OIKEUSREKISTERIKESKUS
RÄTTSREGISTERCENTRALEN

Lausunto

01.10.2018 236/00/2018

Asia: VM183:00/2017 ja VM/1631/03.01.00/2018

Luonnos hallituksen esitykseksi eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

-

2. Arvionne lukuun 2 Nykytila

Oikeusrekisterikeskus on esityksen kanssa yhtä mieltä siitä, että tiedonhallintaa koskeva sääntely on nykytilassa hajanaista ja vaatii käsitteellistä yhtenäistämistä.

3. Arvionne lukuun 3 Esityksen tavoitteet ja keskeiset ehdotukset

Oikeusrekisterikeskus pitää esityksen tavoitetta tiedonhallintaan kohdistuvan sääntelyn yhtenäistämisestä yhden yleislain alle hyvänä. Perusajatus tiedon elinkaaren hallinnasta käsitteellisesti yhtenäisellä sääntelyllä, jossa tietoon sen käsittelyn eri vaiheissa kohdistuvat velvollisuudet ja vastuut ovat selkeästi kuvattu, on kannatettava. Samoin tavoitteet tiedon entistä tehokkaammasta hyödynnettävyydestä ja yhteentoimivuudesta ovat kannatettavia.

5. Kommentit ja huomiot lakiehdotuksen lukuun 1 yleiset säännökset (pykälät 1-4 ja niiden yksityiskohtaiset perustelut)

Oikeusrekisterikeskus kiinnittää huomiota luonnoksen soveltamisalan ja määritelmien yhteensovittamiseen. Luonnoksen 3 §:n 1 momentin mukaan lakia sovellettaisiin tiedonhallintayksikköjen ja niissä toimivien viranomaisten tiedonhallintaan niiden käsitellessä tietoaineistoja, ellei muualla laissa ole toisin säädetty. Luonnoksen 2 §:n 1 momentin 1 ja 2 kohdissa on määritelty viranomainen ja tiedonhallintayksikkö. Ensin mainitussa viitataan julkisuuslain 4 §:ssä säädettyyn viranomaisen määritelmään. Tiedonhallintayksikön määritelmäksi ehdotetaan luetteloa, josta on jätetty pois muun muassa julkisuuslain 4 §:n 3 momentissa säädetyt julkista tehtävää hoitavat yhteisöt, laitokset ja säätiöt. Oikeusrekisterikeskus kehottaa tarkistamaan, onko tiedonhallintayksikön määritelmästä tarkoituksenmukaista jättää pois julkisuuslain 4 §:ssä mainittuja toimijoita.

3 § 3 momentin Ahvenanmaata käsittelevässä viimeisessä virkkeessä on kirjoitusvirhe ja virkkeen sisältö jää epäselväksi.

6. Kommentit ja huomiot lakiehdotuksen lukuun 2 Julkisen hallinnon tiedonhallinnan yleinen ohjaus (pykälät 5-9 ja niiden yksityiskohtaiset perustelut)

Oikeusrekisterikeskuksen näkemyksen mukaan tietoturvallisuuden yleisen ohjauksen voisi lisätä osaksi julkisen hallinnon tiedonhallinnan yleistä ohjausta tai yhteentoimivuuden ohjauksessa yhdeksi varmistavaksi tekijäksi, koska HE luonnoksesta tämä jää epäselväksi.

Tiedonhallintalautakunnan ja mahdollisten neuvottelukuntien, asiantuntijajaoksien, valtiovarainministeriön asettamien toimielimien, valtiovarainministeriön JulkICT-osaston ja Väestörekisterikeskukselle siirtyneiden tehtävien väliset roolit ja vastuut jäävät HE luonnoksessa epäselviksi. Olisi hyvä perustella lisää uusien toimijoiden tarvetta, etenkin jos muita toimijoita ei lakkauteta. Kysymyksinä vastuista esim. minkä toimijan vastuulla olisi nykyisiä vastaavien JHS- ja VAHTI-ohjeiden tekeminen, miten vältetään toimijoiden mahdollisesti samaan aihealueeseen antamien ohjeistuksien ristiriitaisuudet tai minkä tasoisia ohjeita eri toimijat voivat antaa (esim. ohjeiden velvoittavuuden, ohjaavuuden ja toimialakohtaisuuden näkökulmista)? Näitä rooleja ja vastuita voisi HE luonnokseen tarkentaa ja tarvittaessa tarkentaa myös Väestörekisterikeskuksen tehtäviä, jotta päällekkäisyydet vältetään.

Lisäksi tiedonhallinnan menettelytapojen ja vaatimusten mukaisuuden toteuttamisessa on nyt tunnistettavissa katve erityisesti turvallisuusluokiteltavien tietojen hallintaan ja tietoturvallisuuteen liittyen. Suositeltavaa olisi nopeasti täydentää tiedonhallintalakiluonnosta asetusluonnoksella, ettei synny merkittävää riskiä kansalliselle turvallisuudelle ja yhteiskunnalle, etenkin mikäli myös turvallisuusluokitellun tiedon osalta riskiperusteisuus edelleen lisääntyy ja turvallisuusluokituksen piiri laajenee.

7 §: 2 momentti tiedonhallintalautakunnan kokoonpano. Oikeusrekisterikeskus huomauttaa, että luonnoksen mukaisessa tiedonhallintalautakunnan kokoonpanossa vaille edustusta jäävät asiakirjahallinnon ja rekisteritiedon (metatiedon) asiantuntijat. 3 momentissa tekstissä tulisi mitä ilmeisimmin viitata molemmissa 2 momenttiin, ei 3.

7. Kommentit ja huomiot lakiehdotuksen lukuun 3 Tiedonhallinnan suunnittelu ja kuvaaminen (pykälät 10-12 ja niiden yksityiskohtaiset perustelut)

Mikäli tiedonhallintayksiköiden tiedonhallinnan kuvauksien laajuus ja tarkkuustaso vaihtelevat, ei se välttämättä varmista eikä edistä tavoiteltua yhteentoimivuutta. Lisäksi tulisi vielä riskiarvioida mitä julkiseen tietoverkkoon tiedonhallinnankuvauksista asetetaan saataville ja minkä tasoisia julkiset versiot tulisivat olemaan, ettei julkistenkin tietojen yhdistämisellä samalla vaarannu tiedonhallintoyksikköjen kriittiset toiminnot tai yhteistoiminta esim. tietoturvallisuusjärjestelyiden ja riippuvuuksien tahattomalla paljastamisella.

Luonnoksen 10 §:n Tiedonhallintamalli perusteluissa todetaan, että tiedonhallintayksiköllä tulee olla selkeä kuvaus toimintaympäristön tiedonhallinnasta, jolla palvellaan tietojärjestelmien yhteentoimivuutta, tietovarantojen käsittelyn avoimuutta ja julkisuutta sekä tietoaineistojen säilyttämisen ja arkistoinnin ennakollista suunnittelua. Saman kuvauksen alle yhdistettäisiin kuvaukset niin tiedonhallintayksikön toimintaprosesseista, tietovarannoista, tietoaineistojen arkistoinnista ja tuhoamisesta, tietojärjestelmistä sekä tietoturvajärjestelyistä. Oikeusrekisterikeskus huomauttaa, että yhdistettävien kuvausten nykyiset käyttötarkoitukset ja kuvaustarkkuudet vaihtelevat merkittävästi, mikä voi aiheuttaa haasteita tiedonhallintamallia kuvattaessa. Esimerkiksi perusteluissa mainittu kokonaisarkkitehtuurimenetelmä ei välttämättä sovellu arkistonmuodostus- tai tiedonohjaussuunnitelman sisältämien tietojen kuvaamiseen. Koska laissa ei säädettäisi niistä menetelmistä, joilla kuvaukset laadittaisiin, vaan se jäisi tiedonhallintayksikön harkintaan, voi tiedonhallintamallin kuvauksen laadinta vaatia tiedonhallintayksikössä yllättävän paljon pohdintaa ja lisätyötä ja kuvaukset voivat poiketa merkittävästi eri tiedonhallintayksiköiden välillä.

Oikeusrekisterikeskus pitää tiedonhallinnan muutossuunnitelman laadintaa kannatettavana. Muutossuunnitelman roolia tulisi joltain osin vielä selkeyttää, ks. 34 §:ää koskeva kommentti.

8. Kommentit ja huomiot lakiehdotuksen lukuun 4 Tietoturvallisuus (pykälät 13-18 ja niiden yksityiskohtaiset perustelut)

HE luonnos korostaa riskilähtöisyyttä, mikä on hallittuna kannatettavaa. Toimintaympäristön, teknologioiden ja sääntelyn muuttuessa tiheämmin sekä riskiperusteisuuden kasvaessa on kuitenkin tunnistettavissa näistä ja riskinottohalukkuudesta johtuen tilanne, jossa on riskiä siitä, että tietoturvallisuuden taso voi jatkossakin merkittävästi vaihdella julkisessa hallinnossa, julkisen hallinnon palveluissa ja tietojärjestelmissä. Tästä riskistä johtuen, HE luonnosta tulisi kehittää siten, että tiedonhallintayksiköille olisi selkeät, yhtenäiset ja yksilöidyt tietoturvallisuuden vähimmäisvaatimukset. Tarvittaessa tulisi harkita, voisiko säätää vastaavasti kuin turvallisuusluokiteltujen tietoturvavaatimusten osalta, että myös yleisiin tietoturvallisuuden vähimmäisvaatimuksiin voisi valtiovarainministeriön esittelystä säätää tarkemmin valtioneuvoston asetuksella.

Oikeusrekisterikeskus esittää, että velvoittavia tiedonhallintayksikön tietoturvallisuuden vähimmäisvaatimuksia voisivat olla esimerkiksi seuraavat kolmetoista (13) osakokonaisuutta:

- Tietoturvallisuuden suunnittelusta, vastuista ja riittävistä resursseista huolehtiminen (tiedonhallintayksikön toiminnan ja tietoturvallisuuden varmistamiseksi)
- Tietoturvallisuuden tilannekuvan kokoaminen, seuranta ja hyödyntäminen johtamisessa
- Tietoturvallisuuden arviointi koko tietojen käsittelyn elinkaari ja tiedonhallinnan muutokset huomioiden
- Tietojen ja tietojärjestelmien kriittisyys- ja tärkeysluokittelu sekä kriittisien riippuvuuksien tunnistaminen (tietoturvatoimenpiteiden parempi kohdentaminen, lisävaatimusten riskiarviointi kriittisille, yhteentoimivuuden varmistaminen)
- Kaikkien tietojen saatavuuden ja eheyden merkityksen arviointi

- Salassa pidettävien tietojen (ml. henkilötiedot, turvallisuusluokitellut, muut salassa pidettävät) luottamuksellisuuden sekä saatavuuden ja eheyden merkityksen arviointi

- Salassa pidettävien tietojen (ml. henkilötietojen, turvallisuusluokitellut, muut salassa pidettävät) rajaaminen vain niille, joilla niihin on oikeus ja työperusteinen tarve

- Henkilöstön ja palvelutuottajien luotettavuuden selvittäminen tarvittaessa

- Tietojen käsittelyyn ja tietovarantoihin käytettävien tilojen riittävästä turvallisuudesta huolehtiminen

- Tietojärjestelmien ja tietoliikennejärjestelyjen riittävästä tietoturvallisuudesta huolehtiminen (ml. käyttöoikeudet ja vähimmäisien oikeuksien periaate)

- Tietoturvallisuuden häiriö- ja poikkeamatilanteisiin varautuminen, tarvittaessa jatkuvuuden hallinta ja harjoittelu

- Tietojen käsittelyn, tietojärjestelmien ja tietoliikenteen toteuttaminen siten, että niiden tietoturvatilanteet, merkittävät häiriöt ja tietoturvapoikkeamat pystytään riittävästi havaitsemaan ja jäljittämään (ml. lokitusvelvoite, tilannekuva, ja näiden seuranta)

- Ilmoitusvelvollisuus tietoturvallisuuteen liittyvistä poikkeamista viipymättä valtiovarainministeriölle tai sen osoittamalle viranomaiselle (kyberturvallisuusstrategia, tilannekuva, vrt. asetus Valtorista)

Lisäksi HE luonnosta voisi täydentää velvoittamalla tiedonhallintayksiköt suunnittelemaan tietoturvallisuuden vähimmäisvaatimusten lisäksi oman toimialan, toiminnan sekä tietojen käsittely- ja tietojärjestelmäympäristöjen niin edellyttäessä muut tietoturvallisuuden erityisvaatimukset ja erityiset tietoturvatoimenpiteet riskiarvioinnin perusteella sekä seuraamaan ja arvioimaan näidenkin tilaa.

Tietoturvallisuuden vähimmäisvaatimuksien ja lisäksi yleisimpiin tietoturvallisuuden erityisvaatimuksien (esim. henkilötietojen, turvallisuusluokiteltujen tietojen) osalta soveltuvat tietoturvatoimenpiteet, kontrollit sekä näiden käytännön toteutukseen soveltamisohjeita ja toteutusvaihtoehtoja voitaisiin kuvata VAHTI-ohjeina tai muina suosituksina.

13 § - Henkilöiden ja palveluntuottajien luotettavuuden varmistaminen ei ole helppoa ja se edellyttää prosesseja, arvioita, sopimuksia ja sitoumuksia.

Henkilöiden osalta henkilöturvallisuusselvitykset tulisi kuitenkin tehdä vain tarvittaessa Turvallisuusselvityslain (724/2014) mukaisesti. HE luonnokseen voisi lisätä, että henkilöturvallisuusselvityksiä tehdään vain tarvittaessa ja osana laajempaa henkilöstöturvallisuuden prosessia. Lisäksi Turvallisuusselvityslakia olisi tarkennettava ja poistettava kytkentä suojaustasoihin henkilöturvallisuusselvityksen laajuuden määrittämisessä (tähän oli viitteitä perusteluissa) sekä

säilytettävä mahdollisuus henkilöturvallisuusselvityksiin myös muissakin kuin turvallisuusluokiteltujen tietojen ja niitä sisältävien tietojärjestelmien ja tilojen turvaamisessa.

Palveluntuottajien luotettavuuden varmistaminen muilta kuin henkilöstön luotettavuuden osalta jää HE luonnoksessa katvealueeksi. Tähän voisi lisätä, että palveluntuottajien luotettavuuden varmistamiseksi voi tarvittaessa laatia sopimukset ml. sanktiot, turvallisuussopimus, salassapito- sekä salassa pidettävien tietojen ja henkilötietojen käsittelyn velvoitteet.

14 § Tietoaineistojen ja tietojärjestelmien turvallisuus

Tämä HE luonnos ja pykälä 14 lähtevät tietoaineistoista ja tietojärjestelmistä. Tietoturvallisuus perustuu kuitenkin johtamiseen ja riskienhallintaan sekä tietoturvallisuustoimenpiteiden ennakolta suunnitteluun. Tämän voisi tuoda tietoturvallisuusosuuden yhteydessä sekä tiedonhallinnan muutostilanteissa esille.

HE luonnoksesta puuttuvat selkeästi tiedonhallintayksikköjä velvoittavat, yhtenäiset ja yksilöidyt tietoturvallisuuden vähimmäisvaatimukset, vaikka niihin perustelumuistiossa viitataan. Tietoturvallisuuteen liittyviä asioita on luonnoksessa pirstaleisina useissa eri luvuissa ja pykälissä, mikä voi lisätä virheellisiä tulkintoja. HE luonnosta voisi täydentää asettamalla selkeästi tiedonhallintayksiköille velvoittavat ja yhtenäiset tietoturvallisuuden vähimmäisvaatimukset. Tämä lisäisi tiedonhallintayksiköiden ja näiden toiminnan ja tietojen käsittelyn tietoturvallisuutta, toimijoiden välistä luottamusta sekä yhteentoimivuutta.

Pykälissä 14 ja 16 olevia asioita olisi varmaankin yhteensovitettavissa, mutta osa kohdistuu viranomaiseen ja osa tiedonhallintayksikköön. Turvallisuuteen ja tietoturvallisuuteen sisältyy kuitenkin pykälässä 16 yksilöidyt asiat, jotka ovat pääasiassa joko tiedon eheyteen tai tiedon saatavuuteen liittyviä, mutta ei tietojärjestelmiin liittyviä selkeästi. Oikeusrekisterikeskus katsoo, että nämä asiat voitaisiin yhdistää ja nämä voisivat olla osana yleisiä tietoturvallisuuden vähimmäisvaatimuksia.

15 § Tietojen siirtäminen verkossa

HE luonnoksesta pykälän 15 kohdalla on riskinä mahdollinen tulkinta tai virhetulkinta, että tiedot voitaisiin todella luovuttaa ennen vastaanottajan tunnistamista. Tämä on merkittävä riski. Toimintatapa soveltuisi hyvin vain hyvin rajattuihin käyttötapauksiin ja rajattuihin tietoihin. On myös huomioitava se, että salauksen riittävyys on arvioitava suhteessa aikaan ja käytännössä kaikki salaukset ovat murrettavissa tietyssä ajassa tietyllä laskentateholla (joka on riippuvaista

teknologisesta kehityksestä). Oikeusrekisterikeskus esittää, ettei lähtökohtaisesti luovuteta tietoja ennen kuin vastaanottaja on tunnistettu ja lisäksi vastaanottajan oikeus tietoihin on varmistettu.

Oikeusrekisterikeskus kiinnittää huomiota myös velvoittavaan salaukseen tai muuhun suojauksen. Mikäli pykälässä 15 tarkoitetaan kaikkia tietoverkkoja eli myös perinteisesti turvallisempina katsottuja nk. viranomaisverkkoja ja sisäverkkoja, niin luonnosta tulisi harkita tarkennettavan ja tätä kohtaa rajattavan. Ilman tarkennusta ja rajausta salauksen laajentaminen kaikkiin tietoverkkoihin aiheuttaisi merkittäviä tietojärjestelmä- ja tietoliikennekustannuksia verrattuna nykytilaan vrt. olisi merkittävästi tietoturvallisuusasetusta tiukempi. Oikeusrekisterikeskus esittää, että näiltä osin tämä kohta tarkennetaan ja sisällytetään osaksi yleisempänä tietoturvallisuuden vähimmäisvaatimuksiin tietoverkkojen turvaamisena. Eri tietoverkkoihin ja eri käyttötapauksia liittyen voisi salauksien riittävyyttä ja muita suojatoimenpiteitä ennemmin kuvata VAHTI-ohjeissa tai muina suosituksissa.

16 § vrt. pykälän 14 kommentit.

17 § Tietojärjestelmien käyttöoikeuksien hallinta

HE luonnos ei suoraan edellytä vähimpien oikeuksien periaatetta vaan tehtäviin liittyviä käyttötarpeita. Vähintäänkin tiettyjen käyttöoikeuksien ja tiettyjen tietojen osalta olisi syytä aina noudattaa vähimpien oikeuksien periaatetta. Oikeusrekisterikeskus kiinnittää huomiota siihen, että vaaralliset työyhdistelmät tulisi aina huomioida ennen käyttöoikeuksien myöntämistä. Lisäksi Oikeusrekisterikeskus kiinnittää huomiota käyttöoikeuksien hallinnan hankaluuteen tietojärjestelmien elinkaaressa. Mikäli käyttöoikeuksia ei tarkisteta tai aseteta määräaikaisina, kasvavat jatkuvasti tähän toimintatapaan ja sen yleisyyteen liittyvät riskit sekä todennäköisyydet tietoturvapoikkeamista ja henkilötietojen tietoturvaloukkauksista.

18 § Lokitietojen kerääminen

Oikeusrekisterikeskus kiinnittää huomiota siihen, että HE luonnos rajaa osin lokitietojen käsittelyä vain keruu vaiheeseen. Samoin on rajattu vain tietojärjestelmiin, vaikka perusteita on paperilla olevien tietojen ja rekisterien lokitietojen keräämiselle.

Lokitietojen käyttötarkoituksia voisi lisätä: tulisi olla tarvittaessa jäljitettävissä kuka muutti julkista tietoa tai kuka teki palvelunestohyökkäyksen tai tietosuojan toteuttaminen ja valvominen.

Termiä tietojärjestelmien käyttö voisi avata vähintäänkin perusteluihin, kattaisiko se tietojärjestelmään kohdistuneet kirjautumistiedot, tiedot tiedon muuttajasta, tiedot

tietoturvallisuuden kannalta merkittävistä tapahtumista sekä lisäksi lokitietoihin kirjattavien asioiden/toimenpiteiden onnistumisesta tai epäonnistumisesta (jotta saadaan yhtä lailla virhetilanteet kuin palvelunestohyökkäyksen tai identiteettivarkauden selvittämiseksi tarvittavat lokitiedot ja todisteet jne).

9. Kommentit ja huomiot lakiehdotuksen lukuun 5 Turvallisuusluokittelu (pykälät 19-22 ja niiden yksityiskohtaiset perustelut)

Oikeusrekisterikeskus pitää hyvänä turvallisuusluokitusperusteiden laajentamista, vaikka se aiheuttaakin selvitystyötä. Oikeusrekisterikeskus kiinnittää huomiota kuitenkin siihen, ettei samalla ole lausunnoilla arvioitavana asetusluonnosta ja näin ollen vaikutusarvioinnitkin ovat puutteellisia ja voivat kohdistua tietoturvallisuusvaatimusten osalta vain turvallisuusluokkaan IV.

21 § Turvallisuusluokiteltujen asiakirjojen tietoturvallisuusvaatimukset

Oikeusrekisterikeskus pitää hyvänä, että pykälä 21 selkeästi kokoaa turvallisuusluokiteltujen asiakirjojen tietoturvallisuusvaatimukset, joita on mahdollisuus asetuksella myös tarkentaa.

Oikeusrekisterikeskus kiinnittää huomiota kuitenkin siihen, että HE luonnoksen mukaan yleisen tietoturvallisuuden vähimmäisvaatimukset riittäisivät myös turvallisuusluokka IV käsittelyyn ja tietoturvallisuuden varmistamiseen. Mikäli kaikki yleiset tietoturvallisuuden vähimmäisvaatimuksetkin ovat riskiperusteisia tai mikäli osaa tietoturvallisuuden vähimmäisvaatimuksista ei erikseen velvoiteta pakolliseksi turvallisuusluokka IV käsittelemiseksi, voi tästä aiheutua merkittävä riski kansalliselle turvallisuudelle.

10. Kommentit ja huomiot lakiehdotuksen lukuun 6 Asian ja palvelujen tiedonhallinta (pykälät 23-26 ja niiden yksityiskohtaiset perustelut)

23 §:ssä määritellään asian yksilöintitunnuksen sisältö. Oikeusrekisterikeskus huomauttaa, että uuden asiatunnuksen käyttöönotosta syntyy kustannuksia, kun esimerkiksi nykyisiä tietojärjestelmiä tulee kehittää tämän mukaisesti.

24 §:ssä säädetään asian pakollisista rekisteröintitiedoista. Oikeusrekisterikeskus huomauttaa, onko asiakirjan saapumistapa sellainen tieto, että se tulee määritellä lain tasolla pakolliseksi. Asiakirjan saapumistavasta huolimatta viranomaisen on kirjattava ja käsiteltävä asia yhtenäisellä toimintaprosessilla. Pykälän perusteluissa todetaan, että tiedonhallintayksikkö voi täydentää laissa määriteltyjen tietojen lisäksi rekisteröintitietojaan, jos katsoo sen tarpeelliseksi.

Luonnoksen 25 §:n 1 momentissa ehdotetaan tiedonhallintayksikön ylläpidettäväksi kuvausta siitä, missä tietojärjestelmissä sillä on asiarekisteriin kuuluvia tietoja. Pykälän 3 momentin mukaan tiedonhallintayksikön on julkaistava kuvaus asiarekisteristä yleisessä tietoverkossa siltä osin kuin tiedot eivät ole salassa pidettäviä. Luonnoksen 24 §:n yksityiskohtaisissa perusteluissa todetaan, että asiarekisterillä tarkoitetaan viranomaisten diaareja, asiakirjarekistereitä ja muita vastaavia hakemistoja. Oikeuskäytännössä on katsottu, että viranomaisen diaari muodostaa henkilörekisterin (KHO 2008:34). Tämän vuoksi useat viranomaiset ylläpitävät diaaristaan tälläkin hetkellä joko henkilötietolain 10 §:n mukaista rekisteriselostetta tai EU:n yleisen tietosuoja-asetuksen 13 ja 14 artikloista johdettavaa rekisteröityjen informointiasiakirjaa, jotka ovat useissa tapauksissa saatavilla viranomaisten www-sivuilla. Oikeusrekisterikeskuksen näkemyksen mukaan erillisen asiarekisterin kuvaus lisää hallinnollista työtä turhaan. Oikeusrekisterikeskus ehdottaa, että 25 §:n yksityiskohtaisiin perusteluihin lisätään maininta siitä, että tiedonhallintalaissa ehdotettu asiarekisterin kuvaus voitaisiin yhdistää osaksi yleisessä tietosuoja-asetuksessa tarkoitettua rekisteröidyn informointia, jolla täytettäisiin sekä ehdotetun tiedonhallintalain että yleisen tietosuoja-asetuksen vaatimukset (ks. vastaava esimerkki yhdistämisestä HE 31/2018 vp, s. 48).

11. Kommentit ja huomiot lakiehdotuksen lukuun 7 Tietoaineistojen muodostaminen ja sähköinen luovutustapa (pykälät 27-31 ja niiden yksityiskohtaiset perustelut)

Esityksen 27 § mukainen asiakirjojen ensisijainen sähköinen säilytysmuoto on kannatettava. Kuitenkaan kaikilla viranomaisilla ei tällä hetkellä ole käytössään kokonaan digitaalisen asia- ja asiakirjahallinnan edellyttämiä tietojärjestelmiä, minkä vuoksi vuoden siirtymäaika on liian lyhyt. Kokonaan digitaalinen asiankäsittely edellyttää siihen soveltuvien asianhallintajärjestelmien käyttöönottoa, jotta käsittely voidaan toteuttaa luotettavasti esimerkiksi tietoturvan ja tietojen säilymisen näkökulmasta. Oikeushallinnossa on käynnissä lukuisia toiminnan kehittämisen hankkeita, joiden myötä oikeushallinnossa siirrytään laajalti kokonaan digitaaliseen asiankäsittelyyn ja arkistointiin. Kehittäminen vaatii kuitenkin vielä useamman vuoden kehitystyön.

29 § ja perustelut: Ensimmäisessä momentissa kuvattua vakiosisältöistä tietojen luovuttamista teknisten rajapintojen avulla ei aina ole tarkoituksenmukaista toteuttaa, vaikka luovutus olisi säännöllisesti toistuvaa ja vakiosisältöistä. Esimerkiksi tietojen luovuttaminen korkeamman suojaustason tietoja sisältävästä tietojärjestelmästä alemman suojaustason tietoja sisältävään tietojärjestelmään, saattaa aiheuttaa panos/tuotto suhteessa arvioituna suuria vaikutuksia tietoja vastaanottavaan järjestelmään. Pykälään tulisi saada Oikeusrekisterikeskuksen näkemyksen mukaan joustoa niin, että viranomainen voisi perustellusti poiketa kuvatusta velvollisuudesta. Oikeusrekisterikeskus pitää tärkeänä, että toisen momentin mukainen tietoaineistojen luovuttaminen tiedostopohjaisesti mahdollistetaan perusteluissa mainituista tarkoituksenmukaisuussyistä, esimerkiksi toisen viranomaisen tietovarannon ajantasaistamiseksi.

31 § ja perustelut: Pykäläehdotuksen mukaan tiedot luovuttavan viranomaisen olisi varmistettava, että näiden luovutettavien tietojen tietoturvallinen

käsittely on varmistettu tiedon saavan toimijan toiminnassa vastaavilla tietoturvatoimenpiteillä kuin tässä laissa säädetään tiedonhallintayksikölle. Oikeusrekisterikeskus pitää tietojen tietoturvallisen käsittelyn varmistamisen lähtökohtaa perusteltuna ja tällä hetkellä tietoturvakysymyksiä pyritään selvittämään erillisessä tietolupamenettelyssä ennen teknisten käyttöyhteyksien avaamista.

Huomattava on, että julkishallinnon ulkopuolella toimivaan tietojen vastaanottajaan ja sen suorittamaan tietojen käsittelyyn ei kohdistu välttämättä samanlaisia tietoturvavaatimuksia kuin viranomaiseen. Näin ollen tietojen turvallisen käsittelyn varmistaminen voi olla yhteisten standardien puuttuessa mahdotonta. Pykäläehdotukseen liittyen ja yhteneväisten käytäntöjen varmistamiseksi, olisi välttämätöntä saada viranomaisten käyttöön yhteneväiset standardit tai vähintään ohjeistus, miten julkishallinnon ulkopuolella toimivan tietojen vastaanottajan tietojärjestelmiä ja tietojen käsittelyä tullaan arvioimaan.

12. Kommentit ja huomiot lakiehdotuksen lukuun 8 Tietoaineistojen säilyttäminen ja arkistointi (pykälät 32-38 ja niiden yksityiskohtaiset perustelut)

Oikeusrekisterikeskus pitää kannatettavana henkilötietojen käsittelyä sekä asiakirjatietojen säilyttämistä koskevien periaatteiden, käsitteiden sekä käyttötarkoitusten selkeää erottelua toisistaan.

Luonnoksen 32 §:n 2 momentin mukaan arkaluonteisten tietojen säilytysajoista säädetään erikseen. Pykälän yksityiskohtaisten perustelujen mukaan arkaluonteisilla henkilötiedoilla tarkoitetaan erityisiin henkilötietoryhmiin kuuluvia henkilötietoja, rikostuomioita ja rikkomuksia koskevia tietoja ja sosiaalihuollon asiakastietoja. Henkilötietojen suojaa koskeviksi yleislaeiksi ehdotetaan tietosuojalakia (HE 9/2018 vp) ja rikosasioiden tietosuojalakia (HE 31/2018 vp). Edellä mainituissa lakiehdotuksissa ei enää käytetä arkaluonteisten henkilötietojen käsitettä, josta vielä toistaiseksi säädetään kumottavaksi ehdotetun henkilötietolain 11 §:ssä. Oikeusrekisterikeskus huomauttaa, että arkaluonteisten henkilötietojen käsitteestä on tarkoitus luopua.

Esityksen tavoitteissa mainitaan Kansallisarkiston roolin vahvistaminen kulttuuriperintöön liittyviin tietoaineistoihin ja arkistointiin liittyvien prosessien kehittäjänä ja ohjaajana. Esityksen perusteella jää kuitenkin epäselväksi, mitkä ovat ne käytännön keinot, joilla tätä roolia vahvistetaan tai kenelle kuuluu jatkossa vastuu sähköiseen asiakirjahallintaan liittyvien toimintatapojen ohjaamisessa ja mitkä ovat ohjauskeinot. Oikeusrekisterikeskus pitää tärkeänä, että näihin tehtäviin varataan jatkossakin riittävän selvät roolit, vastuut ja resurssit.

Luonnoksen 34 §:n 1 momentin mukaan tiedonhallintayksikön on toimitettava Kansallisarkistolle tiedonhallinnan muutossuunnitelmaan sisältyvät tietoaineiston arkistointia ja tuhoamista koskevat tiedot lausunnon antamista varten, jos suunnitelluilla muutoksilla on vaikutusta tietoaineistojen arkistointiin tai tuhoamiseen. Luonnoksen 11 §:n 1 momentin mukaan tiedonhallintayksikön on laadittava tiedonhallinnan muutossuunnitelma, kun se uudistaa olennaisesti hallintoaan, palvelujaan tai tietojärjestelmiään. Kirjaus antaisi ymmärtää, että kaikkia asiakirjojen säilytysaikoihin liittyviä muutoksia ei kuvattaisi muutossuunnitelmaan olennaisina hallinnon, palvelujen tai tietojärjestelmien muutoksina. Oikeusrekisterikeskus kehottaa kiinnittämään huomiota tähän ristiriitaan jatkovalmistelun aikana. Mahdollisesti tiedonhallinnan muutossuunnitelman roolia tulee vielä täsmentää.

Luonnoksen 36 §:n 3 momentin mukaan arkistoa ylläpitävä tiedonhallintayksikkö määrittää tietorakenteet ja tiedostomuodot, joissa asiakirjatiedot siirretään sähköiseen arkistoon. Niin ikään useat eri viranomaiset voisivat jatkossa toimia arkistoa ylläpitävinä tiedonhallintayksiköinä. Oikeusrekisterikeskuksen näkemyksen mukaan jatkossakin tulisi olla julkiselle hallinnolle yhtenäiset vaatimukset ja rakenteet sähköisten asiakirjatiedon hallinnalle, jotka ohjaavat yhteentoimivuutta ja toimintatapoja. Sähköisen asiakirjahallinnan vaatimukset tulee ulottaa ohjaamaan asiakirjatiedon koko elinkaaren käsittelyä aina asiakirjatiedon syntyvaiheesta tietojen hävittämiseen ja arkistointiin. Samoin vaatimukset tulee voida huomioida myös uusia tiedonhallintajärjestelmiä suunniteltaessa ja hankittaessa. Ilman selkeitä vaatimuksia ja ohjausta on vaarana, että sähköisten asiakirjatietojen käsittelyn toimintatavat mukaan lukien arkistointi hajaantuvat ja yhtenäisiä toimintatapoja ei saavuteta julkisessa hallinnossa. Niin ikään luonnoksen perusteella jää epäselväksi, tuleeko tiedonhallintayksiköiden jatkossa laatia tiedonohjaussuunnitelma, joka tällä hetkellä on muodostanut sähköisen asiankäsittelyn rungon. Entä kuka jatkossa vastaisi sähköisen asiakirjahallinnan toimintatapojen ohjaamisesta ja ohjeistuksesta. Oikeusrekisterikeskus pitää ohjausvastuiden selkeyttämistä ja riittävää resursointia erittäin tärkeänä. Jos arkistointitarkoitukseen säilytettävää tietoa säilytetään toisistaan poikkeavissa tietorakenteissa, voi arkistoitujen tietojen käsittely olla haastavaa yhteentoimivuuden näkökulmasta.

13. Kommentit ja huomiot lakiehdotuksen lukuun 9 Erinäiset säännökset (pykälät 39-40 ja niiden yksityiskohtaiset perustelut)

Oikeusrekisterikeskus huomauttaa, että siirtymäsäännös asiakirjojen kokonaan sähköisen säilytysmuodon osalta vaikuttaa liian lyhyelle, jos siirtymä halutaan tehdä hallitusti vaarantamatta asiakirjatietojen eheyttä, todistusvoimaa ja säilymistä. Perusteltu voisi olla kolmen (3) tai viiden (5) vuoden siirtymäaika ja tähän tulisi osoittaa riittävät resurssit.

Valtionhallinnossa on voimassa tietoturvallisuusasetuksen (681/2010) myötä velvoittava ja yhtenäinen tietoturvallisuuden perustaso sekä säädöksessä yksilöidyt ja yhtenäiset tietoturvallisuuden perustason tietoturvavaatimukset (vrt. viittaukset HE luonnoksen tietoturvallisuuden vähimmäisvaatimuksiin perusteluosiossa). Lisäksi valtionhallinnossa on luotu yhtenäisiä tietoturvakäytänteitä ja tietoturvallisuusasetuksen vaatimuksiin soveltamisohjeita mm. VAHTI-toiminnan ja -ohjeistuksien kautta. Huomioitavaa on, että tietoturvallisuusasetuksen toimeenpanoon annettiin perustason tietoturvallisuuden saavuttamiseksi valtionhallinnolle kolmen (3) vuoden siirtymäaika ja toimitilaturvallisuuden osalta viisi (5) vuotta. Oikeusrekisterikeskus huomauttaa, että luonnoksessa 4 luvun tietoturvallisuusvaatimusten toimeenpanolle ehdotettu 12 kuukauden siirtymäaika vaikuttaa liian lyhyelle. Tietoturvallisuuden vähimmäisvaatimusten toteuttamiseksi voisi esimerkiksi harkita kolmen (3) vuoden siirtymäaikaa.

Oikeusrekisterikeskus huomauttaa, että 18 §:n lokitietojen keräämisen vaatimustenmukaisuuden täyttämiselle annettu 24 kuukauden siirtymäaika vaikuttaa lyhyelle ottaen esimerkiksi huomioon eduskuntakäsittelyssä olevan HE:n 31/2018 niin sanotun rikosasioiden tietosuojalain 63 §:ssä esitetyn lokitietojen keräämisen vaatimustenmukaisuudelle annettu viiden (5) vuoden siirtymäajan.

14. Muut huomiot

Tietoturvallisuusasetuksesta, tietoturvallisuuden perustason tietoturvavaatimuksista ja sen perusteella annetuista VAHTI-ohjeistuksista sekä valtiovarainministeriön järjestämistä yhteishankkeista on ollut suuri merkitys ja hyöty valtionhallinnon viranomaisille yhtenäisemmän tietoturvallisuuden tason kehittämiseksi ja tietoturvallisuuden suunnittelemiseksi ja hallinnan mahdollistamiseksi. Lisäksi hyötyä on ollut valtionhallinnon viranomaisten julkisiin hankintoihin ja yksityisen sektorin palveluntuottajien kanssa sopimuksiin sekä yhteistyön prosessien kehittämiseen. Tietoturvallisuusasetuksesta saatiin tarpeellista selkänojaa valtionhallinnon virastoissa tietoturvallisuuteen ja riskienhallintaan liittyviin periaatteisiin, määräyksiin, ohjeisiin ja tietohallinnon ja tietoturvallisuuden parissa työskenteleville.

Tietoturvallisuuden vähimmäisvaatimukset tuli laajentaa kaikille tiedonhallintayksiköille, mutta ne tulisi HE luonnosta selkeämmin yksilöidä. Tietoturvallisuuden vähimmäisvaatimukset varmistaisivat samalla, että viranomaiset saavat selkänojaa toiminnan turvaamiseen, tiedonhallinnan kehittämisen sekä yhteentoimivuuden tukemiseen.

Kansallisarkistolla on tärkeä rooli viranomaisten asiakirjahallintoa ja arkistotointa ohjaavana organisaationa mukaan lukien sähköisen/digitaalisen asiakirjahallinnan ohjaamisessa ja yhtenäisten standardien ja toimintatapojen kehittämisessä. Jos näitä vastuita ollaan siirtämässä pois Kansallisarkistolta, tulisi näiden tehtävien hoitoon määritellä selkeät vastuut ja riittävät resurssit.

Vaikutusten arviointi

Tiedonhallinnan suunnittelu ja kuvaaminen:

Esitys jättää monin paikoin epäselväksi, mitkä tulevassa mallissa ovat esimerkiksi tietoturvallisuuteen, tietojen sähköiseen luovuttamiseen ja tietojen arkistointiin liittyvät vastuut toiminnan ohjaamisen näkökulmasta. Nykyisessä esityksen muodossa tiedonhallintayksiköiden vastuu kyseisten asioiden määrittelyssä kasvaisi. Tämä lisää tiedonhallintayksiköiden työtä. Selkeiden toimintalinjausten sekä sitovien ohjausten ja määräysten puuttuminen voi johtaa esityksen tavoitteista poiketen toimintatapojen pirstoutumiseen julkisessa hallinnossa esimerkiksi tietoturvallisuuden ja tietojen säilyttämisen osa-alueilla. Tämä olisi vastoin esityksen kannatettavia tavoitteita tiedonhallinnan toimintatapojen ja yhtenäisyyden parantamisesta. Lisäksi esityksessä kuvattu kasvava dokumentointivelvoite lisää tiedonhallintayksiköiden työtaakkaa. Oikeusrekisterikeskus kiinnittää huomiota siihen, että esimerkiksi esityksen yksityiskohtaisissa perusteluissa voisi tarkemmin kuvata, millä tavalla jo olemassa olevaa tietosuojan ja tiedonhallinnan dokumentaatiota voitaisiin hyödyntää tiedonhallintamallin kuvaamisessa, jotta vältytään tarpeettomalta työltä ja samojen asioiden useaan kertaan kuvaamiselta.

Tietoturvallisuus:

Tietoturvan minimitason tarkan määritelmän puuttuminen sekä tulevien ohjausvastuiden selkeän kuvauksen puuttuminen jättää tiedonhallintayksiköille paljon tulkinnan varaa ja omaa määrittelytyötä. Oikeusrekisterikeskus huomauttaa, että tämä voi johtaa tietoturvan vaarantumiseen ja vaatimuskentän hajautumiseen julkisessa hallinnossa.

Nykyisessä muodossaan HE luonnos lisäisi merkittävästi hallinnollista työtä. Henkilöstöä on uudelleen koulutettava ja ohjeistettava läpi julkisen hallinnon ja laajemminkin. Soveltamiskäytännöistä, dokumentaatioista ja tietoturvallisuuden tasoista eri tiedonhallintayksiköissä voi tulla hyvin kirjavia. Mikäli siirtymäaika on lyhyt, ei myöskään ole mahdollista asianmukaisesti organisoida esimerkiksi tiedonhallinnan ja tietoturvallisuuden yhteishankkeita, joiden avulla nyt esitetty laaja kokonaisuus voitaisiin jalkauttaa hallitusti. Lisäksi tiedonhallintayksiköiden olisi arvioitava omaa ja yhteistä tietojen käsittelyään, tietojen uudelleen luokittelua sekä tietojärjestelmiään sen suhteen, että täyttävätkö nämä tiedonhallinnan ja tietoturvallisuuden muuttuneet vaatimukset. Tämä arviointi tulisi dokumentoida ainakin EU:n yleisen tietosuoja-asetuksen mukaan. Valtiohallinnolle tämä tarkoittaisi arviointivelvoitetta sekä joko tietoturvallisuuden tason nostamiseksi tietyiltä osin (mm. HE luonnoksen lokituksen laajentaminen ja tiettyjen tietojen tai tietoliikenneyhteyksien salaaminen tai muu suojaaminen voivat aiheuttaa merkittäviäkin kustannuksia). Toisaalta, tietyiltä osin tietoturvallisuuden tason laskua on arvioitava ja riskiarvioitava miten uudelle tietoturvallisuuden vähimmäistasolle uudelleen luokitteluiden seurauksena tulisi edetä (mm. jopa nykyiset salassa pidettävät, suojaustaso III, mikäli eivät laajene turvallisuusluokituksen piiriin sekä turvallisuusluokitellut KÄYTTÖ RAJOITETTU ST IV). Hallinnollisesti myös sopimuksia on merkittävissä määrin arvioitava, että voidaanko niiden suojaustasoihin kytkettyjä tietoturvallisuudelle ja dokumentoinnin osalta päivitettävä tiedonhallinnan edellyttämälle vähimmäistasolle jopa sopimuskauden aikana siirtymäsäännösten ollessa kovin lyhyitä. Valtionhallinnon osalta syntyy kustannuksia myös tietojärjestelmien mahdollisista siirroista ja uusien tietojärjestelmäympäristöjen ryhmittelystä luokittelun muututtua aiempien suojaustasoihin perustuvien tietojärjestelmä- ja verkkoarkkitehtuurien sijaan.

Asian ja palvelujen tiedonhallinta:

23 §:ssä määritellään asian yksilöintitunnuksen sisältö. Oikeusrekisterikeskus huomauttaa, että uuden asiatunnuksen käyttöönotosta syntyy kustannuksia, kun esimerkiksi nykyisiä tietojärjestelmiä tulee kehittää tämän mukaisesti.

Tietoaineistojen luovuttaminen ja sähköinen luovutustapa:

Jotta viranomaisten asiankäsittelyssä ja asiakirjahallinnassa voidaan siirtyä kokonaan digitaaliseen käsittelyyn, tulee organisaatioiden kehittää ja hankkia tämän edellyttämät tietojärjestelmät. Nämä vaatimukset täyttäviä tietojärjestelmiä ei vielä ole käytössä läheskään kaikissa julkisen hallinnon organisaatioissa, mikä varovaisenkin arvion mukaan tulee aiheuttamaan huomattavia kehittämiskustannuksia. Poiketen esityksen taloudellisia vaikutuksia käsitelleestä luvusta, julkisen hallinnon organisaatioissa ei vielä muunneta kaikkia niihin saapuvia analogisia asiakirjoja ja lomakkeita sähköiseen muotoon, eikä tämä ole järkevääkään, ennen kuin organisaatioilla on käytössään kokonaan digitaalisen työtavan ja asiankäsittelyn edellyttämät tietojärjestelmät. Nämä seikat tulisi tarkemmin huomioida tulevan lain siirtymäsäännöksissä sekä taloudellisissa vaikutuksissa. Tietojärjestelmien kehittämiseen tulee varata riittävät resurssit, jotta toiminnassa voidaan luotettavasti siirtyä kokonaan sähköiseen työtapaan.

Oikeusrekisterikeskuksen ylläpitämä varallisuusrangaistusten valtakunnallinen täytäntöönpanojärjestelmä ja sakkorekisteri ei esimerkiksi täytä tämän hetken sähköisen säilyttämisen (Sähke-normi) vaatimuksia ja siihen rekisteröidyt asiakirjat säilytetään analogisessa muodossa. Sähköistä säilyttämistä koskevien viranomaisvaatimusten sisällön pysyessä samalla tasolla, tulee täytäntöönpanojärjestelmän kehittämiseen osoittaa riittävät resurssit, jotta siirtymä kokonaan digitaalisen asiakirjatiedon käsittelyyn voidaan tehdä hallitusti ja tiedon eheyttä ja todistusvoimaa vaarantamatta.

Jos vakiomuotoisten tietojen luovuttamiseen sähköisen rajapinnan avulla ei liity tarveharkintaa ja joustoa, voi rajapintojen rakentamisesta koitua huomattaviakin taloudellisia kustannuksia, joiden arviointi ennalta on hyvin haastavaa.

Tietoaineistojen säilyttäminen ja arkistointi:

Jos arkistointitarkoitukseen säilytettävien tietojen rakenne ja tiedostomuodot eivät pohjaudu yhtenäisiin toimintatapoihin ja standardeihin, on vaarana, että arkistoitujen tietojen hyödynnettävyys, säilyminen ja yhteentoimivuus vaarantuvat pitkällä tähtäimellä ja julkiseen hallintoon syntyy toisistaan poikkeavia käytäntöjä.

Muuta huomioitavaa:

Raatikainen Ritva-Liisa
Oikeusrekisterikeskus

Huhta Iivari
Oikeusrekisterikeskus