



25.9.2019

Luonnos valtioneuvoston asetukseksi asiakirjojen turvallisuusluokittelusta valtionhallinnossa – yhteenveto saaduista lausunnoista

Valtiovarainministeriössä on valmisteltu luonnos valtioneuvoston asetukseksi asiakirjojen turvallisuusluokittelusta valtionhallinnossa.

Julkisen hallinnon tiedonhallinnasta annetun lain (906/2019, *tiedonhallintalaki*), voimaantulon myötä 1.1.2020 asiakirjojen ja niiden käsittelyn tietoturvaselvoitteista sekä turvallisuusluokiteltavista asiakirjoista säädetään tiedonhallintalaissa. Laki sisältää vähimmäisvaatimukset asiakirjojen, mukaan lukien salassa pidettävien asiakirjojen tietoturvalliselle käsittelylle.

Tiedonhallintalain 18 §:n 1 momentin mukaan valtion virastoissa ja laitoksissa toimivien viranomaisten, tuomioistuimen ja valitusasioita käsittelemään perustettujen lautakuntien on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvasuustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan. Turvallisuusluokkaa koskeva merkintä on tehtävä, 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.

Lausuntopyynnön kohteena olevalla valtioneuvoston asetuksella on tarkoitus tiedonhallintalain 18 §:n 4 momenttiin sisältyvän asetuksenantovaltuuden mukaisesti säätää turvallisuusluokittelusta, turvallisuusluokiteltaviin asiakirjoihin tehtävistä merkinnöistä ja turvallisuusluokiteltujen asiakirjojen käsittelyyn liittyvistä tietoturvasuustoimenpiteistä.

Tiedonhallintalain kanssa samaan aikaan tulee voimaan viranomaisten toiminnan julkisuudesta annetun lain (621/1999) asiakirjojen luokittelua ja tietoturvaselvoitevaatimuksia sekä asetuksenantovaltuutta koskevien säännösten kumoaminen (907/2019), jonka johdosta kumoutuu myös julkisuuslain nojalla annettu asetus tietoturvaselvoitteesta valtionhallinnossa (681/2010, *tietoturvaselvoiteasetus*). Kansainvälisten tietoturvaselvoitteiden noudattamisen näkökulmasta on tärkeää, että turvallisuusluokiteltuja asiakirjoja koskevan asetuksen vaatimukset tulevat voimaan samaan aikaan kun edelliset vaatimukset lakkaavat olemasta voimassa. Asetuksen on siten tarkoitus tulla voimaan 1.1.2020.

Lausuntopyyntö, jakelu ja lausunnon antaneet

Asetusluonnos oli lausuntokierroksella 12.6.–30.8.2019.

Lausuntopyyntöön jakelussa olivat ministeriöt, Ahvenanmaan Maakuntahallitus, Ahvenanmaan valtionvirasto, Aluehallintovirastot, Eduskunnan kanslia Eduskunnan oikeusasiamies, Elinkeinoelämän keskusliitto, ELY-keskukset, ELY-keskusten ja TE-toimistojen kehittämis- ja hallintokeskus (KEHA-keskus), Energiavirasto, Espoon kaupunki, Finanssiala ry, Finanssivalvonta, Geologian tutkimuskeskus, Hansel Oy, Helsingin hallinto-oikeus, Helsingin hovioikeus, Helsingin kaupunki, Huoltovarmuuskeskus, Hämeenlinnan hallinto-oikeus, Häätäkeskuslaitos, Ilmatieteenlaitos, Itä-Suomen hovioikeus, Kansallisarkisto, Kansaneläkelaitos, Keskusrikospoliisi, KEVA, Kilpailu- ja kuluttajavirasto, Konkursiasiamiehen toimisto, Korkein hallinto-oikeus, Korkein oikeus, Kuluttajariitalautakunta, Lahden kaupunki, Liikenne- ja viestintävirasto, Luonnonvarakeskus, Lääkealan turvallisuus- ja kehittämiskeskus Fimea, Maahanmuuttovirasto, Maanmittauslaitos, Markkinaoikeus, Metsäkeskus, Mikkelin kaupunki, Museo- virasto, Oikeuskanslerinvirasto, Oikeusrekisterikeskus, Onnettomuustutkintakeskus, Opetushallitus, Opintotuen muutoksenhakulautakunta, Oulun kaupunki, Patentti- ja rekisterihallitus, Pelastuslaitokset, Pelastusopisto, Poliisiammattikorkeakoulu, Poliisihallitus, Puolustushallinnon rakennuslaitos, Pääesikunta, Rajavartiolaitoksen esikunta, Rikosseuraamuslaitos, Ruokavirasto, Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira), Sosiaaliturva-asioiden muutoksenhakulautakunta, Suojelupoliisi, Suomen Erillisverkot Oy, Suomen Kuntaliitto, Suomen Pankki, Suomen ympäristökeskus, Suomen Yrittäjät ry, Säteilyturvakeskus, Tampereen kaupunki, Tasavallan presidentin kanslia, Teknologiateollisuus ry, Terveysten ja hyvinvoinnin laitos, Tietoliikenteen ja tietotekniikan keskusliitto, FiCom ry, Tietosuojavaltuutetun toimisto, Tilastokeskus, Tulli, Turun hallinto-oikeus, Turun hovioikeus, Turvallisuus- ja kemikaalivirasto, Työneuvosto, Työtuomioistuin, Vaasan hallinto-oikeus, Vaasan hovioikeus, Vakuutusosasto, Valtakunnansyyttäjänvirasto, Valtakunnanvoudinvirasto, Valtiokonttori, Valtion talous- ja henkilöstöhallinnon palvelukeskus, Valtion tieto- ja viestintätekniikkakeskus Valtori, Vantaan kaupunki, Verohallinto, Väestörekisterikeskus ja Yhdenvertaisuus- ja tasa-arvolautakunta.

Varsinaisia lausuntoja saatiin yhteensä 68 kappaletta. Lausuntonsa toimittivat seuraavat tahot:

Ahvenanmaan maakuntahallitus
 Ahvenanmaan valtionvirasto
 Eduskunnan oikeusasiamiehen kanslia (EOA)
 Eduskunta
 Elinkeinoelämän Keskusliitto (EK)
 ELY-keskusten ja TE-toimistojen kehittämis- ja hallintokeskus (KEHA-keskus)
 Finanssivalvonta
 Hansel Oy
 Helsingin hallinto-oikeus
 Huoltovarmuuskeskus (HVK)
 Ilmatieteen laitos
 Itä-Uudenmaan pelastuslaitos
 Kansallisarkisto
 Kansaneläkelaitos (Kela)
 KEVA
 Korkein hallinto-oikeus (KHO)
 Liikenne- ja viestintäministeriö (LVM)
 Liikenne- ja viestintävirasto (Traficom)
 Länsi-Uudenmaan pelastuslaitos
 Lääkealan turvallisuus- ja kehittämiskeskus (Fimea)
 Maahanmuuttovirasto (Migri)
 Maanmittauslaitos (MML)
 Maa- ja metsätalousministeriö (MMM)
 Oikeuskanslerinvirasto (OKV)

Oikeusministeriö (OM)
 Oikeusrekisterikeskus (ORK)
 Opetus- ja kulttuuriministeriö
 Oulu-Koillismaan pelastuslaitos
 Pelastuslaitosten kumppanuusverkosto
 Pelastusopisto
 Poliisihallitus (POHA)
 Puolustushallinnon rakennuslaitos
 Puolustusministeriö (PLM)
 Rahoitusvakuusvirasto (RVV)
 Rajavartiolaitos (RVL)
 Ruokavirasto
 Senaatti-kiinteistöt (Senaatti)
 Sisäministeriö (SM)
 Suojelupoliisi (SUPO)
 Suomen Asianajajaliitto (Asianajajaliitto)
 Suomen Erillisverkot Oy
 Suomen Kuntaliitto ry (Kuntaliitto)
 Suomen metsäkeskus
 Suomen Pankki
 Suomen Yrittäjät ry
 Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira)
 Sosiaali- ja terveysministeriö (STM)
 Säteilyturvakeskus (STUK)
 Terveysten ja hyvinvoinnin laitos (THL)
 Tietojohtaminen ry
 Tietosuojavaltuutetun toimisto (TSV)
 Tilastokeskus
 Tulli
 Turun hovioikeus
 Turvallisuus- ja kemikaalivirasto (Tukes)
 Ulkoministeriö (UM)
 Vakuutusosikeus (VakO)
 Valtakunnansyyttäjänvirasto (VKSV)
 Valtakunnanvoudinvirasto (VVV)
 Valtiokonttori (VK)
 Valtioneuvoston kanslia (VNK)
 Valtion talous- ja henkilöstöhallinnon palvelukeskus (Palkeet)
 Valtion tieto- ja viestintätekniikkakeskus (Valtori)
 Valtiovarainministeriö (VM)
 Verohallinto
 Väestörekisterikeskus (VRK)
 Yhdenvertaisuus- ja tasa-arvolautakunta
 Ympäristöministeriö (YM)

1 Yhteenveto lausunnoista

Ehdotettua sääntelyä pidettiin tarpeellisena. Tarkoituksenmukaisena pidettiin myös sitä, että muiden kuin turvallisuusluokiteltavien asiakirjojen luokittelusta luovutaan ja kyseisten asiakirjojen osalta viranomainen voi määrittellä tietoturvallisuustoimenpiteet riskiarvion mukaisesti.

Tarkempia säännöksiä ja ohjeistuksia pidettiin tarpeellisina siksi, etteivät säännöksissä käytetyt osin väljät kriteerit ja riskiperusteinen lähestymistapa eriyttäisi ohjeistusta ja käytäntöjä viranomaisten ja hallinnonalojen välillä.

Useissa lausunnoissa vastustettiin TLIII -asiakirjoille ehdotettuja aiempaa tiukempia käsittelyvaatimuksia muun muassa säilyttämisen ja käsittelyn kirjaimisvelvollisuuden osalta.

Lisäksi useissa lausunnoissa kiinnitettiin huomiota käsitteiden johdonmukaiseen käyttöön muun muassa asiakirjan käsittely -käsitteen osalta.

Lisäksi kiinnitettiin huomiota ehdotettujen säännösten vaikutuksiin ja soveltuvuuteen asiakirjojen käsittelyyn tuomioistuimissa.

Saadut kommentit on ryhmitelty pykäläkohtaisesti, jonka jälkeen on tuotu erikseen esiin kansainvälisiä tietoturvaselvoitteisiin liittyviä näkökohtia ja muita kommentteja sekä asetuksen vaikutuksiin liittyviä kommentteja.

2 Pykäläkohtaiset kommentit

2.1 Soveltamisala (1 §)

Soveltamisalan organisatorinen laajuus

Itä-Uudenmaan pelastuslaitos totesi, että vaikka pelastuslaitokset kunnallisina viranomaisina eivät ole asetuksen soveltamisalan piirissä, muutos turvallisuusluokittelun pakollisuudesta vaikuttaa myös alueen pelastusviranomaisen käytäntöihin. Suomen Erillisverkot Oy nosti saman huomion esiin oman toimintansa osalta. Eduskunta huomautti, että vaikka asetusta ei koske eduskuntaa, sen hallinto pyrkii soveltamaan asetusta yhtenäisten tietoturvakäytänteiden edistämiseksi. Ahvenanmaan maakuntahallitus huomautti, ettei ehdotettua sääntelyä suoraan sovelleta Ahvenanmaalla.

Kuntaliitto painotti pelastustoimea esimerkkinä käyttäen, että tiedot olisi suojattava yhtenäisin ja yhteisin menetelmin käytännössä ja lainsäädännössä. Kuntaliitto esitti, että tiedonhallintalain ja tätä kautta asetuksen sovellusala laajennettaisiin käsittämään sellaiset kunnalliset ja valtiolliset turvallisuusviranomaiset, joilla on tarve käsitellä turvallisuusluokiteltavaa aineistoa. Tällä tavoin turvataan turvallisuusviranomaisten välinen tietojen vaihto sekä viranomaisyhteistyö. Myös Länsi-Uudenmaan ja Oulu-Koillismaan pelastuslaitokset katsoivat, että soveltamisalaa tulisi laajentaa myös kunnallisiin viranomaisiin. Pelastuslaitosten kumppanuusverkosto esitti, että sääntely koskisi kaikkia julkisuuslain 4 §:ssä tarkoitettuja organisaatiota, toimielimiä ja henkilöitä, jotka saavat oikeuden käsitellä turvallisuusluokiteltuja asiakirjoja.

Senaatti katsoi, että valtionhallinnon viranomaisen määritelmään pitäisi sisällyttää myös Senaatti, koska se on jo velvollinen noudattamaan tiedonhallintalakia ja julkisuuslakia. Soveltamisalan laajennuksella välttäisiin työllistäviltä tietoturvaselvoitteita varmistavilta sopimusmenettelyiltä.

MMM katsoi, että perustelumuiotissa pitäisi mainita, ettei asetusta (asetuksenantovaltuudesta johtuen) sovelleta valtion liikelaitoksissa tai itsenäisissä julkisoikeudellisissa laitoksissa.

VakO huomautti, että se käsittelee myös asioita, joissa päätöksentekijä on yksityinen taho ja että jatkovalmistelussa tulisi tarkastella asiaa uudelleen siltä osin, luetaanko valtionhallinnon viranomaisiin esimerkiksi julkista valtaa käyttävät yksityiset yhtiöt tai yksityishenkilöt.

EOA totesi, että tuomioistuimet eivät lainkäyttötoiminnassaan ensisijaisesti sovelle julkisuuslakia vaan oikeudenkäynnin julkisuudesta hallintotuomioistuimissa annettua lakia (381/2007) tai oikeudenkäynnin julkisuudesta yleisissä

tuomioistuimissa annettu lakia (370/2007), jotka ovat julkisuuslakiin nähden erityislakeja. Oikeudenkäynnin ja oikeudenkäyntiasiakirjojen julkisuus on aihepiiri, joka kuuluu perus- ja ihmisoikeuksien ytimeen. Luonnostellun asetuksen merkitykseen on tällaisessa asiayhteydessä suhtauduttava jo lähtökohtaisesti hyvin varauksellisesti.

Myös OM:n, KHO:n ja VakO:n mukaan asetuksessa tai vähintään perustelu-muistiossa tulisi ottaa tuomioistuimen lainkäyttö paremmin huomioon. KHO:n ja VakO:n mukaan tulisi harkita, sovelletaanko kaikkia vaatimuksia tuomioistui-miin lainkaan tai samanlaisina kuin valtionhallinnon viranomaisiin.

Muut kommentit

EOA totesi, että asetusluonnoksen 1 §:n 1 momentin termin tietoturvallisuus-toimenpide kohdalla voisi olla informatiivista viitata tiedonhallintalain 2 §:n 8 kohdan määritelmään.

Valvira ehdotti 1 §:n 1 momenttiin mainintaa myös siitä, että asetuksessa sää-detään asiakirjojen turvallisuusluokittelun perusteista (3 §).

MMM ehdotti 1 §:n 2 momenttiin muotoilua ”*Asiakirjan merkinnöistä ei seuraa sen salassapidettävyys, vaan viranomaisen asiakirjan julkisuudesta ja asiakir-jan saamista koskevan pyynnön käsittelystä säädetään viranomaisten toimin-nan julkisuudesta annetussa laissa (621/1999)*”.

2.2 Määritelmät (2 §)

OM:n mukaan viranomaisen toiminta voidaan organisoida viraston tai laitok-sen muotoon. Päätöksenteon eriyttäminen ei merkitse uuden viranomaisen perustamista, vaikka eriytetystä päätöksenteosta säädettyä saattaa olla tarpeen noudattaa PL 119.2 §:n vaatimuksia. Viranomaisella viitattaneen vi-ranomaisten toiminnan julkisuudesta annetun lain 4 §:ssä tarkoitettuun viran-omaiseen, sillä tiedonhallintalaissa käytetään tätä viranomaisen käsitettä. Jul-kisuuslain 4 §:n 1 momentin 1 kohdan mukaan virasto on mainitussa laissa tarkoitettu viranomainen. Viranomaiset on määritelty julkisuuslain 4 §:n 1 mo-mentissa organisatorisin perustein (ks. HE 30/2008 vp.) Siten laissa tarkoite-tun viranomaiskäsitteen piiriin kuuluvat sellaiset julkisoikeudelliset orgaanit, joiden viranomaisasema on johdettavissa suoraan niiden perustamista ja jär-jestysmuotoa sekä tehtäviä koskevista säännöksistä. Laissa tarkoitettuja viran-omaisia ovat 1 momentin 1 kohdan mukaan valtion hallintoviranomaiset sekä muut valtion virastot ja laitokset. Valtion hallintoviranomaisia ovat ne valtion toimielimet, jotka on asetettu hoitamaan hallintotehtäviä. Niitä ovat esimerkiksi valtion keskushallintoviranomaiset eli valtioneuvosto ja ministeriöt sekä muut valtioneuvoston alaisuuteen kuuluvat hallintoviranomaiset, joiden alueellinen toimivalta on yleinen. Virastossa toimiva viranomainen on määritelmänä vas-toin vakiintunutta käsitystä, ja edellä sanottu huomion ottaen myös eräänlai-nen kehäpäätelmä (Ks. määritelmistä lainkirjoittajan opas kappale 23). Valtion-hallinnon viranomaisen määritelmä on myös viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetussa laissa (1406/2011), jossa valtionhallinnon viranomaisella tarkoitetaan valtion hallinto-viranomaisia ja muita valtion virastoja ja laitoksia sekä tuomioistuimia ja muita lainkäyttöviranomaisia. Määritelmä on sama kuin voimassa olevassa tietotur-vallisuusasetuksessa 681/2010. OM:n näkemyksen mukaan, jos valtionhallin-non viranomaisen määrittäminen asetuksessa on välttämätöntä pitäisi tukeu-tua edellä mainittuihin määritelmiin.

HVK katsoi, että 1 kohdan ilmaisun ”*valtion virastoissa ja laitoksissa toimivia viranomaisia*” tiukka tulkinta johtaa epäselvyyksiin asetuksen soveltamisesta

silloin, kun asiakirja on laadittu muiden kuin viranomaisen henkilöstöön kuuluvien muodostamassa työryhmässä. HVK piti tärkeänä, että asetuksessa tai sen taustamuistiossa huomioitaisiin merkinnän käyttäminen silloin, kun julkisuuslain 4 §:n 1 mom 8 kohdassa mainittu viranomainen laatii salassa pidettävän ja turvallisuusluokiteltavan asiakirjan viranomaisen toimeksiannosta.

Valvira nosti esiin kysymyksen, onko valtioneuvoston asettamien lautakuntien osalta tehty niin tarkka kartoitus, että vain valitusasioita käsittelemään perustetuissa lautakunnissa voi tulla vastaan turvallisuusluokiteltavia asiakirjoja.

RVL:n mukaan asiakirjan käsittelyn käsitteeseen tulisi lisätä kuuluvaksi myös asiakirjan lähettäminen sekä rekisteröinti. TSV esitti harkittavaksi myös hakuja käyttö-ilmainsujen lisäämistä käsittelyn määritelmään. VRK ehdotti asiakirjan lähettämisen mainitsemista. UM piti asiakirjan käsittelyn määritelmässä käytettyjen tietosuoja-asetuksen mukaisten käsitteiden "tallettaminen" ja "tuhoaminen" sijaan parempina arkistolain käsitteitä "tallentaminen" ja "hävittäminen". STUK ei pitänyt lakiteknisesti onnistuneena määritelmää, jossa asiakirjan käsittely pitää sisällään toimintoja, joissa sitä ei varsinaisesti käsitellä (esim. säilytys).

Useiden lausuntojen mukaan käsittely-sanaa pitäisi käyttää johdonmukaisesti (esim. UM, OM, POHA ja Palkeet), esim. TL III- ja II asiakirjoja saa käsitellä hallinnollisella alueella, mutta ei säilyttää, vaikka säilytys kuuluu käsittelyyn. OM:n mukaan esimerkiksi 11 §:ssä rinnastetaan termit "käsitellä" ja "tallettaa" ja 10 §:n 1 momentissa mainittu käsittely kattaa määritelmän mukaan myös säilyttämisen, jolloin säilyttämiseen liittyen vaikuttaa olevan 3 momentissa säädettäväksi ehdotettu huomioon ottaen kaksi eri sisältöistä normia.

Tulli toivoi muiden informatiivisten viittausten tapaan viittausta myös asiakirjan määritelmään. VNK ehdotti, että asetuksessa määriteltäisiin myös asiakirja.

2.3 Turvallisuusluokittelu ja turvallisuusluokan merkitseminen (3 §)

Yleisesti pidettiin tarkoituksenmukaisena, että muiden kuin turvallisuusluokiteltavien asiakirjojen luokittelusta luovutaan ja kyseisten asiakirjojen osalta viranomainen voi määrittellä tietoturvallisuustoimenpiteet riskiarvion mukaisesti.

Toisaalta Senaatti piti ongelmallisena sitä, jos valtionhallinnon viranomaiset vaativat ei-turvallisuusluokiteltavien salassa pidettävien asiakirjojen osalta toisistaan poikkeavia käsittelysääntöjä. Senaatti toivoi sekä käsittelystä että tila- ja järjestelmäturvallisuudesta uusia ohjeita asetuksen kanssa yhtäaikaaisesti. Myös VK huomautti, että riskiperusteinen lähestymistapa on perusteltu, mutta sen toteuttaminen edellyttää ohjausta ja ohjeistamista. Tietojohtaminen ry nosti esiin kysymyksen vanhan ST-luokituksen korkeampien suojaustasojen käsittelyvaatimuksista tulevaisuudessa. Myös Valvira toivoi ohjeistusta siitä, miten vanhan ST-luokittelun poistuminen vaikuttaa esimerkiksi aiemmin STIII- ja STIV-tasolle luokiteltujen terveystietojen käsittelyyn.

OM:n mukaan ehdotetun turvallisuusluokituksen edellytykset on rajattu paitsi tiettyihin salassapitoperusteisiin, myös potentiaalisen vahingon aiheutumiseen tietyille lain säännöksessä mainituille intresseille. Tämä aiheuttaa yhteismitattomuutta lain 18 §:n turvallisuusluokiteltavien asiakirjojen määritelmän ja ehdotettujen turvallisuusluokkien välillä. Erityisen vaikeatulkintaiseksi muodostuu turvallisuusluokkaa IV koskeva säännös, jossa mainittuun luokkaan on luokiteltava asiakirja, jos asiakirjaan sisältyvän salassapidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitettulle yleiselle edulle. Turvallisuusluokitus voi kuitenkin tiedon-

hallintalain 18 §:n mukaan ylipäätään tulla kansallisten asiakirjojen osalta sovellettavaksi vain tilanteessa, jossa tiedon paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa, joka vakiintuneesti on haitan aiheutumista korkeampi kynnyks. Lisäksi vahingon tulee luokitussäännöksestä poiketen aiheutua yleistä etua tiukemmin laissa määritellyille nimenomaiselle eduille.

EOA kiinnitti huomiota siihen, että turvallisuusluokittelun alimmilla portaita sääntely ei välttämättä kohtaa julkisuuslaissa olevan salassapitosääntelyn kanssa esimerkiksi IV-luokassa edellytetyn "haitan" ollessa eräissä julkisuuslaissa vahinkoedellytyslausekkeissa mainittua "vaarantamista" kevyempi vaatimus.

YM huomautti, että turvallisuusluokkien III ja IV välinen ero kulminoituu käsitteisiin vahinko ja haitta, ja näiden käsitteiden tulkinnanvaraisuus on aiheuttanut käytännön haasteita luokittelutyössä. Myös Ruokavirasto toivoi tähän käsittejakoon selkeytystä. Tulli katsoi, että eri tasoilla olevat vahingon asteet tulisi käytännössä avata asetuksen perusteluissa. Myös Tukes toivoi käytännön ohjeita luokittelun soveltamiseen.

EOA huomautti myös, että yleisen tuomioistuimen salatessa ratkaisunsa perusteluja ei turvallisuusluokitusmerkinnän tekeminen ratkaisuun ole tällä hetkellä yhteensopivaa tuomioistuinta koskevan erityissääntelyn kanssa.

UM painotti kansainvälisestä näkökulmasta, että neliportainen luokittelu tulee säilyttää.

Tulli huomautti, että perustelumuiotissa mainitaan vain turvallisuusluokitusmerkinnän tekemisestä asiakirjan kopiaan, kun tiedonhallintalain 18 §:n esitöissä mainitaan myös asiakirjan metatiedot. Myös Kansallisarkisto kiinnitti huomiota samaan asiaan. Palkeet huomautti, että säännöksessä tulisi olla maininta myös sähköiseen asiakirjaan tehtävästä merkinnästä, koska tulostettaessa asiakirja paperille merkintä jää vain tietojärjestelmään, jos sitä ei ole merkitty itse asiakirjaan. OM:n ja POHA:n mukaan asiakirjan kopiosta säätämisen systematiikkaa olisi hyvä arvioida jatkovalmistelussa. Voimassa olevan tietoturvasäätöasetuksen 17 §:n 2 momentissa on ollut erillinen säännös asiakirjan kopion luokittelusta.

EOA huomautti, että turvallisuusluokitukset "LUOTTAMUKSELLINEN" tai "KÄYTTÖ RAJOITETTU" antavat yleiskielisen merkityksensä perusteella kuvan vähemmän salaisesta kuin salainen tai salassa pidettävä. Fimea piti tarpeettomana kahden erillisen merkintätavan käyttöä esimerkiksi "ERITTÄIN SALAINEN" tai "TL I", ja piti selkeämpänä pelkkää sanallista merkintää.

STUK piti pykälää vaikeaselkoisena ja esitti pykälän kuvaamista esimerkiksi taulukkomuotoisena tai muutoin selkeämmin.

2.4 Turvallisuusluokituksen vastaavuus kansainvälisiä tietoturvasäätövelvoitteita toteutettaessa (4 §)

STUK piti asetusluonnoksen rajapintoja suhteessa kansainvälisiin tietoturvasäätövelvoitteisiin jossain määrin vaikeaselkoisena ja ehdotti, että kansainvälisistä tietoturvasäätövelvoitteista aiheutuvat poikkeukset ja turvallisuusluokituksen vastaavuus koottaisiin säädöksen loppuun.

VNK:n mukaan pykälään olisi syytä selventää minkä kielisenä tehdään turvallisuusluokitusmerkintä (leima) muunkielisiin asiakirjoihin kuin suomen- ja ruotsinkielisiin. Kysymys on toistuvasti epäselvä valmistelijoille ja kääntäjille, eikä ole helppo ymmärtää, että suomen- tai ruotsinkielisiä leimoja ei voi kääntää.

2.5 Turvallisuusluokkaa koskevan merkinnän poistaminen tai muuttaminen (5 §)

YM totesi, että on perusteltua, että merkinnän saa poistaa tai muuttaa ainoastaan asiakirjan laatineen viranomaisen luvalla. Toisaalta muutos voi tuoda luokiteltavia asiakirjoja vastaanottavalle viranomaiselle turhia haasteita asiakirjojen käsittelyssä ja säilyttämisessä, mikäli laatija on luokitellut asiakirjat korkeampaan luokkaan kuin mitä olisi tarpeen. SUPO korosti, että vaatimus merkinnän muuttamisesta vain asiakirjan laatineen viranomaisen luvalla on erityisen tärkeää. SUPO huomautti ao. perustelumuiustion kohtaan, jossa todetaan ilmeisen perusteettomuuden täyttyvän julkiseksi tulleiden tietojen osalta, että tahallisesti tai tahattomasti julkisuuteen päätyneiden tietojen osalta turvallisuusluokittelu ei voisi automaattisesti poistua.

VNK:n mukaan pykälän ensimmäinen kappale ei ota huomioon laajasti salassa pidettäviä asiakirjoja käsittelevien viranomaisten asiakirjojen määriä. Tuhansia turvallisuusluokiteltuja asiakirjoja käsittävässä arkistokokonaisuuksissa turvaluokitusmerkinnän poistaminen asiakirjakohtaisesti ei ole työmäärällisesti tarkoituksenmukaista, etenkin jos koko kokonaisuus on tullut julkiseksi yleisen 25 vuoden salassapitoajan umpeuduttua. Sen sijaan tapauksessa, jossa yksittäisen asiakirjan turvallisuusluokitus kumotaan tai salassapitopäätöksen mukaisesti lakkaa ennen 25 vuotta, tulee jatkossakin toimia pykälässä esitetyn mukaisesti.

VNK:n mukaan tulee myös ottaa huomioon, että salassapitomerkinä on sekä rekisterissä että asiakirjassa. Pykälää tulisi täsmentää sen osalta, että tarkoiteaanko sekä rekisteriä että itse asiakirjaa. Pykälän nykymuotoisen muotoilun toteutusmahdollisuus tulisi harkita uudelleen myös sen osalta, että säädöstekstin lähtökohtana tuntuu olevan säilytysmuotona paperiasiakirja. Kuitenkin suuri osa valtionhallinnon viranomaisten salassa pidettävistä asiakirjoista on sähköisesti asianhallintajärjestelmissä (pääsääntöisesti kaikki STIV-luokitellut) ja asiakirjan tallennusmuoto usein kuvamuotoinen tiedosto (esim. pdf). Pitkäaikaisempaan säilytykseen asiakirjat usein siirretään asianhallinnasta lukutilaiseen passiivikantaan. Siten on useita syitä, joiden vuoksi sähköisistä asiakirjoista leiman poistaminen voi olla mahdotonta, tai ainakin teknisesti suuritöistä. Edelleen pykälässä tulisi ottaa kantaa siihen, miten salassapitomerkinän poistamisen vastuu jakautuu viranomaisen ja valtionhallinnon asiakirjojen pitkäaikaissäilyttämisestä vastaavan Kansallisarkiston kesken. Lähtökohta valtionhallinnossa on, että sähköisessä asianhallinnassa arkistoidaan rinnan julkiset ja TL IV –luokitellut asiakirjat ja ne siirretään jatkossa kansalliseen säilytyspalveluun (esim. Sapa-palvelu) selvästi nopeammassa aikataulussa kuin yleinen 25-vuoden salassapitoaika päättyy.

Kansallisarkisto huomautti, että vaatimus turvallisuusluokkamerkinän poistamisesta tai muuttamisesta tehtävästä merkinnästä merkitsee Kansallisarkistolle pysyvästi säilytettävien asiakirjojen lopullisena sijoituspaikkana runsaasti työtä, ellei alkuperäisiä (vanhentuneita) merkintöjä ”kumota” siinä vaiheessa, kun asiakirjat siirretään Kansallisarkistoon. Toisaalta Kansallisarkisto voisi monissa tapauksissa käsityksensä mukaan poistaa tälle luovutetun asiakirjan turvallisuusluokituksen 2 momentin perusteella, jos salassapitoaika on umpeutunut.

Palkeet ehdotti, että kohtaa, jossa säädetään ”*jollei ole selvää, ettei perusteita turvallisuusluokan käytölle enää ole*”, tarkennetaan siltä osin, mitä tarkoitetaan selvällä perusteella.

STUK huomautti, että asetusluonnoksesta tai sen perusteluista ei käy ilmi, ketä on pidettävä ulkopuolisena. STUK ehdotti säännöksen muuttamista esimerkiksi muotoon ”...*tarkistettava viimeistään tietoa luovutettaessa.*” Myös UM

kiinnitti samaan asiaan huomiota, ja pyysi täsmennystä siihen, tarkoitetaanko säännöksessä asiakirjan luovuttamisella ulkopuoliselle luovuttamista asiakirjan laatineen viranomaisen ulkopuolelle vai valtion viranomaisten ulkopuolelle.

OM ehdotti, että 5 §:n 1 momentin sanamuodon osalta voisi jatkovalmistelussa arvioida, tarkoitetaanko siinä turvallisuusluokituksen muuttamista vai asiakirjan turvallisuusluokituksen muuttamista.

Fimea piti hankalana merkinnän poistamista paperiasiakirjasta, ja toivoi poistamista kannanottoa.

2.6 Turvallisuusluokitellun asiakirjan antamisen edellytykset (6 §)

Itä-Uudenmaan pelastuslaitos, Kuntaliitto ja Kela esittivät, että asetuksessa, perusteluissa tai ohjaamalla kuvattaisiin menettelytapaa, jolla voitaisiin varistua asianmukaisesta suojaamisesta, kun asiakirja annetaan muulle kuin valtionhallinnon viranomaiselle. Kela toivoi, että asetuksen ylätasoinen kuvauksia täsmällisemmät järjestelmiin kohdistuvat minimivaatimukset olisi kuvattu ja otettu huomioon jo lainsäädännössä.

Ahvenanmaan maakuntahallitus totesi, että koska sääntely ei suoraan ole sovellettavaa Ahvenanmaalla, tulisi valtion puolelta luoda toimivat käytännöt sille, että asiakirjoja voidaan tarvittaessa luovuttaa myös ahvenanmaalaisille viranomaisille.

STUK piti asetusluonnoksen 6 §:n sääntelyä julkisuuslain alaan kuuluvana sääntelynä, josta ei voida säätää asetuksessa. STUK katsoi myös, että asetusluonnoksesta voi saada virheellisen käsityksen, ettei toista valtionhallinnon viranomaista olisi pidettävä salassapidon kannalta ulkopuolisena.

Kansallisarkisto piti jossain määrin epäselvänä asetusluonnoksen 6 §:n ja julkisuuslain 27 §:n suhdetta, jos Kansallisarkistoon siirretään asiakirja, jonka turvallisuusluokitus on vielä voimassa.

Palkeet ehdotti 1 momentin muuttamista seuraavaksi: *”Valtionhallinnon viranomaisen on ennakolta varmistuttava siitä, että turvallisuusluokitellun asiakirjan suojaamisesta huolehditaan asianmukaisesti, kun se antaa turvallisuusluokitellun asiakirjan muulle asiaa hoitavalle tai käsittelevälle taholle.”*

Eduskunta piti 6 §:n 2 momentin ilmaisutapaa kapulakielisenä. Eduskunta ehdottaa muotoiluksi kutakuinkin *”Viranomaisen velvollisuus on tarkistaa ja noudattaa viranomaisten julkisuudesta annetun lain 26 §:n 3 momentin säätelyä tietojen salassapidosta ja suojaamisesta asianmukaisesti tietojen luovuttamisessa muulle kuin valtionhallinnon viranomaiselle”*.

MMM ehdotti julkisuuslakiviittausta siten, että muoto *”... on voimassa, mitä ... säädetään”* korvataan muodolla *”... säädetään ...”*.

EOA huomautti, että yleinen tuomioistuimien ei voine samanaikaisesti noudattaa oikeudenkäyntiin sovellettavaa julkisuuslakia ja toimia turvallisuusluokittelun edellyttämällä tavalla siten kuin luonnostellussa asetuksessa on kaavailtu. VKSV huomautti, että oikeudenkäyntimateriaali on asianosaisjulkista, jolloin mahdollisesti turvaluokiteltu aineisto voidaan joutua luovuttamaan muulle kuin viranomaiselle, eikä luovutukselle voi asettaa ehtoja tietynlaisesta tietoturvallisuudesta käsittelevästä.

Myös Asianajajaliitto totesi, ettei oikeudenmukaisen oikeudenkäynnin edellytyksiä saa vaarantaa turvallisuusluokittelulla tai luokiteltuja asiakirjoja koskevilla käsittelyvaatimuksilla. Asianajajaliiton mukaan tulee turvata rikosprosessin oikeudenkäynnin osapuolille yhtäläinen oikeus käsitellä asiakirjoja, esimerkiksi muuttamalla turvaluokitusta tilanteeseen sopivalla tavalla tai - mikäli edellinen ei ole mahdollista - järjestämällä kaikkien osapuolien oikeus käsitellä asiakirjoja siihen tapaan, jolla oikeudenkäynnin se osapuoli, jolla on vähäisin oikeus käsitellä asiakirjaa, pystyy käsittelemään asiakirjaa. Mikäli tätä vaatimusta ei pystytä täyttämään, tulee turvaluokiteltujen asiakirjojen käyttö olla kyseisen rikosprosessin osapuolilta kielletty.

KHO huomautti, että asetuksessa tai muistiossa ei kerrota, mitä toimia viranomaisen on käytännössä tehtävä, jos turvallisuusluokiteltava asiakirja annetaan esimerkiksi asianosaisen tiedonsaantioikeuden perusteella. KHO katsoi, ettei viranomaisilla ole käytännössä keinoja valvoa yksityisten tekemää tietojen käyttöä eikä yksityisellä taholla ole velvoitetta suojata salassa pidettäviä tietoja sisältäviä asiakirjoja ja niihin sisältyviä tietoja lukuun ottamatta vaitiolovelvollisuutta ja hyväksikäyttökieltoa koskevia velvoitteita. KHO huomautti, että mikäli säännöstä ei ole tarkoitettu sovellettavaksi asianosaisen tiedonsaantioikeuden tilanteessa ja esimerkiksi kuulemismenettelyssä, se pitäisi ilmetä säännöksestä selvästi. Niin ikään säännöksen suhdetta julkisuuslain 16 §:ään tulisi KHO:n mukaan avata. Myös Helsingin hallinto-oikeus kiinnitti samaan asiaan huomiota.

2.7 Monitasoinen suojaus (7 §)

RVL esitti säännökseen selkeitä turvallisuusluokittasoisia vaatimuksia ja jaoteltua.

Kasauman vaikutusta suojaamisvaatimuksissa pidettiin hyvänä huomiona perustelumuistiossa. TSV kaipasi kuitenkin esimerkkejä. EK huomautti, että kasaamalla voidaan tarkoittaa salassa pidettävän tietoaineiston numeraalista määrää tai toisaalta tietojärjestelmän tietojoukkoa, jonka yksittäiset tietueet eivät ole salassa pidettäviä, mutta joita yhdistelemällä niiden voidaan arvioida jossain tilanteissa muodostavan salassa pidettävän kokonaisuuden. EK huomautti, että vaikutuksen korostaminen saattaa johtaa ylilyönteihin, jotka heikentävät merkittävästi toiminnan tehokkuutta ja tietojen sujuvaa käyttämistä.

EK piti tärkeänä, että 7 §:ään on kirjattu toiminnan perustuvan riskienhallinnan periaatteisiin. Tosin samalla asetusluonnos sisältää varsin yksityiskohtaisia vaatimuksia tiedon suojaamisesta, mikä osaltaan vähentää mahdollisuutta aitoon riskiperusteisuuteen. Runsaasti turvallisuusluokiteltua tietoa käsittelevät viranomaiset voivat siksi EK:n mukaan olla haasteiden edessä huomioiden, että ympäristöt ja tiedon käyttämisen tarpeet voivat olla hyvin erilaisia.

Eduskunta huomautti, että organisaatiokohtaiset riskiarvioinnit ja kontrollit eivät tuota yhtenäisiä käytänteitä ja vaatimuksia turvaluokitellun asiakirjan suojaamiseen. LVM piti myös mahdollisena, että riskit lisääntyvät, jos kaikki hallinnonalat tekevät omat riskiarvionsa omilla kriteereillä. Kansallisarkisto ja THL pitivät 7 §:n säännöksiä varsin yleisen tason säännöksiä, jolloin vaarana ilman tarkentavaa ohjeistusta on viranomaisten käytäntöjen eriytyminen. Tilastokeskus ja YM toivoivat selkiytettävän tai ohjeistettavan, mitä riittävä tässä säännöksessä tarkoittaa. YM huomautti, että ylipäättään asetuksen eri kohdissa puhutaan riittävästä toimenpiteistä. Oman riskiarvion korostaminen jättää YM:n mukaan viranomaiselle paljon liikkumavaraa tietoturvallisuuden toteutuksessa ja mitoituksessa. VNK:n mukaan asetusluonnos jättää useassa kohdin vaatimukset niin yleiselle tasolle, etteivät minimivaatimukset ole kaikilta osin riittävän konkreettiset. VNK korosti, että asetuksen vaatimuksia ei voi tiukentaa,

laventaa tai tulkita alempitaisoisella Vahti-ohjeella. Asetuksen ja ohjeen vaatimusten eroavaisuudet voisivat aiheuttaa merkittäviä tulkittamisongelmia esimerkiksi valtionhallinnon viranomaisten jakaessa salassa pidettävää tietoa tai esimerkiksi tietoturvallisuusauditointien kriteeristöjen määrittelyn yhteydessä.

STUK esitti harkittavaksi, olisiko pykälään tarpeen lisätä toimintamallit mahdollisen rikostutkinnan mahdollistamiseksi, viranomaisten tietojen vaihdon turvaamiseksi sekä kokemuksista oppimiseksi ja suojausten kehittämiseksi.

STUK esitti, että pykälässä on lakitekniistä korjaustarvetta, sillä pykälän johdantokappale ja kohdat eivät muodosta loogisia virkkeitä, kuten niiden pitäisi.

VRK ehdotti kohdittain toistuvan ilmaisun "tietojärjestelmän tai tietoliikennejärjestelyn taikka fyysisesti suojatun turvallisuusalueen suojausta" ottamiseksi osaksi johdantotekstiä, jolloin sen toistolta välttyttäisiin.

Tulli huomautti sanamuodon osalta, että yhtäältä säännöksessä puhutaan riskiarvioinnista ja toisaalta ennaltaehkäisevien toimenpiteiden yhteydessä puhutaan uhkien tunnistamisesta. Tullin näkemyksen mukaan riskiarvion voidaan tietyissä tilanteissa ymmärtää sisältävän uhkien tai riskien tunnistamisen.

OM kiinnitti huomiota terminologiaan. Asetuksen 7 §:ssä puhutaan turvallisuusluokittelun sijaan turvaluokittelusta.

2.8 Käsittelyoikeudet ja niiden luettelointi (8 §)

Käsittelyoikeus (1 momentti)

RVL:n mukaan ilmaisu "*työtehtäviensä vuoksi*" tulisi muuttaa ilmaisuksi "*työtai muiden tehtäviensä vuoksi*" esim. tietoja käsittelevien reserviläisten vuoksi. Palkeet esitti sanamuotoa täsmennettävän siten, että asiakirjan käyttöoikeus ulotetaan muun muassa koskemaan asianosaisen oikeutta asiakirjaan.

Kansallisarkisto piti kysymyksiä herättävänä sitä, kuinka viranomaisen tulee osoittaa 1 momentin mukaisten selvitysten antaminen.

Tulli huomautti, että 8 §:n otsikossa käytetään ilmaisua käsittelyoikeudet, kun taas 1 momentissa käyttöoikeus.

KEHA-keskus totesi, että turvallisuus selvityksiä koskevaa kohtaa tulisi selkeyttää, nykyinen muotoilu jättää tulkinnanvaraa henkilöiden tehtävien ja turvaluokitellun aineiston käsittelyn osalta.

STUK totesi vielä, kun kysymys on henkilötietoja koskevasta velvoitteesta, kuuluisi siitä säättäminen henkilötietojen suojan vuoksi STUK:n tulkinnan mukaan asetuksen sijasta mahdollisesti lain alaan.

Luettelointivaatimus (2 momentti)

POHA ehdotti, että käsittelyoikeuksien luettelovaatimuksen sijaan asetustekstiä muotoiltaisiin siten, että viranomaisilla on oltava tieto henkilöistä, joilla on oikeus käsitellä turvallisuusluokkien III–I asiakirjoja. POHA piti vaatimusta vanhentuneena mm. siksi, että TL III asiakirjoja käsitellään pääsääntöisesti ja lähtökohtaisesti sähköisissä tietojärjestelmissä, jotka ovat käyttöoikeushallinnan piirissä. Tätä muutosta kannatti myös EOA.

VNK ei kannattanut muutosta, että myös TLIII-käsittelyoikeus olisi jatkossa erikseen annettava ja siitä pidettävä kirjaa.

Palkeet ehdotti luettelointivelvoitetta luokissa TL II–I, luokan TLIII aineiston osalta tulisi pitää yllä tietoa työtehtävistä, joissa on käsittelytarve sanottuun aineistoon.

STUK katsoi luettelon pitämisen aiheuttavan tarpeetonta hallinnollista taakkaa. Myös VRK viittasi tähän. Esimerkiksi VakO ja VKSV totesivat, että luettelo katkaisi käytännössä koko henkilökunnan. Migri puolsi niin ikään asian uudelleen harkintaa.

YM totesi, että luettelointivaatimus tehostaa tietoturvallisuuden suunnittelua ja toimenpiteiden kohdentamista, kun tiedetään, ketkä organisaatiossa käsittelevät TL III asiakirjoja. Tulli piti luetteloa muun muassa need to know -periaatteen toteutumisen kannalta tärkeänä.

KHO huomautti, että lainsäädännössä ei ole säädetty tällaisen luettelon salassapidosta ja luettelon julkisuudesta voisi olla tuomioistuimen toiminnalle ja siinä mainituille virkamiehille haittaa. Myös Tulli nosti esiin saman huolen.

VM totesi, että luettelosta syntyy uusi henkilörekisteri, jolloin perustelumuistiossa tulisi ottaa huomioon myös tietosuojasääntely.

Työtehtävien päättymisen (3 momentti)

POHAn mukaan säännöksen sanamuoto on tosiasiallisesti liian tiukkana ongelmallinen, minkä vuoksi se tulisi muotoilla uudelleen avoimemmaksi. Palkeet ehdotti, että momenttiin lisättäisiin maininta käyttöoikeuksien poistamisesta.

VNK:n mukaan ”palautettava” terminä viittaa yksinomaan paperiasiakirjoihin, mutta valtaosa viranomaisten STIV-turvaluokitellusta aineistosta on sähköistä ja siten pääsystä salassa pidettävään tietoon on kyse käyttöoikeuksista tai pääsynhallinnasta. Oikeampi ilmaisu olisikin siten puhua sekä palauttamisesta että käyttöoikeuksista.

Kansallisarkisto piti vaarallisena 3 momentin tuhoamista koskevaa mainintaa, sillä tuhoaminen voi tulla kyseeseen vain, jos siihen on viranomaisen lupa, koska riski on, että työntekijä esimerkiksi itsenäisesti tuhoaisi tietoa, joka olisi pysyvästi säilytettävää.

2.9 Turvallisuusalueet (9 §)

Turvallisuusalueet

VNK:n lausunnon mukaan kansainvälisistä vaatimuksista onnistuneesti on nostettu asetusluonnoksen kansallisiin vaatimuksiin turvallisuusalueet (9 §).

Senaatti huomautti, että tilavyöhykkeet aiheuttavat muutostarpeita sen vuokrasopimusehtoihin. Enää ei voitaisi käyttää tilaratkaisuissa raamina VAHTI-ohjeen perus-/korotetun tason tilalle asettamia vaatimuksia. Myös valtion tilaratkaisuissa yleistyvien monikäyttötilojen ja yhteiskäyttötilojen osalta jää epäselväksi, miten asetuksen tilavyöhykkeet suhtautuvat niihin.

KEHA-keskus esitti, että isommissa virastokomplekseissa voitaisiin rakentaa eri viranomaisille yhteisiä turva-alueita, jolloin virastojen ei tarvitsisi rakentaa omia turva-alueitaan.

LVM esitti kysymyksiä, edellytetäänkö EU:n neuvoston turvasääntöjen mukaisen toimivaltaisen viranomaisen päätöstä tilakohtaisesti tilojen jakamista ja

merkitsemistä hallinnollisiin alueisiin ja turva-alueisiin; ja jos näin on, mikä on se toimivaltainen viranomainen, joka hyväksyy alueiden vaatimusten mukaisuuden ja miten valtionhallinnossa alueet merkitään yhtenevällä kaikkien yhteisesti tunnistamalla tavalla.

Migrin mukaan asetuksen minimivaatimukset tilaratkaisuissa jäävät jossain määrin epäselviksi. UM huomautti, että VN-tasolla käytössä olevat käsitteet valvottu, rajoitettu ja suojattu alue sekä toisaalta asetuksen määrittelemät hallinnollinen ja turva-alue voivat aiheuttaa sekaannusta.

PLM ehdotti, että perustelumuioston 7 tai 9 §:n kohdalla voisi esimerkinomaisesti avata niitä keinoja mitä tilojen turvallisuusjärjestelyissä voi käyttää monitasoisen suojauksen periaatteen mukaisesti. Periaatteen mukaisesti tulisi valita turvallisuustoimien yhdistelmä, joka voi koostua esimerkiksi tilojen rajaamisesta fyysisin estein, kulunvalvonnasta, kameravalvonnasta, tunkeutumisen havaitsemisjärjestelmästä ja muista turvallisuusjärjestelyistä.

Kulku turvallisuusalueelle

RVL ehdotti 2 kohdasta ilmaisun "*tiedonsaantitarpeensa perusteella*" poistamista. RVL perusteli asiaa siten, että tarve tulla alueelle ei läheskään aina perustu tiedonsaantitarpeeseen (esimerkiksi siivoajat ja huoltomiehet). Myös Tulli, STUK ja Palkeet nostivat esiin saman asian.

OKV huomautti, että perustelumuiostiossa puhutaan työtehtävistä, ja ehdotti säännösten ja perustelujen muuttamista toisiaan vastaavaksi, eli esimerkiksi tiedonsaantitarpeen sijaan käytettäisiin ilmaisua "*työtehtäviinsä liittyvän välttämättömän tarpeen*".

STM huomautti että turva-alueelle kulku säilytystä varten voi muodostua ongelmalliseksi käytännössä.

Muut huomiot

STUK huomautti, että sanamuotoa on tarpeen muuttaa pykälän 2 momentin 1 kohdassa siten, että "*asianmukaisesti*" sana poistettaisiin tarpeettomana.

2.10 Asiakirjojen käsittely ja säilyttäminen turvallisuusalueilla (10 §)

RVL ehdotti 3 momenttia muutettavaksi käytännön syistä ja tietoturvallisuuden parantamiseksi muotoon "*Turvallisuusluokan IV asiakirja on säilytettävä lukollisessa säilytysyksikössä hallinnollisella alueella tai turva-alueella. Turvallisuusluokan III—I asiakirja on säilytettävä kassakaapissa tai holvissa turva-alueella.*"

POHA katsoi, että TL III -asiakirjojen säilytysvaatimus turva-alueella voi hankaloittaa merkittävästi operatiivista poliisitoimintaa, ja ehdotti, että TL III -asiakirjoja voitaisiin säilyttää hallinnollisella alueella. Samaa ehdotti myös Migri. YM:n näkemyksen mukaan säilytysvaatimus TL III -asiakirjojen osalta turva-alueella tuntuu kohtuuttomalta. YM huomautti, että tarvitaan konkreettinen ohje, mitä suojaustapoja eri turvallisuusluokkien asiakirjojen käsittelyssä edellytetään.

STUK:n mukaan sääntelyä olisi syytä selkeyttää erityisesti siten, että etätöiden tekemisen edellytyksiä ei tarpeettomasti rajoiteta. THL toivoi selvennystä hallinnollisen alueen käsitteeseen ja siihen, millaisilla teknisillä ratkaisuilla etäyhteydet asiakirjojen käsittelemiseksi olisivat mahdollisia.

Valvira nosti esiin pelon turvallisuusriskistä, jos turvallisuusviranomaisissa TL II -aineistoja ryhdytään käsittelemään hallinnollisella alueella.

Tulli toivoi tarkempaa ohjeistusta asetuksen täytäntöönpanosta, ja esimerkiksi siitä kuinka kansallista turvallisuusauditointikriteeristöä (KATAKRI) tulee soveltaa turvallisuusluokiteltavien tietojen suojaamisessa.

STUK:n mukaan 10 §:n osalta sanamuoto ”*on mahdollista*” olisi korvattava mahdollisuuden sijaan oikeutta ilmaisevalla sanamuodolla ”*saa*”. Sama koskee STUK:n mukaan 12 ja 13 §:iä.

VNK:n mukaan pykälässä tulisi ottaa huomioon, että tyypillisesti valtaosa viranomaisen salassa pidettävästä asiakirjallisesta tiedosta säilytetään keskitetysti arkistossa. Muu osa aineistosta on laajasti hajautuneena virkamiesten työtiloissa. Sähköisen aineiston osalta palvelin- ja muut kriittiset ict-infran tilat olisi syytä erikseen huomioida. Pykälä voisi turvallisuuksaluokkalähtöisten vaatimusten ohella huomioida vaatimukset salassa pidettävän tiedon keskitetylle säilyttämiselle ja samoin huomioida vaatimuksia nostava tiedon kasautumisvaikutus, esimerkiksi arkistojen ja palvelintilojen osalta.

2.11 Asiakirjan sähköinen käsittely (11 §)

Yleisesti

VNK:n mukaan valtionhallinnon yhteinen minimivaatimustaso salassa pidettävien asiakirjojen sähköiselle käsittelylle tulisi luonnosta selkeämmin kirjata asetukseen.

Suomen Yrittäjät korosti, että valtion viranomaisen toimiessa hankintayksikkönä sen ei tule vastaisuudessaakaan asettaa asetukseen vedoten liiallisia tietoturva-vaatimuksia suhteessa asiakirjan turvallisuusluokittelun tasoon ja hankittavan tietojärjestelmän, tietoliikennejärjestelyn tai muun palveluratkaisun luonteeseen. Näin on erityisesti silloin, kun hankinnan kohteena on ainoastaan TL IV -asiakirjojen käsittelyyn tarkoitettu järjestelmä.

Eduskunta ehdotti säännökseen lisättäväksi myös vaatimusta TL III–II aineistojen käsittelyyn käytettävien tietojärjestelmien ja tietoliikennejärjestelyiden säännöllisestä auditoinnista.

MML ehdotti 1 momentin johdantoa muutettavaksi seuraavaksi: ”*turvallisuusluokiteltuja asiakirjoja saa käsitellä tai tallentaa vain tietojärjestelmissä ja tietoliikennejärjestelyissä, jotka täyttävät seuraavat vähimmäisvaatimukset (ja kohdat 1-10)*”. MML esitti, että olisi kustannustehokasta, jos valtionhallinnossa arvioidaan keskitetysti toimittajat ja keskitetyt palvelutoimittajat, jotka tuottavat koko hallinnon palveluita. MML:n mukaan on jäänyt avoimeksi, miten viranomaisen tulee toimia, jos palvelussa, tietojärjestelmässä tai tietoliikennepalvelussa havaitaan puutteita ja 11 §:ssä mainitut vaatimukset eivät täyty.

VK huomautti, että monet asetuksen 11 §:ssä esitetyistä toimenpiteistä ovat Valtorin vastuulla, ja siten toimenpiteiden toteuttamisessa olisi perusteltua tehdä yhteistyötä valtionhallinnon sisällä.

STUK piti pykälää pitkänä ja monipolvisena sekä sellaisenaan vaikeaselkoisena. STUK ehdotti luettelon pilkkomista osiin, esimerkiksi omiksi pykälikseen. Lisäksi STUK huomautti, että tallentaminen kuuluu määritelmän mukaan käsittelyyn, joten sitä ei tulisi mainita erikseen 1 momentissa.

SUPO esitti toiminnan jatkuvuudenhallinnan ja häiriöstä toipumisen vähimmäisvaatimusten lisäämistä ja organisaatioiden velvoittamista säännöllisesti arvioimaan tietoturvasuojajärjestelyiden tilaa ja riittävyttä. Myös TSV huomautti, että on syytä arvioida tulisiko vähimmäisvaatimuksissa olla erikseen myös vaatimuksia liittyen tietojärjestelmän tai tietoliikennejärjestelyn suojatun tilanteen palauttamiseen. Asia on huomioitu monitasoisista suojausta koskevassa 7 §:ssä, mutta 11 §:ssä erillisenä selkeänä vaatimuksena se selkiyttäisi tietojärjestelmille asetettujen vähimmäisvaatimusten tulkintaa.

1 kohta

RVL ja eduskunta esittävät, että asetuksen 1 kohtaa tulisi tietoturvasuojauksen lisäämiseksi oikealla ja tarkoituksenmukaisella tavalla muuttaa siten, että ensimmäisessä virkkeessä mainitut luokat IV-II tulisi muuttaa luokiksi IV-III sekä viimeisessä virkkeessä mainittu turvallisuusluokka I laajentaa turvallisuusluokiksi I-II.

Valtori pyysi täsmennystä kohtaan, tarkoitetaanko säännöksellä sitä, ettei TL IV-II asioita ja tietoja saa käsitellä ja tallentaa samassa tietojärjestelmässä matalamman tason turvallisuusluokitellun tietoaineiston kanssa vai tarvitaanko kaksi eri järjestelmää.

PLM ehdotti 1 kohdan osalta, että sääntelyn tulisi mahdollistaa tiedon siirtäminen matalamman turvallisuusluokan tietojärjestelmistä myös TL I tiedon käsittelyyn tarkoitettuihin tietojärjestelmiin. Vastaavasti TL I -tietojärjestelmiin sisältyvää matalamman turvallisuusluokan tietoa olisi voitava siirtää matalamman luokan tiedon käsittelyyn tarkoitettuihin tietojärjestelmiin. Asetuksessa voisi säätää ehdottoman liitännäkiellon sijaan sen riittävästä turvallisuudesta ja mahdollisista erityisvaatimuksista.

2 kohta

VM piti 2 kohdan ilmaisua yleisestä haitallisesta sähköisestä viestistä epätasällisenä ja tulkinnanvaraisena. STUK:n mukaan 2 kohtaan on lisättävä jäsana (tai-sanana sijaan), jotta velvoite edellyttää kumpaakin uhkaan vastaan tapahtuvaa suojautumista.

4 ja 7 kohta

STUK huomautti, että 4 ja 7 kohdassa tulisi miettiä, onko välttämättömyysvaatimus korvattavissa tarpeellisuusvaatimuksella. VRK piti välttämättömyysarviointia 4 kohdassa vaikeana toteuttaa.

VM:n tulkinnan mukaan 4 ja 7 kohdissa jää epäselväksi se, koskevatko vaatimukset vain turvallisuusluokiteltujen asiakirjojen käsittelyä vai järjestelmiä itsessään yleisluonteisesti.

5 kohta

POHA piti 5 kohtaa mahdollisesti vaikeana toteuttaa sen ehdottoman muotoilun vuoksi. Käyttöoikeuksia myönnetään työtehtävien edellyttämässä laajuudessa. Mikäli henkilöllä on käyttöoikeus, voi olla mahdotonta estää tietojen luovutusta käsittelyä. Muotoilu tulisi arvioida uudelleen vähemmän ehdottomaksi.

VRK myös huomautti, että asiakirjojen eheyden varmistamiseksi asiakirjat tulisi allekirjoittaa hyväksytyllä sähköisellä allekirjoituksella.

2 momentti

Kuntaliitto ehdotti lauseen ”*käsittelyssä turvallisuusluokan III—I asiakirjoja sähköisesti, on pidettävä huolta, että hajasäteilyyn ja elektroniseen tiedusteluun liittyviä riskejä on pienennetty riittävästi*” täsmentämistä.

VRK ja Palkeet kyseenalaistivat sääntelyn tarpeellisuuden TL III asiakirjojen osalta.

POHA ei pitänyt vaatimusta TEMPEST-työasemista ongelmattomina, kun runsaasti TLL III -asiakirjoja käsittelevässä organisaatioissa syntyisi valtavasti kustannuksia uusista hankittavista työvälaineistä ja toisaalta tekisi TLL III -asiakirjojen käsittelystä poliisin operatiivisessa kenttätoiminnassa mahdotonta.

2.12 Asiakirjan siirtäminen tietoverkon kautta (12 §)

Eduskunta katsoi, että TL IV -asiakirjaa pitäisi voida siirtää viranomaisen fyysisesti suojatussa verkossa ilman salausta, ja toisaalta TL II ja I -aineiston siirron turva-alueella pitäisi edellyttää salattua siirtoa vähintäänkin tietoliikenteen osalta. SUPO ehdotti, että hallinnollisella ja turva-alueella myös tietoverkossa tapahtuvan TL II–I -tiedonsiirron tulee olla salattua.

STUK katsoi, että asetuksen sanamuoto jättää epäselväksi, tarkoitetaanko säännöksessä itse asiakirjan vai tietoliikenteen salaamista.

Valvira huomautti, että pykälästä ei käy riittävän hyvin selville voidaanko myös TL I -asiakirjoja siirtää tietoverkon kautta. Salaamatonta tiedonsiirtoa ei Valviran näkemyksen mukaan pitäisi hyväksyä missään tilanteessa eikä missään turvallisuusluokissa.

2.13 Asiakirjan kuljettaminen (13 §)

POHA ja Migri totesivat, että vaatimus jatkuvasta valvonnasta sulkisi pois nykykäytännönä olevan kirjatun kirjeen käytön mahdollisuuden. Myös RVV piti vaatimusta useimmissa tapauksissa pitää riskiin nähden ylimitoitettuna. Jatkossa TL III -aineiston kuljettaminen edellyttäisi käytännössä kuriiria, mikä hidastaa merkittävästi tehtävien hoitamista ja lisää kustannuksia.

VRK huomautti, että asiakirjojen eheyden varmistaminen onnistuisi muun muassa hyväksytyllä sähköisellä allekirjoituksella. VKSV ehdotti riittävien salausten menetelmien osalta annettavan selkeitä ohjeita, kun esimerkiksi syyttäjät kuljettavat asiakirjoja turvallisuusalueilta oikeudenkäyntiin. STUK huomautti, että pykälä olisi mahdollista kirjoittaa noudattaen pääsääntö–poikkeus-muotoilua.

2.14 Asiakirjan käsittelyn seuraaminen (14 §)

SM:n, VNK:n POHA:n Migrin, Valtorin, RVV:n ja Pelastusopiston näkemyksen mukaan käsittelyä, sekä saapumista ja lähettämistä koskevan kirjaamisvelvollisuuden ulottaminen myös TL III -asiakirjoihin aiheuttaa merkittävää lisätyötä. Lisäksi viranomaisilta puuttuvat tällä hetkellä järjestelmät, joihin tiedot voitaisiin tarkoituksenmukaisella tavalla kirjata. SM:n näkemyksen mukaan 14 §:n 1 momentin 1 kohdasta tulee poistaa velvoite kirjata TL III -asiakirjan käsittely.

SUPO ehdotti, että TL III -asiakirjojen osalta tiedon sähköisen käsittelyn automaattinen ja kattava lokitietojen kerääminen voidaan katsoa myös asiakirjan lähettämisen ja vastaanottamisen kirjaamisvaatimuksen täyttäväksi.

Myös eduskunta ja UM pitivät riittävänä kirjaamisvelvollisuuden ulottamista II ja I -tasolle luokiteltaviin asiakirjoihin. UM huomautti lisäksi, että kv-velvoitteita

mukaileva kirjaamiskäytäntö TLIII -luokassa ei tässä yhteydessä ole kannatettava. UM totesi, että 1 momentin 2 kohdan osalta saapuvien ja lähtevien asiakirjojen kirjaamisvelvoite TL III asiakirjojen osalta tulisi koskea ainoastaan kansainvälisten tietoturvallisuusvelvoitteiden alaisia asiakirjoja.

VNK:n mukaan pykälässä voisi selkeästi todeta, että vaatimusten toteuttaminen tulee hoitaa keskitetysti, tyypillisestihän tehtävä kuuluu kirjaamolle. Hajautettu tai vastuuttamaton malli ei ole viranomaisen tietoturvan toteutumista tukeva ratkaisu, eikä käsittelytieto tosiasiallisesti eheästi ole käytettävissä jälkikäteen.

VRK ehdotti 2 kohdassa asiakirjojen aikaleimausta eIDAS-hyväksytyllä aikaleimalla. RVL kannatti säännöksen muotoilua sellaisenaan.

Tietojohtaminen ry huomautti, että sanamuodosta "on kirjattava" huolimatta lokitietojen tulisi kirjautua automaattisesti järjestelmään. Tietojohtaminen ry huomautti myös, että asetuksessa tulisi selkeyttää ja terävöittää sitä, ettei kirjaamisvelvollisuudesta huolimatta tietoja tallenneta julkisten tietojen kanssa samaan järjestelmään.

STUK esitti, että esitetty kopiointia koskeva lupavelvoite on omiaan lisäämään tarpeetonta byrokratiaa. STUK katsoi myös, että nousee esiin kysymys, miten ja kenelle viranomaisessa ilmoitus tai hakemus on tehtävä. Lakiteknisesti STUK piti 14 §:ää hankalasti rakennettuna, ja ehdotti, että poikkeustapaus tuotaisiin esiin johdantokappaleen sijaan omissa momentissaan.

VRK ehdotti säännökseen myös kopion haltijan yksilöivän vesileiman käyttöä.

2.15 Asiakirjan tuhoaminen (15 §)

VNK:n mukaan tarpeettomaksi käyneen TL I-II asiakirjan kopio tuhoamista tai palauttamista koskeva vaatimus ohjaa tiedonhallinnan kannalta väärin käytäntöihin. TL I ja II asiakirjat tulee aina palauttaa viranomaisen rekisterinpitäjälle (yleensä kirjaamo), joka joko dokumentoidusti hävittää asiakirjakopion, poistaa asiakirjakopion rekisterin seurannasta ja/tai arkistoi sen arkistointikäytäntöjen mukaisesti. Tietoturvanäkökulmasta myös toisen viranomaisen jakaman asiakirjan palauttaminen laatijaorganisaatiolle tulisi olla poikkeus, turvallisempaa on raportoida hävitetyistä asiakirjasta kuin turhaan kuljettaa asiakirjaa viranomaisten välillä. Toisen momentin mukaan otettaisiin kansainvälisistä käytännöistä kansalliseen käytäntöön myös TL I-II luokitellun asiakirjan hävittämisestä ilmoittaminen laatineelle organisaatiolle. Kansainvälisissä yhteyksissä on käytössä keskusrekisteri, siis kansallisesti vain yksi taho jolle raportoida. Suomessa kansallinen STII luokiteltu aineisto jaetaan ristiin valtion eri viranomaisten kesken ja siten tuhoamisesta liittyvä ilmoittaminen (raportointi) olisi kansainvälistä esimerkkiä huomattavasti työllistävämpi ja vaikeampi tehtävä. Myös raportoinnin vastaanottaminen merkittävästi lisäisi kirjaamon työmäärää. Mihin tätä raportointia tosiasiallisesti käytettäisiin? Nykyinen käytäntö on ollut toimiva, jossa tarvittaessa on tapauskohtaisesti selvitetty toiselta viranomaiselta tietyn asiakirjakopion elinkaaren käsittelyvaiheet ja tietoon tutustuneet.

POHA huomautti, ette ole aivan ongelmatonta, että arkistoinnista mainitaan tuhoamista koskevassa pykälässä. Kun lähtökohtana ovat tiedon elinkaari ja ennen kaikkea yleisen edun mukaiset arkistointitarkoitukset, ehdotuksesta voi POHA:n mukaan saada vääränlaisen vaikutelman siitä, että tuhoaminen päätää turvallisuusluokiteltujen asiakirjojen elinkaaren. Tältä osin sääntelyä tulisi täydentää ja täsmentää, jottei syntyisi liian suurta riskiä säilytettävän tiedon tuhoamiselle.

Traficom katsoi, että säännös jättää tuhoamisvelvollisuuden osalta tulkinnanvaraiseksi täyttykö tuhoamiseen oikeutetun henkilön vaatimukset, jos tallennusvälineiden (USB-tikut ja kiintolevyt) fyysinen tuhoaminen tapahtuu yksityisen yrityksen työntekijän toimesta viranomaisen valvonnassa. Lisäksi on tulkinnanvaraista, riittääkö useita eri asioita sisältäviä tallennusvälineitä kerralla hävitettäessä turvallisuusselvitetyt valvojan hyväksyminen yleisesti käsittelemään II-I -tason aineistoja vai tulisiko henkilöllä olla tiedonsaantitarve kaikkiin asiakirjoihin, joita hävitettävillä tallennusvälineillä on. Traficom ehdotti, että säännöstä muutettaisiin seuraavaksi: *"Tuhoamisen saa suorittaa vain henkilö, jonka viranomainen on tähän tehtävään määrännyt ja jolla on tuhottavien asiakirjojen turvallisuusluokkaa vastaava turvallisuusselvitys."*

Tullin näkemyksen mukaan säännökseen, perustelumuietioon taikka soveltamisohjeisiin olisi hyödyllistä sisällyttää viittaus siitä, minkälaista menettelyä on noudatettava, kun asiakirja tuhoamisen sijaan palautetaan asiakirjan laatineelle viranomaiselle.

STUK katsoi, että säännös toiselle viranomaiselle tehtävästä ilmoituksesta tuhoamisvaiheessa aiheuttaa tarpeetonta hallinnollista taakkaa, eikä pitänyt muutosta kannatettavana.

UM huomautti, että säännöksessä käytetään erikseen käsitettä asiakirjan kopia. Säännöksissä on UM:n mukaan syytä huomioida, että monet UM:n virkamiehet käsittelevät ainoastaan asiakirjojen kopioita.

VNK:n mukaan informatiivinen viittaus arkistolakiin tulisi muuttaa valtionhallinnon arkistointivastuuta vastaavaan muotoon. Pelkkä viittaus arkistolakiin ei toimi, koska arkistolaissa ei ole yleisiä tai yksityiskohtaisia kirjauksia turvallisuusluokiteltujen asiakirjojen arkistoinnista. Lisäksi tiedonhallintalain 21 § mukaan säilytysaikojen määrittämisen vastuista tullaan säätämään erikseen.

Kansallisarkisto piti säännöksen määräyksiä ja erityisesti perustelumuietion sanamuotoja asiakirjan tuhoamisesta jossain määrin ongelmallisina, sillä niistä ei selkeästi käy ilmi, että muut kuin pysyvään säilytykseen määrätyt/arkistoitavat asiakirjat olisi tuhottava viipymättä säilytysajan päättymisen jälkeen. Kansallisarkiston mukaan asetuksen perusteella ei ole täysin selvää, sovelletaanko asetusta arkistoituihin tietoihin, kun 15 §:ssä säädetään, että turvallisuusluokiteltujen asiakirjojen arkistoinnista säädetään arkistolaissa.

Tietojohtaminen ry huomautti, että asiakirjan tuhoaminen viittaa epäsuorasti siihen, että kaikki turvaluokitellut tietoaineistot tuhoataan, vaikka arkistoinnista säädetäänkin arkistolaissa. Yhdistyksen mukaan turvaluokiteltuun aineistoon kohdistuu tieteellisen tutkimuksen näkökulmasta juuri erityinen intressi, jolloin aineistot pääasiallisesti tulisi säilyttää pysyvästi, jollei erityistä syytä niiden hävittämiseen ole. Yhdistys ehdotti, että 15 §:n otsikossa mainitaan arkistointi.

Valvira huomautti, että turvallisuusluokiteltujen asiakirjojen arkistoinnista ei löydy nykyisestä arkistolaista säännöstä, tältä osin pitäisi asetusta tarkistaa yhdessä tekeillä olevan arkistolain kanssa yhdessä.

VRK ehdotti arkistolaki-viittauksen poistamista tarpeettomana.

Valtorin mukaan säännöstä tulisi muuttaa siten, että viittaus arkistolakiin muutetaan ensimmäiseksi momentiksi luonnoksen viimeisen momentin sijaan. Lisäksi otsake tulisi muuttaa muotoon Asiakirjojen arkistointi ja tuhoaminen. Muutoin asetuksen pykälä viittaa siihen, että turvaluokiteltu aineisto tuhoataan aina. Aineistolla voi olla kansallista merkitystä myös julkiseksi tulon jälkeen tieteellisen tutkimuksen käytössä ja pysyvästi säilytettynä.

2.16 Voimaantulo ja siirtymäsäännökset (16 §)

Senaatti huomautti, että sääntely saattaa aiheuttaa suuren määrän muutostarpeita eri viranomaisen käyttämiin toimitiloihin ja toimitiloja koskeviin vuokrasopimuksiin. Nämä muutostyöt tulevat väistämättä aiheuttamaan myös lisäkustannuksia valtiohallinnolle. Tulli kiinnitti huomiota siihen, ovatko asetusluonnoksen 10 §:n velvoitteet asiakirjojen säilyttämisestä ja käsittelystä turvallisuusalueilla toteutettavissa asetuksessa säädettävän siirtymäajan puitteissa.

VK totesi, että asetusluonnokseen kirjattu riittävä siirtymäsäännös mahdollistaa toimenpiteiden toteuttamisen virastotasolla. STM piti siirtymäsäännöksen kolmen vuoden aikaa erittäin hyvänä. Tulli kannatti vähintään kolmen vuoden siirtymäaikaa. Samalla se kuitenkin huomautti, että mittavat tietojärjestelmä-hankkeet voivat kestää kauemminkin. Haasteita voi myös tulla niiden toimitilojen osalta, jotka on suunniteltu otettavaksi käyttöön ennen kuin on kulunut kaksi vuotta asetuksen voimaantulosta. Näin ollen tulisi pohtia, pitäisikö voimaantulo- ja siirtymäsäännöksiä tarkentaa.

STUK huomautti, että on epäselvää, kattaako siirtymäaika koko asetuksen. STUK:n mukaan siirtymäsäännösten kolmen vuoden aika ja vanhan tietoturvasetuksen kumoutuminen tiedonhallintalain voimaantulon myötä nostaa esiin kysymyksen, mitä säännöksiä valtionhallinnon viranomaiset ovat velvollisia noudattamaan 1.1.2020 alkaen. Siirtymäsäännöstä ei ole rajattu/yksilöity tarkemmin pykälittäin. Tällöin kysymykseksi jää, mitä luokittelumerkintöjä valtionhallinnon viranomaisen on käytettävä 1.1.2020 alkaen. Mikäli uusia luokittelumerkintöjä on tarkoitus soveltaa jo lainvoimaantulosta, olisi 16 §:ää ja sen perusteluja hyvä tältä osin vielä selkeyttää.

STUK huomautti myös, että asiakirjan käsittelyn sisältäessä määritelmän mukaisesti jo arkistoinnin ja säilyttämisen, ei asiakirjaa voi ottaa ”uudelleen käsittelyyn” säännöksen tarkoittamalla tavalla. KHO kiinnitti huomiota samaan asiaan ja katsoi vielä olevan syytä asian tarkastelulle.

Helsingin hallinto-oikeus huomautti, että käsittelyn määritelmä huomioiden jo asiakirjan katselu itsessään voi luoda tarpeen turvallisuusluokittelulle, mille on vaikea nähdä tosiasiallista käytännön tarvetta. VakO totesi, että ”asiakirjan ottaminen uudelleen käsittelyyn” tulisi määritellä tarkemmin, ettei esimerkiksi aiempien ratkaisujen katsominen oikeuskäytännön yhtenäisyyden vuoksi aiheuta luokittelutarvetta.

Kansallisarkisto piti tärkeänä selventää siirtymäsäännöksen käytännön soveltamista siltä osin kuin kyse arkistoidun tiedon uudelleen käsittelystä esimerkiksi tutkimustarkoituksiin.

3 Suhde kansainvälisiin tietoturvallisuusvelvoitteisiin

VNK totesi, että lähtökohta kansallisen salassa pidettävän tiedon käsittelykäytäntöjen lähentämisestä vastaamaan kansainvälisen turvallisuusluokitellun aineiston käytäntöjä on sinänsä myönteinen. Kansainvälisten ja kansallisten turvallisuusluokiteltujen asiakirjojen luonne kuitenkin poikkeaa merkittävästi. Esimerkiksi kansainvälisiä turvallisuusluokiteltuja asiakirjoja käsittelee huomattavasti pienempi määrä viranomaisia kuin kansallisia turvallisuusluokiteltuja asiakirjoja ja lisäksi viranomaisten henkilöstöstä kansainvälisiä turvallisuusluokiteltuja asiakirjoja käsittelee suppeampi PSC-todistukset omaava virkamiesjoukko kuin kansallisia turvallisuusluokiteltuja asiakirjoja. Poikkeavat käsittelysäännöt eivät sen johdosta ole olleet merkittävä ongelma. Tämän johdosta asiakirjojen käsittelysääntöjen rinnastaminen esimerkiksi EU confidential

ja TLIII-luokituksen kesken, eli TLIII-käsittelyvaatimuksien tiukentaminen, aiheuttaisi huomattavaa työmäärän kasvua asiakirjojen käsittelyssä valtionhallinnossa, niin valmistelijoille kuin asiakirjahallinnon henkilöstölle. Valtaosin TLIII – asiakirjojahan edelleen käsitellään analogisesti paperilla.

POHA:n mukaan kansainvälisten asioiden hoitamisen näkökulmasta asetusluonnoksessa on nähtävissä ainakin kaksi merkittävää ongelmaa. Ongelmat juontuvat tiedonhallintalain 18 §:n velvoitteesta turvallisuusluokitteluun sekä turvallisuusluokittelun perusteiden laajentamiseen, joista erityisesti poliisia koskee JulKL 24.1 § 5 kohta. Joidenkin valtioiden viranomaiset eivät oman lainsäädäntönsä nojalla voi käsitellä Suomen lähettämiä turvallisuusluokiteltuja asiakirjoja. Normaali yhteistyö ja tiedonvälitys vaarantuu tai lamaantuu, jos turvallisuusluokittelu on pakollista. Asiakirjan julkisuusluonne on totutusti ilmaistu muulla tavalla kuin sitä kuvaavalla leimalla.

POHA:n mukaan kansainvälisessä yhteistyössä (mm. Europol ja Interpol), jossa Suomi on mukana, on omat tiedonkäsittely- ja tiedonvaihtosääntönsä sekä -kanavansa. Ensisijaisesti näissä yhteistyömuodoissa tulisi käyttää kulloinkin kyseessä olevan järjestelyn mukaisia luokitteluja ja suojattuja viestikanavia. Pakollisen turvallisuusluokittelumerkinnän poikkeukset ja suhde rikos- ja poliisiasioiden tiedonvaihdossa käytettäviin omiin kanaviin ja merkintöihin tulisi mainita asetuksessa ja lainvalmisteluaineistossa selvästi. Lainvalmisteluaineistossa tulisi olla poikkeussäännöistä kirjaus, jossa selkeästi mainitaan erityisjärjestelyistä ja niiden ensisijaisuudesta. (Esimerkiksi suoraan sovellettavassa Europol-asetuksen 29 artiklassa on määritelty, miten luokitellaan Europolille tai Europol-kanavaa käyttäen muulle jäsenvaltiolle toimitettavat tiedot.)

POHA totesi myös, että tietoturvaluusussopimuksissa määritellään sopimusosapuolina olevien valtioiden välillä se, mikä on turvallisuusluokka-leimojen vastaavuus ja miten turvallisuusluokiteltua tietoa vaihdetaan sopimusosapuolien välillä. Aikaisemmin omaksutun tulkintalinjan mukaan poliisissa ja erityisesti sen kv-viestinvaihtoon liittyvissä toiminnoissa käytetään valtaosin ja ensisijaisesti salassapitomerkintöjä, jotka ovat julkisuuslain, Europolin tai Interpolin sääntöjen mukaisia. Tällöin on voitu välttää se, että poliisin salassa pidettävän tiedon välittäminen voisi tulla jonkun muun valtiollisen toimijan tehtäväksi Suomessa. Suomi on sitoutunut sopimuksiin, jotka sisältävät määräyksiä siitä, että turvallisuusluokiteltu tieto välitetään hallitusten välisiä kanavia, ei toimivaltaisten viranomaisten kanavia pitkin. Jos turvallisuusluokkamerkintää joudutaan käyttämään pakollisena, nousee kysymykseksi, millä perusteella asia ollaan lähettämässä jotain muuta kuin sopimuksen mukaista hallitusten välistä kanavaa pitkin, jollei tätä oikeuttavaa järjestelyä ole sovittu.

MML:n mukaan sillä on jatkuvia ja sopimusperusteisia toimintoja, jotka tukevat asiakkaita, kumppaneita tai muita viranomaisia. Osa laitoksen palveluista tukee kansainvälisiä organisaatioita tai hankkeita tai projekteja. Sanottuihin jatkuviin toimintoihin ja sopimuksenomaiseen toimintaan on olemassa oma ohjeistuksensa, jonka noudattamiseen MML on sitoutunut sopimuksin. MML:n asiakkailla tai kumppaneilla voi olla turvallisuusluokituksesta poikkeavia tai sitä tarkempia ohjeistuksia. Kun kysymys on kansainvälisestä, Euroopan unionin, PohjoisAtlantin liiton (NATO) tai Puolustushallinnon toiminnasta, MML noudattaa ko. ohjeistusta.

LVM:n lausunnon mukaan asetuksen muistio tarkentaa riittävästi kansainvälisten tietoturvalvelvoitteiden käytänteitä.

PLM:n mukaan sääntelyä on osin tarkennettu aiemmasta ja osin kirjoitettu yleisemmällä periaatetasolla, minkä johdosta muotoilu kestää paremmin muuttuvia olosuhteita sekä vastaa paremmin kansainvälistä sääntelyä.

4 Muut kommentit

Yhdenvertaisuus- ja tasa-arvolautakunta totesi, ettei asetus- tai muistioloanonoksesta ilmene riittävän selkeästi, minkä laajuisiin toimenpiteisiin viranomaisen on ryhdyttävä esimerkiksi monitasoisen suojauksen (7 §) käsittelyoikeuksien ja niiden luetteloinnin (8 §) tai turvallisuusalueiden (9 §) toteuttamiseksi organisaatiossa, jossa turvallisuusluokiteltavien asiakirjojen käsittely on periaatteessa mahdollista, mutta epätodennäköistä.

Itä-Uudenmaan pelastuslaiton piti rikoslain pakkotilasäätelyn esiin nostoa asetuksen perustelumuistion luonnoksessa tärkeänä.

TSV:n mukaan turvallisuusluokittelusta ja henkilötietojen käsittelyn osalta erityisesti on tietoturvallisuusasetuksen voimassaoloaikana kertynyt kokemuksia, jotka olisi hyvä tuoda asetuksen perusteluissa esille. Vähintään perusteluissa olisi hyvä tuoda täsmällisemmin sille, miten säännösten käytännön soveltamista tullaan ohjaamaan

POHA:n mukaan ehdotetut tiukennukset TL III -asiakirjojen käsittelyn osalta eivät kaikin osin ole tarkoituksenmukaisia eivätkä huomioi niitä organisaatioita, jotka käsittelevät runsaasti asetuksen soveltamisalaan lukeutuvia tietoaineistoja. Migrin näkemyksen mukaan TL III -asiakirjojen käsittelylle asetettuja vaatimuksia on syytä arvioida vielä erityisesti toiminnallisuuden ja taloudellisuuden kannalta, huomioiden eri viranomaisten toiminnan erityispiirteet.

POHA kiinnitti lisäksi huomiota muutamiin käsitteellisiin seikkoihin. Asetusluonnoksessa puhutaan useasti "riittävästä". POHA katsoi, että semanttisen yhdenmukaisuuden vuoksi olisi tarkoituksenmukaisempaa puhua "kohtuullisesta". Tätä käsitettä käytetään tietosuojalainsäädännössä.

OM:n, VNK:n, UM:n, PLM:n ja STM:n mukaan ohjeistusta tarvitaan. STM:n mukaan esimerkiksi "riittävä"-sanaa (11 §:ssä) tulee konkretisoida – samoin ilmaisuja "mikäli on toteutettu korvaavia toimenpiteitä" (10 §:ssä) sekä "asianmukaisesti" (6 §:ssä). Myös riskiarvion perusteella toteutetut tietoturvallisuustoimenpiteet voivat eriyttää ohjeistuksia. KEHA-keskus esitti, että VM koordinoisi ja tukisi asetuksen toimeenpanoa riittävästi. EOA ja MMM totesivat, että käytetyt ilmaisut ovat osin epätasällisia. Velvoitteet määritellään väljästi; on toteutettava "riittävät", "asianmukaiset" tai "tarpeelliset" toimenpiteet. Virkavelvollisuuksien määrittelyn tarkkarajaisuuden ja siihen liittyvän laillisuusvalvonnan toteuttamisen kannalta asetusluonnos on tässä suhteessa ongelmallinen. VNK:n mukaan kokonaisuuden hahmottamiseksi olisi ollut tärkeää saada samalla arvioitavaksi Vahti 2/2010 –ohjeen korvaajaksi valmistellun Vahti 100 – ohjeistuksen luonnos. VNK:n mukaan valtionhallinnon salassa pidettävän tiedon käsittelyä koskevien muutoksien laajuutta tai kokonaisuutta ei ole tällä hetkellä helppo hahmottaa.

EK katsoi, että asetuksessa tai vähintään sen perusteluteksteissä tulisi vielä erikseen selkeyttää ja korostaa miten yritysten luokittelemaa tietoa käsitellään valtionhallinnon viranomaisessa. EK:n mukaan esimerkiksi yrityksen omia luokittelumerkintöjä ei tulisi missään tapauksessa poistaa, vaan tietoa tulisi suojata viranomaisessa aina vähintään yrityksen menettelyjä vastaavasti.

Yhdenvertaisuus- ja tasa-arvolautakunnan lausunnon mukaan sen ja tiedonhallintayksikkönä toimivan OM:n vastuunjako ei ole riittävän selkeää muun muassa lautakunnan riippumattomuuden näkökulmasta.

Kansallisarkiston mukaan pääpaino sääntelyssä on yhtä asiaa koskevissa "kirjetyyppisissä" asiakirjoissa tietojärjestelmien ja tietokantojen sijaan. Asetusluonnoksessa kuten muussakin julkisuuslainsäädännössä keskitytään melko täydellisesti nykyhetkeen, uusiin asiakirjoihin. Niissä ei juuri oteta huomioon ajan kulumisen vaikutusta säädösten soveltamiseen, mikä Kansallisarkiston näkökulmasta on toisinaan haasteellista.

KHO:n mukaan muistiossa ei ole arvioitu sääntelyn vaikutusta tuomioistuimissa perinteisesti yleiseen ja myös valtionhallinnossa alati yleistyvään etätyöskentelyyn sellaisten asioiden parissa, joihin tyyppillisesti liittyy turvallisuusluokiteltua aineistoa.

Palkeet piti tärkeänä, että asetuksella säädettäisiin myös velvoite toimintaohjeen antamisesta, jossa olisi huomioitu tarkempi ohjeistus tietojen luokittelusta, tietoverkoista, käyttöoikeuksista, suojaamisesta, käsittely- ja käyttöympäristöistä (järjestelmät, laitteet, tilat, siivoukset, huollot), tietojen lähettämisestä ja säilyttämisestä.

MMM esitti seuraavat kommentit perustelumuiotioon:

- * s.6 "Viittaus 10 §:ään tarkoittaa"-kohdassa tulisi ilmaista, että kyse on 9 §:n 2 momentin viittauksesta
- * s.8 "Pykälän 1 kohdan"-kohdassa tulisi ilmaista, että kyse on 11 § n 1 momentista
- * s.8 "Säännös ei estäisi"-kohdassa tulisi yksilöidä säännös
- * s.8 "Kohdan 3 mukaan" ja seuraavat kohtia 4–10 koskevat maininnat tulisi maininnalla vielä yhdistää 11 §:n 1 momenttiin.

Tietojohtaminen ry esitti, että ohjeistuksessa täsmennettäisiin, tarvitaanko aikaisemman yhden ns. salaisen tietojärjestelmän ("salainen diaari") lisäksi useita erillisiä salaisia tietojärjestelmiä samassa organisaatiossa. Lisäksi Tietojohtaminen ry huomauttaa, että oman tiedonhallintaympäristön esille tuominen asetusluonnoksessa ei ole riittävän selkeästi tuotu esille ja että asetusluonnoksesta puuttuu maininta siitä, miten menetellään, jos samaan asiaan liittyy eri turvallisuusluokituksen aineistoa.

VKSV piti tärkeänä, että toimeenpanoa tuetaan joko hallinnonalan tai valtionhallinnon yhteisillä resursseilla ja toimenpiteillä.

Suomen Yrittäjät ry:n mukaan, koska velvoitteita ei ole tarkoitus olennaisesti tiukentaa asetuksella, perustelumuiotiossa olisi painotettava suhteellisuusperiaatteen noudattamisen tärkeyttä myös tietoturva-vaatimusten osalta.

OM totesi lausunnossaan, että myös laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelmien tietoturvallisuuden arvioinnista (1406/2011) ja laki tietoturvallisuuden arviointilaitoksista (1405/2011) tulee siirtää VM:n vastuulle (jälkimmäisen osalta on myös LVM mahdollinen). Mainitut lait valmisteltiin ja esiteltiin aikanaan OM:n toimesta. Niiden kytkös OM:n toimialan muuhun lainsäädäntöön on kuitenkin nykyisin vähäinen.

5 Vaikutukset

SM:n mukaan 14 §:ssä ehdotetut käsittelyn kirjaamisen vaatimusten laajentaminen koskemaan myös TL III -asiakirjoja aiheuttaa merkittäviä taloudellisia ja toiminnallisia vaikutuksia yksittäisiin toimialoihin. Erityisesti tämä koskee turvallisuusviranomaisia.

Myös VKSV nosti esiin aiheutuvat taloudelliset vaikutukset.

KEHA-keskuksen mukaan on odotettavaa, että alkuvaiheessa turvallisuusluokittelu aiheuttanee lisätöitä kuten myös tiedonhallintalain soveltaminen. Saavutettavat tuottavuushyödyt tullevat tulevaisuudessa, kun soveltamisesta on saatu käytännön kokemuksia ja uusia kevyempiä toimintatapoja on otettu käyttöön.

ORK:n mukaan kustannusvaikutukset tulevat kasvamaan hallinnollisen työn lisääntyessä ja toimitilojen vaatiessa merkittäviä muutoksia. Myös tietojärjestelmien eriyttämisestä syntyy kustannuksia turvallisuusverkon ulkopuolisissa viranomaisissa.

VM:n mukaan ehdotetut muutokset saattavat aiheuttaa merkittäviä vaatimuksia valtiohallinnon yhteisiä palveluita tarjoaville palvelukeskuksille. Vaikutuksissa tulee arvioida palvelukeskuksien osuutta ja tarvetta muutoksiin sekä toimituskykyä, koska palvelukeskusten kyvykkyydellä on suoria vaikutuksia valtiohallinnon viranomaisen kykyyn täyttää asetusten uudet vaatimukset siirtymäsäännösten puitteissa. Lisäksi palvelukeskusten toiminnalle asetettujen vaatimusten merkitsemät uudet kustannukset voivat näkyä asiakashinnoittelun nousuna.

Palkeet pyysi huomioimaan, että tulevina vuosina valtion budjetissa varaudutaan myös näiden lakisääteisten velvoitteiden toteuttamiseen rahoitukseen (tilat, laitteet, tietojärjestelmät, tietoympäristö ja resurssit).

LVM huomautti, että vaikutuksia on hallinnonaloittain muun muassa asiakirjojen käsittelyyn, merkintöihin sekä tilaturvallisuudesta annettuihin ohjeisiin ja määräyksiin, jotka pitää tarkastaa, korjata tai kumota. Lisäksi uusi sääntely edellyttää koko henkilöstön kouluttamista. Koulutuskustannukset nosti esiin myös Valvira.

Valviran mukaan asetuksella on sellaisia kustannusvaikutuksia, joita vaikutusten osalta ei ole ennakoitu riittävästi. Näitä vaikutuksia ovat esimerkiksi kuntien turva-alueet ja valtionhallinnon viranomaisten tarkastukset niissä tarvittaessa.

OM:n mukaan asetusehdotuksessa on useita muutoksia verrattuna nykytilaan, jotka edellyttävät lisää hallinnollisia toimenpiteitä sekä toiminnallisia ja teknisiä ratkaisuja sekä tiloja, joilla voi olla yhteensä merkittäviäkin kustannusvaikutuksia varsinkin lyhyin siirtymäajoin, esim:

- 6 §:n mukaan valtionhallinnon viranomaisten antaessa turvallisuusluokittelun asiakirjan muulle kuin valtionhallinnon viranomaiselle tulisi ennakolta varmistaa, että suojaamisesta huolehditaan asianmukaisesti. Erityisesti suhteessa kuntaviranomaisiin tämä edellyttää valtionhallinnon viranomaisilta paljon rinnakkaisia hallinnollisia varmistamistoimenpiteitä jokaisen kunnan ja myös toimialan osalta erikseen, kuten turvallisuussopimuksia, selvityksiä, arvioiteja, lupia tai sopimusjärjestelyjä, jotta turvallisuusluokiteltujen asiakirjojen käsittely olisi mahdollista ja suojaamisen järjestelyt varmistettu. Epäselväksi tosin säännöksen perusteella jää, millä tavalla ennakolta varmistumisen on tarkoitettu tapahtuvan. Julkisuuslain 13.2 §:n mukaan pyydetessä saada tieto salassa pidettävästä asiakirjasta taikka viranomaisen henkilörekisteristä tai muusta asiakirjasta, josta tieto voidaan luovuttaa vain tietyin edellytyksin, tiedon pyytäjän on, jollei erikseen toisin säädetä, ilmoitettava tietojen käyttötarkoitus sekä muut tietojen luovuttamisen edellytysten selvittämiseksi tarpeelliset seikat sekä tarvittaessa tiedot siitä, miten tietojen suojaus on tarkoitus järjestää. Ehdotetun säännöksen suhdetta mainittuun julkisuuslain säännöksen ei muistiossa ole arvioitu.
- 8 §:ssä ehdotetaan käsittelyoikeuksien luettelointia laajennettavaksi myös turvallisuusluokkaan III. Kansainvälisistä tietoturvelvoitteista johdettu

laajennus lisää luetteloiden laatimiseen ja ylläpitämiseen liittyvää hallinnollista työtä. Henkilöihin sidottujen työtehtävien luetteloiden sijaan voisi käytännön näkökulmasta olla luontevampaa ylläpitää toiminto-, ryhmä- tai roolikohtaisia oikeuksia asiakirjoihin, sillä usein tietojärjestelmissä oikeudet ylläpidetään käyttöoikeusroolien tai -ryhmien avulla, joihin henkilön käyttäjätunnus liitetään työtehtävien perusteella.

- Säännökset turvallisuusalueista saattavat aiheuttaa merkittäviäkin kustannuksia ja uudelleen sopimisen tarvetta Senaatin kanssa. Ehdotettu kolmen vuoden siirtymäaika vaikuttaa käytännössä liian lyhyeltä, sillä myös tietoturvallisuusasetuksen viiden vuoden siirtymäaika osoittautui käytännössä haastavaksi toimitilojen pitkien elinkaarien vuoksi. Tilamuutosten toteuttaminen olisi järkevintä uusien toimitilojen rakentamisen tai vanhojen tilojen korjaustarpeiden yhteydessä. Lisäksi tilaturvallisuuden osalta kustannuksia, sekä myös viranomaisten välisiä tulkintaeroja, saattaa syntyä viranomaisen toimitilojen ulkopuolella toimimisen osalta, kuten onko turvallisuusluokka IV asiakirjojen käsittely sallittua jatkossa etätyössä, liikkuvassa työssä tai sellaisilla tietojärjestelmillä, jotka sijaitsevatkin 11 § 1 momentin 1 kohdan tarkoittamassa matalamman turvallisuustason tietojärjestelmissä tai tietoliikennejärjestelyissä tai viranomaisverkkojen ulkopuolella. Voimassa olevassa tietoturvallisuusasetuksessa on erillinen 15 §:n säännös ”*ellei viranomaisen luvasta, toimeksiannosta tai antamista ohjeista muuta johdu*”.
- Lisäksi saattaa syntyä merkittäviäkin kustannuksia erityisesti TL IV-asiakirjojen osalta ehdotetun 11 §:n 1 ja 10 kohtien vaatimuksiin sekä turvallisuusverkkoon (TUVE) kuulumattomille toimijoille TL III-asiakirjojen osalta 11 §:n 2 momentin vaatimuksiin liittyen, sillä vaatimukset saattavat johtaa nykyisten sähköisten työvälineiden työasemien, mobiililaitteiden ja tietojärjestelmien sijaan paperiprosessien käyttämiseen tai merkittäviin työasemien, mobiililaitteiden, tietojärjestelmien ja tietoliikennejärjestelyjen kehittämis- ja eriyttämiskustannuksiin, ja myös TEMPEST-suojauksien rakentamiseen sekä rajattuihin tietojärjestelmiin että rajattuihin viranomaisen toimitiloihin kohdistuu merkittäviä tilaturvallisuuden kehittämistarpeita.

6 Lausuntopalautteen vaikutus

Kaikki saatu lausuntopalaute on valtiovarainministeriössä eritelty ja koottu jatkovalmistelua varten. Tässä lausuntoyhteenvedossa ei ole käsitelty lausuntojen aiheuttamia muutoksia ehdotukseen valtioneuvoston asetukseksi. Lausuntojen aiheuttamat muutokset ovat keskeisiltä osin kirjattu perustelumuistioon.

Jakelu Lausuntokooste julkaistaan valtioneuvoston hanketietosivulla