisäinen merkintä vai olisiko kolmannen osapuolen mahdollista saada asiakirja, jossa olisi mainittu merkintä. Jälkimmäisessä tilanteessa tulisi myös säätää merkinnän oikeusvaikutuksista, mm. asiakirjan haltijan oikeuksista ja velvollisuuksista tällaisen asiakirjan käsittelyssä. Jatkossakin Julkisuuslain 25 §:n 2 momentin mukaan salassapitomerkintä voitaisiin tehdä muihinkin kuin em. pykälän 1 momentissa tarkoitettuihin asiakirjoihin, ei Traficom näe käyttötarpeita ehdotetulle HARKINNANVARAISESTI ANNETTAVA -merkinnälle. Joka tapauksessa viranomaisen on aina asiakirjapyynnön saatuaan harkittava, onko kyseinen asiakirja luovutettavissa vai ei, joten HARKINNANVARAISESTI ANNETTAVA -merkintä olisi omiaan hämärtämään tätä menettelyä.

Vastine

Merkinnöistä on tällä hetkellä turvallisuusluokiteltujen tietojen osalta säädetty tietoturvallisuusasetuksessa ja lisäksi ohjeistettu VAHTI-ohjeessa.

Merkintöjen velvoittavuuden vuoksi myös salassapitoa koskeva merkintä on perusteltua kirjata säädännön tasolle - eikä merkitsemisestä säätäminen valtiovarainministeriön näkemyksen mukaan vaaranna julkisuuslain luonnetta yleislakina, koska julkisuuslain mukaiset salassa pidettävät asiakirjat kuin turvallisuusluokitellut merkittäisiin jatkossa hyvin yksiselitteisesti merkinnällä ”SALASSA PIDETTÄVÄ”.

Voimassaolevan tietoturvallisuusasetuksen 9 §:n 2 momentin mukaan suojaustasoon IV kuuluvaksi voidaan luokitella muukin kuin salassa pidettäväksi säädetty asiakirja, jos asiakirjan luovuttaminen on lain mukaan viranomaisen harkinnassa tai asiakirjaan sisältyviä tietoja saa lain mukaan käyttää tai luovuttaa vain määrättyyn tarkoitukseen ja jos tiedon oikeudeton paljastuminen voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä.

Säännöstä pidetään edelleen tarpeellisena, koska asiakirjan merkitseminen voi olla tarpeellista 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 merkintä olisi mahdollista, jos asiakirjaan sisältyviä tietoja saa lain mukaan käyttää tai luovuttaa vain määrättyyn tarkoitukseen. Esimerkiksi tiedon luovuttaminen viranomaisten henkilörekisteristä 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.

Mikäli valmisteluvaiheen asiakirja tai henkilötietoja sisältävä asiakirja on sisällöltään salassa pidettävä, tulisi siihen luonnollisesti tehdä salassapitoa koskeva merkintä, koska asiakirjan luovuttamista ja siihen kohdistettavat tietoturvallisuustoimenpiteet tulee toteuttaa siten kuin salassa pidettävien asiakirjojen osalta on säädetty.

Koska valmisteluvaiheen asiakirjojen ja henkilötietojen osalta kyseessä eivät välttämättä kuitenkaan ole varsinaisesti salassa pidettävät asiakirjat, vaan viranomaisella on mahdollisuus antaa niistä tietoja julkisuusperiaate huomioon ottaen harkintansa mukaan tai henkilötietojen käsittelyä koskevien säännösten mukaisesti, ehdotetaan nämä asiakirjat jatkossa merkittäväksi salassapitomerkinnän sijaan merkinnällä ”HARKINNANVARAISESTI ANNETTAVA”.

Merkinnällä ei laajennettaisi julkisuuslain salassapitovelvollisuuden kattamaa alaa, vaan merkinnän tarkoituksena olisi ainoastaan ilmaista asiakirjan käsittelijälle, että asiakirjaan sisältyy tietoja, joiden luovuttamiseen kohdistuu erityisiä edellytyksiä. Kaikkia valmisteluvaiheen asiakirjoja ei olisi tarkoitus merkitä – ainoastaan ne, joissa päädytään julkisuusolettaman mukaisen harkinnan taikka henkilötietojen suojan näkökulmasta siihen, että asiakirjaa ei ole syytä ainakaan tuossa vaiheessa paljastaa rajaamattomalle käyttäjäpiirille. Merkintä ei

muuttaisi sitä, että asiakirjat eivät kuuluisi julkisuuslaissa säädetyn salassapitovelvollisuuden piiriin eikä esimerkiksi sellaisten valmisteluasiakirjojen paljastaminen, jotka eivät sisällä varsinaisesti salassa pidettävää tietoa, ole virkasalaisuuden rikkomisena rangaistava teko.

Julkisuuslain säätämisen yhteydessä kumottiin rikoslain 40 luvun 6 §, jossa säädettiin rangaistavaksi ns. ei julkisen asiakirjan paljastaminen. Tällä haluttiin mm. lisätä valmistelun avoimuutta. Tällaisen tiedon paljastaminen ja tässä momentissa tarkoitetun tiedon paljastaminen voisi julkisuuslain perustelujen (HE 30/1998, rikoslain 40 luvun 6 §:n muutoksen yksityiskohtaiset perustelut) mukaan olla virkavelvollisuuden rikkomista, ei salassapitovelvollisuuden rikkomista. Henkilötietojen paljastamisen osalta on toki otettava huomioon henkilötietojen käsittelijän vaitiolovelvollisuus.

Suojaustasomerkinnästä luopuminen ja vastaavien ns. harkinnanvaraisesti julkisten asiakirjojen merkitseminen on syytä mahdollistaa. Suojaustasomerkintää koskeva käytäntö on voinut johtaa harhaanjohtavasti pitämään suojaustasomerkinnöin varustettuja asiakirjoja salassa pidettävinä. Tässä mielessä merkintä ”HARKINNANVARAISESTI ANNETTAVA” on julkisuusmyönteisempi eikä muuta nykyistä asiantilaa sen osalta, kuka päättää ja millä edellytyksillä valmisteluvaiheen asiakirjan antamisesta taikka henkilötietojen luovuttamisesta.

Valtiovarainministeriö katsoo, etteivät mainitut huomautukset anna aihetta muuttaa lakiehdotusta.

Täydennetyt muutosehdotukset hallituksen esityksen lakiehdotuksiin

Valtiovarainministeriö esittää, että lakiehdotuksiin tehtäisiin seuraavia muutoksia valiokuntakäsittelyssä perustuen edellä mainittuihin turvallisuuluokittelua koskeviin asioihin sekä eräisiin muihin aiemmassa vastineessa ja muutoin valiokuntakäsittelyn kuluessa esiin tulleisiin seikkoihin.

Hallituksen esityksen 1. lakiehdotuksen 3 §:n 1 momentti	**Muutosehdotus**
Tätä lakia sovelletaan tiedonhallintaan ja tietojärjestelmien käyttöön, kun viranomaiset käsittelevät tietoaineistoja, ellei muualla laissa toisin säädetä. Mitä tässä laissa säädetään viranomaisesta, sovelletaan myös yliopistolaissa (588/2009) tarkoitettuihin yliopistoihin ja ammattikorkeakoululaissa (932/2014) tarkoitettuihin ammattikorkeakouluihin.	Tätä lakia sovelletaan tiedonhallintaan ja tietojärjestelmien käyttöön, kun viranomaiset käsittelevät tietoaineistoja, *jollei* muualla laissa toisin säädetä. Mitä tässä laissa säädetään viranomaisesta, sovelletaan myös yliopistolaissa (588/2009) tarkoitettuihin yliopistoihin ja ammattikorkeakoululaissa (932/2014) tarkoitettuihin ammattikorkeakouluihin.

Perustelut: Muutos on tekninen kieliasuun liittyvä sana ”ellei” korvataan sanalla ”jollei”, jolloin merkityssisältö ei jää tulkinnanvaraiseksi.

Hallituksen esityksen 1. lakiehdotuksen 3 §:n 2 momentti	**Muutosehdotus**
Asiankäsittelyssä ja palvelujen tuottamisessa noudatettavista menettelyistä, salassapidosta ja tiedonsaantioikeudesta viranomaisten asiakirjoihin sekä asiakirjojen arkistoinnista säädetään erikseen. Tiedonhallinnasta Suomen evankelis-luterilaisessa kirkossa säädetään kirkkolaissa (1054/1993).	Asiankäsittelyssä ja palvelujen tuottamisessa noudatettavista menettelyistä, salassapidosta ja tiedonsaantioikeudesta viranomaisten asiakirjoihin sekä asiakirjojen arkistoinnista säädetään erikseen. Tiedonhallinnasta *ja tietojärjestelmien käytöstä* Suomen evankelis-luterilaisessa kirkossa säädetään kirkkolaissa (1054/1993).

Perustelut: Koska ehdotettua 1. lakiehdotusta sovellettaisiin sekä tiedonhallintaan että tietojärjestelmien käyttöön, on tarpeen lisätä evankelis-luterilaisen kirkon toimintaan liittyvä viittaus myös *tietojärjestelmiin* vastakohtaispäätelmien välttämiseksi siitä, että lakia sovellettaisiin suoraan evankelis-luterilaiseen kirkkoon.

Hallituksen esityksen 1. lakiehdotuksen 14 §	Muutosehdotus
14 § **Tietojen siirtäminen tietoverkossa** Viranomaisen on toteutettava tietojensiirto tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja. Käyttäjän tunnistamisesta yleisölle tarjottavissa digitaalisissa palveluissa säädetään digitaalisten palvelujen tarjoamisesta annetussa laissa (/).	**14 §** **Tietojen siirtäminen yleisessä tietoverkossa** Viranomaisen on toteutettava tietojensiirto *yleisessä* tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja. Käyttäjän tunnistamisesta yleisölle tarjottavissa digitaalisissa palveluissa säädetään digitaalisten palvelujen tarjoamisesta annetussa laissa (/).

Perustelu: Selvyyden vuoksi pykälää ehdotetaan muutettavaksi vastaamaan sen tarkoitusta siten, että pykälästä ilmenee se, että sääntely koskee yleisessä tietoverkossa (Internetissä) tapahtuvaa tietojen siirtämistä. Pykälää ei sovellettaisi tilanteissa, joissa tietojen siirtäminen tapahtuu muussa tietoverkossa kuin yleisessä tietoverkossa. Siten pykälä ei tulisi sovellettavaksi esimerkiksi viranomaisen sisäisessä verkossa tapahtuvaan tietojen siirtämiseen, koska siinä tietojen siirtoon liittyvät riskit eivät ole vastaavia kuin yleisessä tietoverkossa tietoja siirrettäessä.

Hallituksen esityksen 1. lakiehdotuksen 12 §	Muutosehdotus
Tiedonhallintayksikön on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta. Turvallisuusselvitysten tekemisestä säädetään turvallisuusselvityslaissa (726/2014) ja muusta henkilöarvioinnista yksityisyyden suojasta työelämässä annetussa laissa (759/2004).	Tiedonhallintayksikön on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta. *Henkilöturvallisuusselvityksen laatimisen edellytyksistä säädetään turvallisuusselvityslaissa (726/2014). Työnantajan oikeudesta selvittää työntekijän luotettavuuden arvioimiseksi häntä koskevat luottotiedot ja käsitellä huumausainetestejä koskevia tietoja säädetään yksityisyyden suojasta työelämässä annetussa laissa (759/2004).*

Perustelu: Pykälän sisältöä täsmennettäisiin siten, että informatiiviset viittaukset asianomaisiin säädöksiin ja niiden sisältöihin olisivat täsmällisiä.

Hallituksen esityksen 1. lakiehdotuksen 18 §	Muutosehdotus

Turvallisuusluokiteltavat asiakirjat valtionhallinnossa	*Turvallisuusluokiteltavat asiakirjat*
Valtion hallintoviranomaisen, tuomioistuimen ja muun lainkäyttöelimen sekä muun valtion viraston ja laitoksen on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskeva merkintä, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2, 5 tai 7—11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.	*Asiakirja voidaan turvallisuusluokitella ja siihen voidaan tehdä turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuusvaatimuksia asiakirjaa käsiteltäessä noudatetaan. Turvallisuusluokkaa koskeva merkintä voidaan tehdä,* jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2, 5 tai 7—11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.
Turvallisuusluokkaa koskevaa merkintää ei saa käyttää muissa kuin 1 momentissa tarkoitetuissa tapauksissa, ellei merkinnän tekeminen ole tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai asiakirja muutoin liity kansainväliseen yhteistyöhön.	Turvallisuusluokkaa koskevaa merkintää ei saa käyttää muissa kuin 1 momentissa tarkoitetuissa tapauksissa, ellei merkinnän tekeminen ole tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai asiakirja muutoin liity kansainväliseen yhteistyöhön.
Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004) tarkoitettuihin asiakirjoihin on tehtävä turvallisuusluokituksesta merkintä siten kuin mainitussa laissa säädetään.	Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004) tarkoitettuihin asiakirjoihin on tehtävä turvallisuusluokituksesta merkintä siten kuin mainitussa laissa säädetään.
Turvallisuusluokittelusta, turvallisuusluokiteltaviin asiakirjoihin tehtävistä merkinnöistä ja niiden käsittelystä säädetään tarkemmin valtioneuvoston asetuksella.	*Valtioneuvoston asetuksella voidaan säätää:* *1) valtion hallintoviranomaisen, tuomioistuimen ja muun lainkäyttöelimen sekä muun valtion viraston ja laitoksen velvollisuudesta tehdä turvallisuusluokkaa koskeva merkintä 1 momentissa tarkoitettuihin asiakirjoihin;* *2) turvallisuusluokittelusta, turvallisuusluokiteltaviin asiakirjoihin tehtävistä merkinnöistä sekä turvallisuusluokiteltujen asiakirjojen käsittelystä.*
Asiakirjoihin tehtävistä salassapitoa ja käyttörajoituksia koskevista merkinnöistä säädetään viranomaisten toiminnan julkisuudesta annetun lain 25 §:ssä.	Asiakirjoihin tehtävistä salassapitoa ja käyttörajoituksia koskevista merkinnöistä säädetään viranomaisten toiminnan julkisuudesta annetun lain 25 §:ssä.

Perustelu: Olisi lain soveltamisen kannalta tarpeellista, että suoraan säännöksestä ilmenisi voimassaolevan lainsäädännön tapaan tietoturvallisuusluokituksen tarkoitusta ilmentäviä syitä. Näiden syiden lisäämisellä 1 momentin säännöksen voidaan asiallisesti myös tarkentaa ja kohdentaa lakiehdotuksen 4 momentissa säädettäväksi ehdotettua asetuksenantovaltuutta. Mikäli pykälän 1 momenttia muutetaan siten, että merkintöjen tekeminen on harkinnanvaraista, olisi tarpeen asetuksenantovaltuudella mahdollistaa kuten voimassaolevassa sääntelyssä, merkintöjen tekemisen velvoittaminen. Tällainen asetuksenantovaltuus on kohdennettava valtion viranomaisiin, koska muita ei voida asetuksentasoisin säännöksin velvoittaa. Hallituksen esitykseen verrattuna myös sisällöllistä asetuksenantovaltuutta olisi aiheellista muuttaa, koska sanojen ”niiden käsittelystä” voidaan ymmärtää viittavan merkintöjen käsittelyyn. Asiallisesti turvallisuusluokiteltujen asiakirjojen käsittelystä asetuksella säätäminen voisi sisältää esimerkiksi 1 momenttiin tässä ehdotetun lisäyksen mukaisia asiakirjojen käsittelyn tietoturvallisuusvaatimuksia.

Hallituksen esityksen 2. lakiehdotuksen 25 §	**Muutosehdotus**
Merkintä voidaan tehdä muihinkin kuin 1 momentissa tarkoitettuihin asiakirjoihin. Salassapitomerkintä tehdään merkitsemällä asiakirjaan ”SALASSA PIDETTÄVÄ” ja ruotsiksi ”SEKRETESSBELAGD”. Merkinnästä tulee käydä ilmi, miltä osin asiakirja on salassa pidettävä ja mihin salassapito perustuu. Jos salassapito perustuu säännökseen, jossa on vahinkoedellytyslauseke, merkintä voidaan tehdä kuitenkin niin, että siitä ilmenee vain se säännös, johon salassapito perustuu. Kun asiakirjan tai siinä olevien tietojen salassapidolle ei enää ole perusteita merkinnän poistamisesta tai muuttamisesta on tehtävä merkintä asiakirjaan, johon alkuperäinen merkintä on tehty. Merkinnän asianmukaisuus on tarkistettava viimeistään asiakirjaa ulkopuoliselle annettaessa. Muuhun kuin lain mukaan salassa pidettävään asiakirjaan voidaan tehdä merkintä ”HARKINNANVARAISESTI ANNETTAVA” ja ruotsiksi ”UPPGES ENLIGT PRÖVNING”, jos asiakirjan luovuttaminen on lain mukaan viranomaisen harkinnassa tai asiakirjaan sisältyviä tietoja saa lain mukaan käyttää tai luovuttaa vain määrättyyn tarkoitukseen ja jos tiedon oikeudeton paljastuminen voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä. Velvollisuudesta tehdä turvallisuusluokkaa koskeva merkintä säädetään julkisen hallinnon tiedonhallinnasta annetussa laissa.	Merkintä voidaan tehdä muihinkin kuin 1 momentissa tarkoitettuihin asiakirjoihin. Salassapitomerkintä tehdään merkitsemällä asiakirjaan ”SALASSA PIDETTÄVÄ” ja ruotsiksi ”SEKRETESSBELAGD”. Merkinnästä tulee käydä ilmi, miltä osin asiakirja on salassa pidettävä ja mihin salassapito perustuu. Jos salassapito perustuu säännökseen, jossa on vahinkoedellytyslauseke, merkintä voidaan tehdä kuitenkin niin, että siitä ilmenee vain se säännös, johon salassapito perustuu. Kun asiakirjan tai siinä olevien tietojen salassapidolle ei enää ole perusteita, merkinnän poistamisesta tai muuttamisesta on tehtävä merkintä asiakirjaan, johon alkuperäinen merkintä on tehty. Merkinnän asianmukaisuus on tarkistettava viimeistään asiakirjaa ulkopuoliselle annettaessa. Muuhun kuin lain mukaan salassa pidettävään asiakirjaan voidaan tehdä merkintä ”HARKINNANVARAISESTI ANNETTAVA” ja ruotsiksi ”UPPGES ENLIGT PRÖVNING”, jos asiakirjan luovuttaminen on lain mukaan viranomaisen harkinnassa tai asiakirjaan sisältyviä tietoja saa lain mukaan käyttää tai luovuttaa vain määrättyyn tarkoitukseen ja jos tiedon oikeudeton paljastuminen voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä. *Turvallisuusluokkaa koskevan merkinnän tekemisestä säädetään julkisen hallinnon tiedonhallinnasta annetussa laissa.*

Perustelu: Jos tiedonhallintalain 18 §:ää koskevaa ehdotusta muutetaan siten, että turvallisuusmerkintä olisi harkinnanvarainen, on julkisuuslain 25 §:n 3 säädettäväksi ehdotettu viittaussäännös muutettava siten, ettei siinä viitata velvollisuuteen. Samalla toistetaan valiokunnalle jo toimitetussa vastineessa 25 §:n 1 momenttiin tehtävä pilkun lisäysehdotus.

Hallituksen esityksen 5. lakiehdotuksen 3 § 1 mom 11) kohta	**Muutosehdotus**
11) luokitellulla asiakirjalla viranomaisten toiminnan julkisuudesta annetun lain 5 §:n 1 momentissa tarkoitettua asiakirjaa, johon julkisen hallinnon tiedonhallinnasta annetun lain (/) tai sen nojalla annettujen säännösten nojalla taikka kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004) nojalla on tehty turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuusvaatimuksia asiakirjaa käsiteltäessä noudatetaan.	11) luokitellulla asiakirjalla viranomaisten toiminnan julkisuudesta annetun lain 5 §:n 1 momentissa tarkoitettua asiakirjaa, johon julkisen hallinnon tiedonhallinnasta annetun lain (/) tai sen nojalla annettujen säännösten nojalla taikka kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004) nojalla on tehty *tai voidaan tehdä* turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuusvaatimuksia asiakirjaa käsiteltäessä noudatetaan.

Perustelu: Mikäli turvallisuusluokittelua koskevaa tiedonhallintalain 18 §:ää muutetaan harkinnanvaraiseksi, on tämä otettava huomioon myös turvallisuusselvityslain määritelmäsäännöksessä. Muutosehdotuksen säännös vastaisi voimassaolevaa määritelmää, joka kattaisi määritelmänä myös sellaiset asiakirjat, joihin säännösten mukaan voidaan tehdä merkintä, vaikkei sellaista merkintää olisikaan tehty. Voimassa olevaan säännöksen verrattuna lainkohta muuttuisi vain viittauksen osalta julkisen hallinnon tiedonhallinnasta annettuun lakiin.

Hallituksen esityksen 5. lakiehdotuksen 19 § 1 mom 1) kohta	**Muutosehdotus**
Perusmuotoinen henkilöturvallisuusselvitys voidaan laatia sellaiseen palvelussuhteeseen tai toimeksiantotehtävää suorittamaan valittavasta taikka palvelussuhdetta tai toimeksianto-tehtävää hoitavasta, joka: 1) saa oikeuden muutoin kuin satunnaisesti käsitellä sellaisia viranomaisen asiakirjoja, jotka tulee turvallisuusluokitella turvallisuusluokkaan II—III kuuluviksi, taikka muutoin hoitaa sellaisia tehtäviä, joissa hän salassa pidettäviä tietoja paljastamalla tai muulla lainvastaisella teolla voi merkittävällä tavalla vaarantaa valtion turvallisuutta, maanpuolustusta, kansainvälisiä suhteita, poikkeusoloihin varautumista, väestönsuojelua tai yhteiskunnan elintärkeitä toimintoja taikka mainittujen etujen suojaamiseksi toteutettuja turvallisuusjärjestelyjä;	Perusmuotoinen henkilöturvallisuusselvitys voidaan laatia sellaiseen palvelussuhteeseen tai toimeksiantotehtävää suorittamaan valittavasta taikka palvelussuhdetta tai toimeksianto-tehtävää hoitavasta, joka: 1) saa oikeuden muutoin kuin satunnaisesti käsitellä sellaisia viranomaisen asiakirjoja, jotka *voidaan tai* tulee turvallisuusluokitella turvallisuusluokkaan II—III kuuluviksi, taikka muutoin hoitaa sellaisia tehtäviä, joissa hän salassa pidettäviä tietoja paljastamalla tai muulla lainvastaisella teolla voi merkittävällä tavalla vaarantaa valtion turvallisuutta, maanpuolustusta, kansainvälisiä suhteita, poikkeusoloihin varautumista, väestönsuojelua tai yhteiskunnan elintärkeitä toimintoja taikka mainittujen etujen suojaamiseksi toteutettuja turvallisuusjärjestelyjä;

Perustelu: Jos tiedonhallintalain 18 §:ää koskevaa ehdotusta muutetaan siten, että turvallisuusmerkintä olisi harkinnanvarainen, on tätä koskeva ilmaus lisättävä myös kyseessä olevaan turvallisuusselvityslain kohtaan.