TIETOSUOJAVALTUUTETUN TOIMISTO

Lausunto

TSV/9194/2025

12.9.2025

kirjaamo.om@gov.fi

Lausuntopyyntö: VN/9885/2025 (Lausuntopyyntö luonnoksesta hallituksen esitykseksi tietosuojalainsäädännön kokonaisuudistukseen liittyvistä muutoksista oikeusministeriön hallinnonalan lainsäädäntöön

Tietosuojavaltuutetun toimiston lausunto

Tietosuojalakiin ehdotettavat muutokset

Kommenttinne koskien tietosuojalain 4 §:n ehdotettavia muutoksia (henkilötietojen käsittely yleistä etua koskevan tehtävän suorittamiseksi tai julkisen vallan käyttämiseksi):

Ei kommentoitavaa.

Kommenttinne koskien tietosuojalain 6 §:n ehdotettavia muutoksia (erityisiin henkilötietoryhmiin ja rikostuomioihin ja rikoksiin liittyvä käsittely):

Vakuutuksenhakijoiden tietojen käsittelystä

Hallituksen esityksessä ehdotetaan muutettavaksi 6 §:n sääntelyä koskien vakuutusyhtiöiden oikeutta käsitellä vakuutustoiminnassa saatuja tietoja vakuutetun ja korvauksenhakijan terveydentilasta, sairaudesta tai vammaisuudesta. Säännökseen ehdotetaan terveydentilatietojen käsittelyperusteen laajennusta vakuutuksenhakijoiden tietoihin siten, että yleisen tietosuoja-asetuksen 9 artiklan 1 kohtaa ei sovellettaisi myöskään vakuutuslaitoksen käsitellessä vakuutustoiminnassa saatuja tietoja vakuutuksenhakijan sekä sen henkilön, jolle vakuutussuojaa haetaan, terveydentilasta, sairaudesta tai vammaisuudesta taikka sellaista häneen kohdistetuista hoitotoimenpiteistä tai niihin verrattavista toimista.

Samanaikaisesti säännöstä ehdotetaan muutettavaksi siten, että edellä mainittujen tietojen käsittelyn edellytyksenä olisi se, että tiedot ovat välttämättömiä vakuutuslaitoksen vastuun arvioimiseksi ja selvittämiseksi. Nykytilassa vakuutusyhtiöiden terveydentilatietojen käsittelyn edellytyksenä on tietojen käsittelyn tarpeellisuus vakuutusyhtiöiden vastuun selvittämisen kannalta. Tältä osin terveydentilatietojen käsittelyn edellytyksiä muutetaan ja ehdotetun muutoksen myötä ei riitä, että tiedot ovat tarpeen vaan niiden käsittely on oltava välttämätöntä vastuun arvioinnissa tai selvittämisessä.

Hallituksen esityksen sivuilla 43–44 on arvioitu ehdotettavan sääntelyn vaikutuksia henkilötietojen suojaan sekä perustuslain 10 §:ssä turvattuun

henkilötietojen ja yksityisyyden suojaan. Ehdotettavan lainsäädännön on arvioitu hallituksen esityksessä täyttävän perustuslain 10 §:stä seuraavat vaatimukset yksityiselämän ja henkilötietojen suojaamiselle.

Olemme hallituksen esityksessä todetun kanssa yhtä mieltä siitä, että käsittelyn rajoittaminen vain välttämättömään säännöksen sanamuodon mukaisesti on tarpeellinen ja oikeasuhtainen toimenpide, joka edistää perustuslain 10 §:n vaatimusten täyttymistä. Tietosuojavaltuutetun käsityksen mukaan ehdotettava sääntely kuitenkin rajoittaisi vakuutuksenhakijoiden henkilötietojen ja yksityiselämän suojaan liittyviä oikeuksia ja vapauksia siltä osin, kun ehdotetun muutoksen myötä vakuutusyhtiöt voisivat käsitellä vakuutuksenhakijoiden terveydentilatietoja jo hakemusvaiheessa suoraan lain nojalla. Terveydentilatiedoissa on kysymys erityisiin henkilötietoryhmiin kuuluvista tiedoista. Tällaisten tietojen käsittelyperusteen laajentaminen voi aiheuttaa rekisteröityjen oikeuksille ja vapauksille erityisen suuria riskejä. Tähän liittyen on todettava, että vakuutusyhtiöiden käytäntönä on jo hakemusvaiheessa ollut esittää terveydentilatietoihin kohdistuvia varsin laajoja ja tarkemmin kohdentamattomia pyyntöjä. Tämä on kysymys, josta sekä tietosuojavaltuutettu henkilökohtaisesti että tietosuojavaltuutetun toimisto saa toistuvasti kansalaisyhteydenottoja ja kanteluita. Tällaisista yhteydenotoista välittyy ihmisten pitävän tällaista henkilötietojen käsittelyä suhteettomana epäoikeudenmukaisuutena.

Katsomme, että hallituksen esityksen tietosuojavaikutusten ja perusoikeusvaikutusten arviointia tulisi vielä tältä osin täydentää. Tietosuojavaikutusten ja perusoikeusvaikutusten arvioinnissa olisi otettava huomioon, että kyseessä on tosiasiassa vakuutuksenhakijoiden oikeuksien rajoittaminen. Hallituksen esityksen perusteluissa on tarpeen arvioida tarkemmin, onko oikeuksien rajoittaminen oikeasuhtainen toimenpide ottaen huomioon sen, mitkä ovat sääntelyllä mahdollisesti saavutettavat tavoitteet. Hallituksen esitys vaikuttaisi olevan myös niukkasanainen sen suhteen, mitkä ovat sääntelyn tosiasialliset tavoitteet siltä osin, kun terveydentilatietojen käsittelyperuste laajennetaan vakuutuksenhakijoihin. Ehdotettavan tietosuojalain 6 §:n 1 kohdan säännöskohtaisissa perusteluissa on todettu, että vakuutuslaitoksella on tosiasiallisesti välttämätön tarve käsitellä terveydentilaa koskevia tietoja vastuunsa arvioimiseksi jo ennen vakuutuksen myöntämistä. Lisäksi säännöskohtaisissa perusteluissa todetaan, että esityksessä ehdotettavilla täsmennyksillä varmistettaisiin, että kohdan sääntely täyttää yleisen tietosuoja-asetuksen edellytykset sääntelyn yleisen edun mukaisuudesta ja oikeasuhteisuudesta.

Perusteluissa jää edellä tarkoitetuilta osin epäselväksi, mikä tämä yleisen edun mukainen tavoite varsinaisesti on. Lisäksi osin epäselväksi jää, miten on päädytty lopputulemaan, että vakuutuksenhakijoiden perustuslain 10 §:n mukaisten oikeuksien ja etujen rajoittaminen on oikeasuhtaista. Tietosuojavaltuutettu pyytää täydentämään hallituksen esityksen perusteluita jatkovalmistelussa tältä osin.

Sääntelyn oikeasuhtaisuuden arvioinnissa sekä perusoikeustarkastelussa tulee ottaa huomioon, onko ehdotettavan sääntelyn mukainen henkilötietojen käsittely vakuutuksenhakijoiden odotusten mukaista. Terveydentilatietojen käsittelyn laajenemisen osalta huomionarvioista on käsittelyn aiheuttama riski vakuutuksenhakijoiden oikeuksien ja vapauksien kannalta. Kiinnitämme huomiota siihen, että vakuutuksenhakijat eivät ole vielä vakuutussopimuksen osapuolia. Kysymys ei ole sopimuksen aikana, vaan esimerkiksi vakuutushakemuksen täyttämisen jälkeen vakuutusyhtiön toteuttamasta terveydentilatietojen käsittelystä. Vakuutuksenhakijat eivät siten välttämättä osaa ennakoida tässä kohtaa vakuutusyhtiöllä olevan oikeus käsitellä heidän terveydentilatietojaan. Yleisen tietosuoja-asetuksen tärkein tavoite on, että luonnollisilla henkilöillä säilyy hallinta omiin henkilötietoihinsa. Siten ehdotettavan muutoksen tietosuojavaikutuksia arvioitaessa olisi otettava huomioon, että sääntelyn laajennuksen myötä terveydentilatietojen käsittely ei kaikissa tilanteissa ole vakuutuksenhakijoiden odotusten mukaisia. Katsomme, että tämä seikka tulee ottaa huomioon sääntelyn oikeasuhtaisuuden arvioinnissa sekä tietosuojavaikutusten sekä perusoikeusvaikutusten tarkastelussa.

Suojatoimista

Pidämme hyvänä ehdotettavana suojatoimena terveydentilatietojen käsittelyn rajoittamista vain välttämättömään käsittelyyn, kun nykytilassa terveydentilatietojen käsittely on rajattu *tarpeellisiin* tietoihin. Lisäksi on hyvä, että perusteluissa on mainittu, että kyseinen välttämättömyysarviointi tulee tehdä erikseen ennen vakuutuksen myöntämistä ja vakuutuksen myöntämisen jälkeen.

Kun tietojen käsittelyn edellytystä rajoitetaan tarpeellisista tiedoista vain välttämättömiin tietoihin, olisi hyvä, että säännöksen perusteluista kävisi ilmi, mitä tämä tosiasiassa tarkoittaa tietojen käsittelyn kannalta. Hallituksen esityksessä 6 §:n säännöskohtaisissa perusteluissa on tällä hetkellä todettu sivulla 29, että vakuutuslaitoksella on tosiasiallisesti välttämätön tarve käsitellä kohdassa tarkoitettuja terveydentilaa koskevia tietoja vastuunsa arvioimiseksi jo ennen vakuutuksen myöntämistä. Lisäksi hallituksen esityksessä on todettu, että vakuutuslaitoksen olisi välttämätöntä arvioida vastuutaan myös vakuutuksen tekemisen jälkeen korvausasiaa ratkaistaessa. Näiltä osin herää kysymys, onko hallituksen esityksen säännöskohtaisiin perusteluihin viitaten terveydentilatietojen käsittely välttämättömästi tarpeellista kaikissa vakuutusyhtiön vastuun arvioinnin ja selvittämisen tilanteissa, eikä tapauskohtaista arviointia tietojen käsittelyn välttämättömyydelle tarvittaisi, kunhan välttämättömyysarvioinnin tekee erikseen ennen vakuutuksen myöntämistä ja vakuutuksen myöntämisen jälkeen. Lisäksi herää kysymys, onko ehdotettavan 6 §:n 1 momentin 1 kohdan sanamuodon muutoksella tosiasiallisesti sellainen vaikutus, että käsittelyedellytykset tiukentuvat nykytilan tarpeellisuusedellytyksestä välttämättömyysedellytykseen.

Hallituksen esityksen säännöskohtaisista perusteluista tulisi käydä ilmi, että käsittelyn välttämättömyysedellytys edellyttää aina tapauskohtaista arviointia sen suhteen, onko terveydentilatietojen käsittely välttämätöntä. Perusteluista tulisi käydä ilmi, että käsittelyn edellytykseksi ei ehdotettavan muutoksen jälkeen riitä vain, että tiedot ovat tarpeen, vaan niiden on oltava välttämättömiä siihen tarkoitukseen, joita varten niitä käsitellään. Sanamuotona tietojen välttämätön käsittely on miellettävä ehdottomasti tarpeelliseksi käsittelyksi, joka on pakko suorittaa. Pitäisimme myös hyvänä, että perusteluista ilmenisi konkreettisia esimerkkejä siitä, miten tai milloin käsittelyn edellytyksen tosiasiallisesti täyttyvät tai jäävät täyttymättä ehdotettavan sääntelyn puitteissa.

Pidämme hyvänä, että ehdotettavan tietosuojalain 6 §:n 1 momentin sääntelyn säännöskohtaisten perusteluissa on erikseen mainittu, että tietojen minimoinnin periaatteen näkökulmasta vakuutuslaitoksen tulisi muun muassa kussakin yksittäistapauksessa arvioida erikseen, tulisiko lainkohdassa tarkoitettuja terveydentilaa koskevia tietoja kerätä ainoastaan rekisteröidyltä itseltään vai olisiko vakuutuslaitoksella välttämätön tarve kerätä tietoja myös muualta kuin rekisteröidyltä itseltään vakuutuslaitoksen vastuun arvioimiseksi ja selvittämiseksi. Pidämme niin ikään hyvänä ja kannatettavana hallituksen esityksen sivun 30 mainintaa siitä, miten vakuutusyhtiöiden tulee yksilöidä ja rajata terveydenhuollon yksiköihin tekemänsä tietopyynnöt koskien vakuutettujen terveydentilatietoja.

Kommenttinne koskien tietosuojalain 7 §:n ehdotettavia muutoksia (rikostuomioihin ja rikoksiin liittyvä käsittely):

Ei kommentoitavaa.

Kommenttinne sertifiointielimien akkreditointia koskevista muutosehdotuksista:

Pidämme nyt esitettyä akkreditointimenettelyyn liittyvää muutosta toiminnan tehokkuuden ja osaamisen takaamisen kannalta hyvänä.

Ehdotamme, että ehdotetun 36 a §:n 2 momenttia muokattaisiin muotoon *Ensisijaisesti tietosuojavaltuutettu tai toissijaisesti kansallisen akkreditointielimen nimeämä asiantuntija toimii akkreditoinnissa teknisenä asiantuntijana. Jos teknisenä asiantuntijana toimii kansallisen akkreditointielimen nimeämä asiantuntija, tietosuojavaltuutetulle on ennen akkreditoinnin myöntämistä varattava tilaisuus lausua akkreditointielintä sitovasti yleisen tietosuoja-asetuksen 43 artiklan 2 ja 3 kohdassa tarkoitettujen, tietosuojaa koskevien kriteerien täyttymisestä.*

Muutosehdotuksen tavoitteena on tuoda näkyville lain tasolla tietosuojavaltuutetun asema ensisijaisena teknisenä asiantuntijana sekä tuoda näkyväksi myös lain tasolla tietosuojavaltuutetun lausunnon merkitys akkreditoinnin kannalta. Koska tietosuojavaltuutetun toimiston lisäkriteeristöön [lisäkriteeristöä ei vielä ole julkaistu] sisältyy myös muita kuin tietosuojaan

liittyviä kriteerejä, näkemyksemme mukaan lausunnon kohdistaminen juuri tietosuojaan liittyviin kriteereihin tekee menettelystä tehokkaan ja resurssoinnin kannalta järkevän.

Ehdotamme, että säännöskohtaisiin perusteluihin lisättäisiin maininta tietosuojavaltuutetun oikeudesta arvioida se, kuinka kauan ja mitä resursseja akkreditointi tietosuojan osalta vaatii. Ottaen huomioon tietosuojaan liittyvien seikkojen arviointiin menevän ajan ja resurssien arvioinnin vaativuuden, näkemyksemme mukaan tämän tehtävän tulisi olla tietosuojavaltuutetulla. Tämä voitaisiin ottaa huomioon pykälän 3 momentissa lisäämällä siihen maininta tietosuojavaltuutetun oikeudesta arvioida teknisenä arvioijana toimimisen vaatimat resurssit ja aikatarpeet.

Ehdotuksen sivulla 23 on todettu, että sertifiointi voisi parantaa henkilötietojen suojan toteutumista sertifiointia hakevien yritysten toiminnassa, koska sertifikaatin saaminen ja voimassa pysyminen edellyttää, että yritys osoittaa vaatimustenmukaisuutensa tietosuojan osalta ja toteuttaa myös tarvittavat korjaavat toimenpiteet. Ehdotamme, että kohdan sana *yritys* muutettaisiin siten, että siinä viitattaisiin rekisterinpitäjiin ja henkilötietojen käsittelijöihin. Näin muoto vastaisi yleisen tietosuoja-asetuksen 42 artiklan sanamuotoa, eikä siitä aiheutuisi virheellistä kuvaa sertifioinnin rajoittumisesta vain yrityksille.

Yleiset kommentit:

Ei yleisiä kommentteja.

<u>Muun oikeusministeriön hallinnonalan lainsäädäntöön ehdotettavat muutokset</u>

Kommenttinne teknisiä rajapintoja ja katseluyhteyksiä koskevien säännösten päivittämisestä:

Ei kommentoitavaa.

Kommenttinne yrityskiinnityslakia koskevista muutoksista:

Ei kommentoitavaa.

Yleiset kommentit:

<u>Muut kommentit:</u>

Yleiset kommentit:

Kiinnitämme huomiota siihen, että valvontaviranomaiselle yleisen tietosuoja-asetuksen 34 artiklan nojalla tehdyn tietoturvaloukkausta koskevan ilmoituksen käsittelyssä ja tapahtuneen tietoturvaloukkauksen johdosta mahdollisesti annettavien määräysten valmistelussa noudatettavasta menettelystä ei ole säädetty erikseen. Näin ollen asiaan sovelletaan tältä

osin hallintolakia (434/2003). Tätä on myös hallinto-oikeus tuoreessa ratkaisussaan (Helsingin hallinto-oikeus 6307/2024, annettu 24.10.2024) korostanut. Pidämme tarpeellisena, että tietosuojalakiin säädetään tätä koskeva poikkeussäännös.

Hallintolain 34 §:n 1 momentin mukaan asianosaiselle on ennen asian ratkaisemista varattava tilaisuus lausua mielipiteensä asiasta sekä antaa selityksensä sellaisista vaatimuksista ja selvityksistä, jotka saattavat vaikuttaa asian ratkaisuun. Saman pykälän 2 momentissa on säädetty tilanteista, joissa asian saa ratkaista asianosaista kuulematta.

Hallintolain 34 §:n 2 momentin mukaan asian saa ratkaista asianosaista kuulematta, jos: 1) vaatimus jätetään tutkimatta tai hylätään heti perusteettomana; 2) asia koskee palvelussuhteeseen tai vapaaehtoiseen koulutukseen ottamista; 3) asia koskee hakijan ominaisuuksien arviointiin perustuvan edun myöntämistä; 4) kuuleminen saattaa vaarantaa päätöksen tarkoituksen toteutumisen tai kuulemisesta aiheutuva asian käsittelyn viivästyminen aiheuttaa huomattavaa haittaa ihmisten terveydelle, yleiselle turvallisuudelle taikka ympäristölle; tai 5) hyväksytään vaatimus, joka ei koske toista asianosaista tai kuuleminen on muusta syystä ilmeisen tarpeetonta.

Apulaistietosuojavaltuutettu on 12.3.2024 päätöksellään ratkaissut asian TSV/2332/2023, jossa on ollut kysymys tietoturvaloukkauksesta. Apulaistietosuojavaltuutettu on antanut rekisterinpitäjälle yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan e alakohdan nojalla määräyksen ilmoittaa henkilötietojen tietoturvaloukkauksesta rekisteröidyille. Rekisterinpitäjä haki päätökseen muutosta hallinto-oikeudelta, joka on hyväksynyt rekisterinpitäjän valituksen ja kumonnut apulaistietosuojavaltuutetun päätöksen (Helsingin hallinto-oikeus 6307/2024, annettu 24.10.2024). Apulaistietosuojavaltuutetun päätös on kumottu kuulemisvirheen perusteella.

Edellä mainittu asia on ollut osa isompaa tietoturvaloukkauskokonaisuutta, johon liittyen tietosuojavaltuutetun toimisto on vastaanottanut 123 eri rekisterinpitäjän tekemää tietoturvaloukkausilmoitusta. Nämä kaikki 123 eri rekisterinpitäjää ovat käyttäneet XX:n tietojärjestelmää SaaS-palveluna ERP-tietojärjestelmässään, käyttäen muun muassa CRM-järjestelmää (asiakastiedot), palkkahallintoa (työntekijöiden palkanmaksuun liittyvä tieto) ja kellokorttipalvelua (työntekijöiden tuntikirjauksia ja poissaolokirjauksia). Tapahtunutta tietoturvaloukkausta on selvitetty käsittelijänä toimineen XX:n kanssa. Rekisterinpitäjiä ei kuultu käsittelijänä toimineen XX:n selvityksestä.

Yleisen tietosuoja-asetuksen 28 artiklan 3 kohdan f ja h alakohdassa säädetysti henkilötietojen käsittelijän suorittamaa käsittelyä on määritettävä sopimuksella tai muulla unionin oikeuden tai jäsenvaltion lainsäädännön mukaisella oikeudellisella asiakirjalla, joka sitoo henkilötietojen käsittelijää suhteessa rekisterinpitäjään ja jossa vahvistetaan käsittelyn kohde ja

kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät, rekisterinpitäjän velvollisuudet ja oikeudet. Tässä sopimuksessa tai muussa oikeudellisessa asiakirjassa on säädettävä erityisesti, että henkilötietojen käsittelijä auttaa rekisterinpitäjää varmistamaan, että 32–36 artiklassa säädettyjä velvollisuuksia noudatetaan ottaen huomioon käsittelyn luonteen ja henkilötietojen käsittelijän saatavilla olevat tiedot sekä saattaa rekisterinpitäjän saataville kaikki tiedot, jotka ovat tarpeen tässä artiklassa säädettyjen velvollisuuksien noudattamisen osoittamista varten.

Apulaistietosuojavaltuutettu on katsonut, että XX:n olisi tullut toimittaa tiedot myös rekisterinpitäjälle, ja rekisterinpitäjän itsensä olisi tullut varmistua siitä, että se tosiasiallisesti myös saa sille kuuluvat tiedot. Vaikka rekisterinpitäjä käyttäisi henkilötietojen käsittelyssä henkilötietojen käsittelijää, on kokonaisvastuu henkilötietojen käsittelystä lähtökohtaisesti rekisterinpitäjällä.

Viitattakoon myös nyt käsillä olevaa kysymystä koskeviin tulkintaohjeisiin. Euroopan tietosuojaneuvosto on ohjeissaan ottanut kantaa muun muassa rekisterinpitäjän ja henkilötietojen käsittelijän käsitteisiin yleisessä tietosuoja-asetuksessa[1], ja Euroopan tietosuojaneuvostoa edeltänyt tietosuojatyöryhmä on puolestaan antanut ohjeita muun muassa henkilötietojen tietoturvaloukkauksesta ilmoittamisesta[2]. Ensin mainituissa suuntaviivoissa todetusti henkilötietojen käsittelijän on ilmoitettava rekisterinpitäjälle aina, kun se havaitsee henkilötietojen tietoturvaloukkauksen, joka vaikuttaa henkilötietojen käsittelijän laitteistoihin tai tietotekniikkajärjestelmiin, ja autettava rekisterinpitäjää saamaan tiedot, jotka on mainittava valvontaviranomaiselle annettavassa raportissa.[3] Todettakoon, että henkilötietojen käsittelijän ei ennen rekisterinpitäjälle ilmoittamistaan tarvitse arvioida tietoturvaloukkauksen aiheuttaman riskin todennäköisyyttä. Tämän arvioinnin suorittaminen on rekisterinpitäjän velvollisuus. Henkilötietojen käsittelijän velvollisuus ilmoittaa loukkauksesta rekisterinpitäjälle antaa rekisterinpitäjälle mahdollisuuden puuttua tapahtuneeseen loukkaukseen ja määrittää, onko loukkauksesta tarpeen ilmoittaa valvontaviranomaiselle yleisen tietosuoja-asetuksen 33 artiklan 1 kohdassa säädetysti ja rekisteröidyille yleisen tietosuoja-asetuksen 34 artiklan 1 kohdassa säädetysti.[4]

[1] Suuntaviivat 07/2020 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä yleisessä tietosuoja -asetuksessa (versio 2.0, annettu 7. heinäkuuta 2021).
[2] Suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta (annettu 3. lokakuuta 2017, viimeksi tarkistettu ja hyväksytty 6. helmikuuta 2018).
[3] Suuntaviivat 07/2020 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä yleisessä tietosuoja-asetuksessa (versio 2.0, annettu 7. heinäkuuta 2021), s. 41. Ks. myös yleisen tietosuoja -asetuksen 33 artiklan 3 kohta.
[4] Suuntaviivat 07/2020 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä yleisessä tietosuoja-asetuksessa (versio 2.0, annettu 7. heinäkuuta 2021), s. 41. Ks. myös yleisen tietosuoja -asetuksen 33 artiklan 3 kohta.

Hallinto-oikeus on edellä sanotusta huolimatta todennut, että yleisessä tietosuoja-asetuksessa säädetty rekisterinpitäjän vastuu henkilötietojen käsittelystä tai tietojen käsittelijän ilmoitusvelvollisuus ei poista viranomaisen velvollisuutta noudattaa menettelyssään hallintolakia. Apulaistietosuojavaltuutettu on hakenut asiassa valituslupaa korkeimmalta hallinto-oikeudelta. Korkein hallinto-oikeus ei kuitenkaan valituslupaa myöntänyt (1911/2025, annettu 4.9.2025).

Tietoturvaloukkausilmoituksista tietosuojavaltuutetun toimiston asiaryhmänä

Tietoturvaloukkausilmoitusten asiaryhmä tietosuojavaltuutetun toimistossa on suuri, ja tietoturvaloukkausilmoitukset muodostavat tietosuojavaltuutetun toimistossa vireille saatettavien asioiden suurimman yksittäisen ryhmän. Vuonna 2024 tehdyt tietoturvaloukkausilmoitukset vastasivat 54 %:ia kaikista vuoden aikana tietosuojavaltuutetun toimistossa vireille saatetuista asioista. Lukumääräisesti tämä tarkoittaa 7 153 asiaa. Joskus kysymys voi olla yhdestä suuresta tietoturvaloukkausasiakokonaisuudesta.

Esimerkkeinä suuremmista tietoturvaloukkausasiakokonaisuuksista mainittakoon julkisuudessakin esillä ollut taloyhtiöitä koskeva tietoturvaloukkaustapahtuma[5] sekä Westlog-yhtiötä koskeva tietoturvaloukkaustapahtuma[6]. Todettakoon selvää olevan, että nyt käsillä olevalla oikeuskysymyksellä on erittäin suuri merkitys tietosuojavaltuutetun toimistolle ja sille, miten tietoturvaloukkausasioita tietosuojavaltuutetun toimistossa käsitellään.

Lisäesimerkkeinä mainittakoon tietoturvaloukkausasiat koskien tietosuojavaltuutetun toimiston asioita TSV/2745/2025, 2985/171/23 ja TSV/2351/2023. Ensimmäisenä mainittu asiakokonaisuus koskee vajaata 500 eri rekisterinpitäjää, jotka kaikki käyttävät samaa henkilötietojen käsittelijää. Toisena mainittu puolestaan koskee lähes tuhatta eri rekisterinpitäjää, jotka niin ikään kaikki käyttävät samaa henkilötietojen käsittelijää. Viimeisenä mainittu puolestaan koskee noin 100 eri rekisterinpitäjää, jotka kaikki myös käyttävät samaa henkilötietojen käsittelijää. Yleistä tietosuoja-asetusta säädettäessä onkin ymmärretty, että sellaiset tietoturvaloukkauskokonaisuudet, joissa on kysymys nyt käsillä olevan kaltaisesta tilanteesta (rekisterinpitäjä käyttää henkilötietojen käsittelijän tietojärjestelmää SaaS-palveluna), saattavat olla merkittävän suuria kokonaisuuksia jo rekisterinpitäjien lukumäärällä mitattuna. Tätä osoittaa osaltaan yleisen tietosuoja-asetuksen 28 artiklan 3 kohdan f ja h alakohdassa säädetty. Mahdoton ei olisi sellainenkaan tietoturvaloukkaustapahtuma, joka samanaikaisesti koskisi kymmeniätuhansia rekisterinpitäjiä. Tietosuojavaltuutetun toimistossa on ollut ainakin yksi tällainenkin asia käsiteltävänä. Asiassa 2409/171/19 vajaa 25 000 eri rekisterinpitäjää käytti yhtä ja

[5] Ks. esimerkiksi https://www.is.fi/digitoday/tietoturva/art-2000006044515.html [vierailtu 17.9.2025].
[6] Ks. esimerkiksi https://www.is.fi/digitoday/tietoturva/art-2000010126122.html [vierailtu 17.9.2025].

samaa henkilötietojen käsittelijää. Kun valvontaviranomaisen on tällaisessakin tilanteessa varattava kullekin rekisterinpitäjälle mahdollisuus lausua henkilötietojen käsittelijän selvityksestä, tällä velvollisuudella on merkittävä resurssivaikutus valvontaviranomaisen toimintaan.

Jos esimerkiksi asiassa TSV/2332/2023 valvontaviranomainen olisi kuullut kaikkia 123 rekisterinpitäjää, olisi tämä tarkoittanut kymmeniä, ellei satoja lisätyötunteja asian ratkaisemiseksi. Lisätyön määrä olisi toki ollut riippuvainen siitä, mitä nämä rekisterinpitäjät olisivat mahdollisissa selvityksissään lausuneet. Selvää kuitenkin on, että mahdollisesti 123 selvitykseen tutustuminen olisi ollut työlästä. Korostettakoon tässä yhteydessä sitä, että nämä rekisterinpitäjät eivät olisi voineet antaa asiassa riittävää selvitystä ilman henkilötietojen käsittelijän myötävaikutusta. Nämä 123 rekisterinpitäjää olisivat joka tapauksessa joutuneet kääntymään asiassa XX:n puoleen, sillä kysymys on ollut XX:n tarjoamasta tietojärjestelmästä. Vain XX:llä on ollut tosiasiallisesti mahdollisuus vastata kaikkiin asiassa esitettyihin kysymyksiin. Asia olisi myös todennäköisesti saatu ratkaistua vasta paljon myöhemmin, millä olisi ollut merkittävä vaikutus tietoturvaloukkauksen kohteeksi joutuneiden henkilöiden asemaan.

Kuulemisvelvollisuudesta luopumisesta

Hallintolain 34 §:n 2 momentin 4 kohdan mukaan asian saa ratkaista asianosaista kuulematta, jos kuuleminen saattaa vaarantaa päätöksen tarkoituksen toteutumisen tai kuulemisesta aiheutuva asian käsittelyn viivästyminen aiheuttaa huomattavaa haittaa ihmisten terveydelle, yleiselle turvallisuudelle taikka ympäristölle.

Hallintolain 34 §:n 2 momentin 4 kohtaa sovellettaessa asia saadaan ratkaista asianosaista kuulematta silloin, kun kuuleminen todennäköisesti olisi esteenä hallintopäätöksellä tavoiteltavien vaikutusten saavuttamiselle.

Hallintolain 34 §:n 2 momentin 5 kohdassa säädetyn osalta viittaamme korkeimman hallinto-oikeuden ratkaisuun KHO:2016:3. Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle on artiklana säädetty nimenomaisesti rekisteröidyn intressejä silmällä pitäen. Tietoturvaloukkauksesta saattaa aiheutua useita erilaisia henkilöihin kohdistuvia haittavaikutuksia, jotka voivat aiheuttaa fyysisiä, aineellisia tai aineettomia vahinkoja loukkauksen kohteeksi joutuneille.

Yleisen tietosuoja-asetuksen johdanto-osan 85 perustelukappaleessa todetusti jos henkilötietojen tietoturvaloukkaukseen ei puututa riittävän tehokkaasti ja nopeasti, siitä voi aiheutua luonnollisille henkilöille fyysisiä, aineellisia tai aineettomia vahinkoja, kuten omien henkilötietojen valvomiskyvyn menettäminen tai oikeuksien rajoittaminen, syrjintää, identiteettivarkaus tai petos, taloudellisia menetyksiä, pseudonymisoitumisen luvaton kumoutuminen, maineen vahingoittuminen, salassapitovelvollisuuden

alaisten henkilötietojen luottamuksellisuuden menetys tai muuta merkittävää taloudellista tai sosiaalista vahinkoa. Loukkauksesta saattaa aiheutua myös muuta merkittävää taloudellista taikka sosiaalista vahinkoa sen kohteeksi joutuneelle henkilölle.

Kuten edellä mainitussa yleisen tietosuoja-asetuksen johdanto-osan 85 perustelukappaleessa on todettu, nopea ilmoittaminen rekisteröidylle on ensiarvoisen tärkeää. Tätä ilmentää myös yleisen tietosuoja-asetuksen 34 artiklan 1 kohdassa säädetty. Tapahtuneesta tietoturvaloukkauksesta on ilmoitettava rekisteröidyille ilman aiheetonta viivytystä.

Saatuaan tiedon tapahtuneesta tietoturvaloukkauksesta rekisteröity voi ryhtyä tarpeellisiksi katsomiinsa toimenpiteisiin. Tietoturvaloukkauksesta riippuen tällaisia toimia voivat olla esimerkiksi salasanojen vaihtaminen, luottokorttien sulkeminen, mahdollisiin tiedonkalasteluyrityksiin varautuminen, laitteiden tyhjentäminen tiedoista ja / tai omaehtoisen luottokiellon tekeminen. Ajan kuluminen tapahtuneen tietoturvaloukkauksen ja rekisteröidylle ilmoittamisen välillä saattaa vaarantaa ilmoittamisen tarkoituksen. Mikäli rekisteröity ei tarpeeksi nopeasti saa tietoa tapahtuneesta tietoturvaloukkauksesta, ei hän välttämättä ehdi toteuttaa sellaisia toimia, jotka saattaisivat estää vaarantuneiden henkilötietojen käyttämisen epätoivottuihin tarkoituksiin.

Henkilötietojen joutuminen kolmannen haltuun saattaa altistaa loukkauksen kohteen myös identiteettivarkaudelle, josta on säädetty rikoslain (39/1889) 38 luvun 9 a §:ssä. Mikäli tietoturvaloukkauksen kohteeksi joutuneen henkilön tietoja taas ehditään käyttää esimerkiksi kiusaamistarkoituksessa, saattaa rekisteröidylle aiheutua paljonkin vaivaa myös tilanteen jälkiselvittämisestä.[7] Tällaisesta selvittämisestä voi aiheutua myös taloudellista vahinkoa loukkauksen kohteeksi joutuneelle. Tämä on tunnistettu myös lain esitöissä.[8]

Tietoturvaloukkauksesta mahdollisesti aiheutuvista seurauksista mainittakoon myös turvakiellon alaisten tietojen vuotamisesta johtuva osoitetiedon joutuminen vainoajan tietoon. Tällaisella vuotamisella voi olla vakavia henkeen ja terveyteen kohdistuvia seurauksia. Mainittakoon esimerkkinä myös potilastietojen sekoittuminen, joka voi johtaa väärään hoitoon tai pahimmassa tapauksessa myös henkilön kuolemaan. Tällaisissa tilanteissa olisi korostuneen tärkeää, että loukkauksen kohteeksi joutunut saisi tiedon loukkauksesta mahdollisimman nopeasti. Tällöin tällainen henkilö voisi itse osata kiinnittää erityistä huomiota omaan turvallisuuteensa ja hoitoonsa.

[7] Ks. esimerkiksi https://www.iltalehti.fi/digiuutiset/a/988d2876-a812-44c6-83de-9b447dc28f0f [vierailtu 17.9.2025].
[8] Ks. esimerkiksi HE 232/2014 vp, s. 37.

Korostettakoon lisäksi, että esimerkiksi erilaiset huijaukset kehittyvät jatkuvasti. Huijaus saattaa onnistua jo verrattain vähinkin henkilötiedoin. Esimerkiksi pelkkä puhelinnumero- ja ikätieto saattavat altistaa niin sanotulle Hei äiti -huijaukselle[9], ja jo henkilötiedoilla, joista on kysymys myös apulaistietosuojavaltuutetun ratkaisemassa asiassa, voidaan henkilöön kohdentaa huomattavankin vakavia petosyrityksiä.[10] Huijauksen kohteeksi joutuminen saattaa koitua kohteelleen paitsi kalliiksi[11] myös aiheuttaa merkittävää inhimillistä kärsimystä. Kun rikolliset saavat haltuunsa henkilöstä esimerkiksi taloudellista asemaa kuvaavia tietoja, voivat he kohdistaa tämän perusteella henkilöön tietyntyyppisiä kehittyneempiä huijaus- tai petosyrityksiä. Kun loukkauksen kohteeksi joutunut rekisteröity saa viivytyksettä tiedon loukkauksesta, saattaa hän esimerkiksi paremmin tunnistaa häneen kohdistetun huijaus- tai petosyrityksen. Kiinnitämme huomiota myös siihen, että onnistuessaan rikoksesta saattaa aiheutua suuria kuluja myös valtiolle, esimerkiksi korvattavina vahingonkorvauskuluina. Esimerkiksi Vastaamon uhreille valtion kassasta maksettavien korvausten kokonaissumma voi nousta kymmeniin miljooniin euroihin.[12] Mitä nopeammin henkilö saa tiedon tietoturvaloukkauksen kohteeksi joutumisestaan, sitä paremmin ja tehokkaammin hän saa torjuttua siitä mahdollisesti aiheutuvia seurauksia.

Ajan kuluminen tapahtuneen tietoturvaloukkauksen ja rekisteröidylle ilmoittamisen välillä saattaa vaarantaa ilmoittamisen tarkoituksen, vaikkakin myöhemmästäkin ilmoittamisesta saattaa olla hyötyä loukkauksen kohteeksi joutuneelle rekisteröidylle. Todennäköisesti tämä hyöty on kuitenkin vähäisempää kuin silloin kun ilmoitus tehdään yleisen tietosuoja-asetuksen 34 artiklassa säädetysti ilman aiheetonta viivytystä. Oikea-aikaisella ilmoittamisella voidaan merkittävästi vähentää tietoturvaloukkauksesta mahdollisesti aiheutuvia haittoja ja väärinkäytöksiä.

Edellä mainituin perustein katsomme, että kuuleminen tällaisissa tilanteissa saattaisi vaarantaa päätöksen tarkoituksen toteutumisen tai kuulemisesta aiheutuva asian käsittelyn viivästyminen aiheuttaa huomattavaa haittaa loukkauksen kohteeksi joutuneelle. Näin ollen esitämme, että tietosuojalakiin säädettäisiin tältä osin kuulemista koskeva poikkeussäännös.

Allekirjoitus

Anu Talus
Tietosuojavaltuutettu

[9] Ks. esimerkiksi https://yle.fi/a/74-20100518 [vierailtu 17.9.2025].
[10] Ks. esimerkiksi https://www.is.fi/digitoday/tietoturva/art-2000009629373.html [vierailtu 17.9.2025].
[11] Ks. esimerkiksi https://yle.fi/a/74-20124331 [vierailtu 17.9.20259.
[12] Ks. esimerkiksi https://yle.fi/a/74-20107845 [vierailtu 17.9.2025].

TIETOSUOJAVALTUUTETUN TOIMISTO

Laura Varjokari
Erityisasiantuntija