ASIAKIRJAN WP243 LIITE – USEIN KYSYTYT KYSYMYKSET

Tämän liitteen tarkoituksena on antaa yksinkertaisia ja helppolukuisia vastauksia joihinkin keskeisiin kysymyksiin, joita organisaatioilla voi olla tietosuojavastaavan nimittämistä koskevista yleisen tietosuoja-asetuksen uusista vaatimuksista.

Tietosuojavastaavan nimittäminen (37 artikla)

1 Minkä organisaatioiden on nimitettävä tietosuojavastaava? (37 artiklan 1 kohta)

Yleisen tietosuoja-asetuksen mukaan tietosuojavastaavan nimittäminen on pakollista kolmessa tapauksessa:

- tietojenkäsittelyä suorittaa viranomainen tai julkishallinnon elin (riippumatta siitä, mitä tietoja käsitellään)
- rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa
- rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu erityisiin henkilötietoryhmiin tai rikostuomioita tai rikkomuksia koskeviin tietoihin.

Unionin tai jäsenvaltion lainsäädännössä voidaan vaatia tietosuojavastaavan nimittämistä myös muissa tilanteissa. Myös silloin, kun yleisessä tietosuoja-asetuksessa ei nimenomaisesti vaadita tietosuojavastaavan nimittämistä, organisaatioiden voi olla hyödyllistä nimittää tietosuojavastaava vapaaehtoisesti. Tietosuojatyöryhmä kannustaa tällaista vapaaehtoista nimittämistä.

Lisätietoja on ohjeiden kohdassa 2.1.

2 Mitä tarkoitetaan ’ydintehtävien’ käsitteellä? (37 artiklan 1 kohdan b ja c alakohta)

’Ydintehtäviä’ tai ’keskeistä toimintaa’ voidaan pitää avaintoimintoina, joita rekisterinpitäjän tai henkilötietojen käsittelijän tavoitteiden saavuttaminen edellyttää. Niihin sisältyvät myös kaikki sellaiset toiminnot, joissa tietojenkäsittely on erottamaton osa rekisterinpitäjän tai henkilötietojen käsittelijän toimintaa. Esimerkiksi terveystietojen, kuten potilaskertomusten, käsittelyä olisi pidettävä yhtenä sairaalan ydintehtävistä, joten sairaaloiden on nimitettävä tietosuojavastaava.

Toisaalta kaikki organisaatiot suorittavat tiettyjä tukitoimintoja, kuten maksavat palkkaa työntekijöilleen tai käyttävät vakiomuotoisia tietoteknisiä tukitoimintoja. Nämä ovat organisaation ydintehtävien tai keskeisen liiketoiminnan tarpeellisia tukitoimintoja. Vaikka nämä toiminnot ovat tarpeellisia tai välttämättömiä, niitä pidetään yleensä ydintehtävien sijaan oheistoimintoina.

Lisätietoja on ohjeiden kohdassa 2.1.2.

3 Mitä tarkoitetaan ’laajamittaisen’ käsitteellä? (37 artiklan 1 kohdan b ja c alakohta)

Yleisessä tietosuoja-asetuksessa ei määritellä laajamittaista käsittelyä. Tietosuojatyöryhmä suosittelee, että määritettäessä, mikä on laajamittaista tietojenkäsittelyä, otetaan huomioon erityisesti seuraavat tekijät:

- asianomaisten rekisteröityjen lukumäärä – joko täsmällinen lukumäärä tai osuus kyseeseen

tulevasta väestöstä
- käsiteltävä tietomäärä ja/tai käsiteltävien tietotyyppien määrä
- tietojen käsittelytoiminnan kesto tai pysyvyys
- käsittelytoiminnan maantieteellinen laajuus.

Esimerkkejä laajamittaisesta käsittelystä:

- potilastietojen käsittely sairaalan tavanomaisessa toiminnassa
- kaupungin joukkoliikennejärjestelmää käyttävien henkilöiden matkatietojen käsittely (esim. seuranta matkakorttien avulla)
- kansainvälisen pikaruokaketjun asiakkaiden reaaliaikaisten sijaintitietojen käsittely tilastollisia tarkoituksia varten sellaisen henkilötietojen käsittelijän toimesta, joka on erikoistunut tällaiseen toimintaan
- asiakastietojen käsittely vakuutusyhtiön tai pankin tavanomaisessa liiketoiminnassa
- henkilötietojen käsittely käyttötottumuksia seuraavaa hakukonemainontaa varten
- puhelin- tai internetpalveluntarjoajien suorittama tietojenkäsittely (sisältö, liikenne, sijainti).

Esimerkkejä tietojenkäsittelystä, joka ei ole laajamittaista:

- yksittäisen lääkärin suorittama potilastietojen käsittely
- yksittäisen asianajajan suorittama rikostuomioita ja rikkomuksia koskevien henkilötietojen käsittely.

Lisätietoja on ohjeiden kohdassa 2.1.3.

4 Mitä tarkoitetaan ’säännöllisen ja järjestelmällisen seurannan’ käsitteellä? (37 artiklan 1 kohdan b alakohta)

Yleisessä tietosuoja-asetuksessa ei määritellä rekisteröityjen säännöllisen ja järjestelmällisen seurannan käsitettä, mutta siihen sisältyvät selvästi kaikenlainen seuraaminen ja profilointi internetissä, myös käyttötottumuksia seuraavaa mainontaa varten. Seurannan käsite ei kuitenkaan rajoitu pelkästään verkkoympäristöön.

Tietosuojatyöryhmän tulkinnan mukaan ’säännöllisellä’ tarkoitetaan yhtä tai useampaa seuraavista:

- toiminta jatkuu tai toteutetaan tietyin aikavälein tietyn ajan
- toiminta toistuu tai toistetaan määritettyinä aikoina
- toiminta on jatkuvaa tai ajoittaista.

Tietosuojatyöryhmän tulkinnan mukaan ’järjestelmällisellä’ tarkoitetaan yhtä tai useampaa seuraavista:

- toiminta on järjestelmän mukaista
- toiminta on ennalta järjestettyä, organisoitua tai menetelmällistä
- toiminta toteutetaan osana yleistä tiedonkeruusuunnitelmaa
- toiminta toteutetaan osana strategiaa.

Esimerkkejä: tietoliikenneverkon ylläpito; tietoliikennepalvelujen tarjonta; uudelleenmarkkinointi sähköpostitse (retargeting); dataohjattu markkinointitoiminta; profilointi ja pisteyttäminen riskinarviointia varten (esim. luottoluokitusta, vakuutusmaksujen määrittämistä, petosten torjuntaa tai

rahanpesun havaitsemista varten); sijainnin seuraaminen (esim. mobiilisovellusten avulla); kanta-asiakasohjelmat; käyttötottumuksia seuraava mainonta; hyvinvointi-, liikunta- ja terveystietojen seuranta puettavien laitteiden avulla; videovalvonta; verkkoon liitetyt laitteet, kuten älymittarit, älyautot ja kodin automaatio.

Lisätietoja on ohjeiden kohdassa 2.1.4.

5 Voivatko organisaatiot nimittää yhteisen tietosuojavastaavan? Jos voivat, millä edellytyksin? (37 artiklan 2 ja 3 kohta)

Yleisen tietosuoja-asetuksen mukaan konserni voi nimittää yhden ainoan tietosuojavastaavan edellyttäen, että ”tietosuojavastaavaan voidaan ottaa helposti yhteyttä jokaisesta toimipaikasta”. Tällä saavutettavuuden käsitteellä viitataan tietosuojavastaavan toimintaan rekisteröityjen ja valvontaviranomaisen yhteyspisteenä ja myös organisaation sisäisenä yhteyspisteenä. Riippumatta siitä, onko tietosuojavastaava organisaation sisäinen vai ulkopuolinen henkilö, saavutettavuuden takaamiseksi on tärkeää varmistaa, että tietosuojavastaavan yhteystiedot ovat saatavilla yleisen tietosuoja-asetuksen mukaisesti. Tietosuojavastaavalla on oltava edellytykset olla tehokkaasti yhteydessä rekisteröityihin ja tehdä yhteistyötä asianomaisten valvontaviranomaisten kanssa. Tämä tarkoittaa sitä, että yhteyttä on pidettävä valvontaviranomaisten ja rekisteröityjen käyttämällä kielellä tai käyttämillä kielillä. Tietosuojavastaavan henkilökohtainen saavutettavuus (riippumatta siitä, työskenteleekö hän työntekijöiden kanssa fyysisesti samassa paikassa vai tapahtuuko yhteydenpito puhelimen tai muun suojatun viestintäkanavan kautta) on olennaista sen varmistamiseksi, että rekisteröidyt voivat ottaa yhteyttä tietosuojavastaavaan.

Lisätietoja on ohjeiden kohdassa 2.3.

6 Onko mahdollista nimittää ulkoinen tietosuojavastaava? (37 artiklan 6 kohta)

Kyllä. Yleisen tietosuoja-asetuksen 37 artiklan 6 kohdan mukaan tietosuojavastaava voi olla rekisterinpitäjän tai henkilötietojen käsittelijän henkilöstön jäsen (sisäinen tietosuojavastaava) tai tietosuojavastaava voi hoitaa tehtäviään palvelusopimuksen perusteella. Tämä tarkoittaa, että tietosuojavastaava voi olla ulkoinen palveluntarjoaja, jolloin tietosuojavastaavan tehtävää hoidetaan henkilön tai organisaation kanssa tehdyn palvelusopimuksen perusteella.

Ulkoiseen tietosuojavastaavaan sovelletaan kaikkia 37–39 artiklan vaatimuksia. Kuten ohjeissa todetaan, jos tietosuojavastaavan tehtävää hoitaa ulkoinen palveluntarjoaja, kyseiselle palveluntarjoajalle työskentelevien henkilöiden ryhmä voi käytännössä hoitaa tietosuojavastaavan tehtävää tiiminä asiakkaalle nimetyn ensisijaisen yhteyshenkilön ja vastuuhenkilön alaisuudessa. Tällöin on olennaista, että jokainen tietosuojavastaavan tehtäviä hoitava ulkoisen organisaation jäsen täyttää kaikki yleisen tietosuoja-asetuksen sovellettaviksi tulevat vaatimukset.

Oikeusvarmuuden ja hyvän organisoinnin varmistamiseksi ohjeissa suositellaan, että palvelusopimuksessa määritellään selkeä tehtävänjako ulkoisen tietosuojavastaavan tiimin jäsenten kesken ja että kullekin asiakkaalle nimetään yksi henkilö ensisijaiseksi yhteyshenkilöksi ja vastuuhenkilöksi.

Lisätietoja on ohjeiden kohdissa 2.3, 2.4 ja 3.5.

7 Millainen ammattipätevyys tietosuojavastaavalla tulisi olla? (37 artiklan 5 kohta)

Yleisen tietosuoja-asetuksen mukaan ”tietosuojavastaavaa nimitettäessä otetaan huomioon henkilön ammattipätevyys ja erityisesti asiantuntemus tietosuojalainsäädännöstä ja alan käytänteistä sekä valmiudet suorittaa 39 artiklassa tarkoitetut tehtävät”.

Tarvittavan erityisasiantuntemuksen taso olisi määriteltävä suoritettujen tietojenkäsittelytoimien ja käsiteltävien henkilötietojen edellyttämän suojan perusteella. Jos esimerkiksi tietojenkäsittelytoiminta on erityisen monimutkaista tai siihen liittyy suuri määrä arkaluonteisia tietoja, tietosuojavastaava voi tarvita tavallista enemmän asiantuntemusta ja tukea.

Tarvittavaan ammattitaitoon ja asiantuntemukseen kuuluvat seuraavat:

- asiantuntemus kansallisesta ja EU:n tietosuojalainsäädännöstä ja alan käytänteistä, myös yleisen tietosuoja-asetuksen perusteellinen tuntemus
- suoritettujen käsittelytoimien tuntemus
- tietojärjestelmien ja tietoturvan tuntemus
- asianomaisen toimialan ja organisaation tuntemus
- valmiudet edistää tietosuojakulttuuria organisaatiossa.

Lisätietoja on ohjeiden kohdassa 2.4.

Tietosuojavastaavan asema (38 artikla)

8 Mitä resursseja tietosuojavastaavalle olisi järjestettävä tehtävien hoitamiseksi?

Yleisen tietosuoja-asetuksen 38 artiklan 2 kohdan mukaan organisaation on tuettava tietosuojavastaavaa ”antamalla tälle resurssit, jotka ovat tarpeen näiden tehtävien täyttämisessä, samoin kuin pääsyn henkilötietoihin ja käsittelytoimiin, sekä tämän asiantuntemuksen ylläpitämiseksi”.

Käsittelytoimien luonteesta ja organisaation toiminnasta ja koosta riippuen tietosuojavastaavalle olisi järjestettävä tarvittavat resurssit varmistamalla, että

- ylempi johto tukee aktiivisesti tietosuojavastaavan tehtävää
- tietosuojavastaavalle varataan riittävästi aikaa tehtävien hoitamiseen
- tietosuojavastaavalle järjestetään riittävästi tukea eli varoja, infrastruktuuri (tilat, palvelut, laitteet) ja tarvittaessa henkilöstö
- tietosuojavastaavan nimittämisestä ilmoitetaan virallisesti koko henkilöstölle
- tietosuojavastaavalle järjestetään pääsy muihin organisaation palveluihin, jotta hän voi saada niiltä olennaista tukea ja tietoa
- tietosuojavastaavalle tarjotaan jatkuvasti koulutusta.

Lisätietoja on ohjeiden kohdassa 3.2.

9 Millä suojatoimilla voidaan varmistaa, että tietosuojavastaava hoitaa tehtävänsä riippumattomasti? (38 artiklan 3 kohta)

Olemassa on useita suojatoimia, joilla varmistetaan, että tietosuojavastaava voi toimia riippumattomasti johdanto-osan 97 kappaleen mukaisesti:

- rekisterinpitäjä tai henkilötietojen käsittelijä ei saa antaa tietosuojavastaavalle ohjeita tämän tehtävien hoitamisesta
- rekisterinpitäjä ei saa erottaa tai rangaista tietosuojavastaavaa tietosuojatehtävien hoitamisen vuoksi
- mahdolliset muut tehtävät ja velvollisuudet eivät saa aiheuttaa eturistiriitaa.

Lisätietoja on ohjeiden kohdissa 3.3–3.5.

10 Mitkä ovat tietosuojavastaavan ’muut tehtävät ja velvollisuudet’, jotka voivat aiheuttaa eturistiriitaa? (38 artiklan 6 kohta)

Tietosuojavastaava ei voi olla organisaatiossa sellaisessa asemassa, jossa hänen on määritettävä henkilötietojen käsittelyn tarkoitukset ja keinot. Koska kullakin organisaatiolla on oma organisaatiorakenteensa, eturistiriitoja on tarkasteltava tapauskohtaisesti.

Yleisesti voidaan katsoa, että esimerkiksi ylemmät johtoasemat (esim. pääjohtaja, hallintopääjohtaja, talousjohtaja, johtava asiantuntijalääkäri, markkinointiosaston päällikkö, henkilöstöpäällikkö tai tietoteknisen osaston päällikkö) voivat aiheuttaa eturistiriidan, mutta sama koskee myös muita tehtäviä organisaatiorakenteen alemmilla tasoilla, jos näissä tehtävissä on määritettävä tietojenkäsittelyn tarkoitukset ja keinot.

Lisätietoja on ohjeiden kohdassa 3.5.

Tietosuojavastaavan tehtävät (39 artikla)

11 Mitä yleisessä tietosuoja-asetuksessa tarkoitetaan ’noudattamisen seuraamisella’? (39 artiklan 1 kohdan b alakohta)

Osana asetuksen noudattamisen seuraamista tietosuojavastaava voi erityisesti

- kerätä tietoa käsittelytoimien yksilöimiseksi
- analysoida käsittelytoimia ja tarkistaa, ovatko ne vaatimusten mukaisia
- antaa tietoa, neuvoja ja suosituksia rekisterinpitäjälle tai henkilötietojen käsittelijälle.

Lisätietoja on ohjeiden kohdassa 4.1.

12 Onko tietosuojavastaava henkilökohtaisesti vastuussa yleisen tietosuoja-asetuksen noudattamatta jättämisestä?

Ei. Tietosuojavastaava ei vastaa henkilökohtaisesti siitä, että yleistä tietosuoja-asetusta ei noudateta. Yleisessä tietosuoja-asetuksessa todetaan selvästi, että rekisterinpitäjän tai henkilötietojen käsittelijän on voitava varmistaa ja osoittaa, että käsittelyssä noudatetaan asetusta (24 artiklan 1 kohta). Tietosuojasääntöjen noudattaminen on näin rekisterinpitäjän tai henkilötietojen käsittelijän vastuulla.

13 Mikä rooli tietosuojavastaavalla on tietosuojaa koskevien vaikutustenarviointien (37 artiklan 1 kohdan c alakohta) ja käsittelytoimia koskevan selosteen (30 artikla) yhteydessä?

Tehdessään tietosuojaa koskevaa vaikutustenarviointia rekisterinpitäjän tai henkilötietojen käsittelijän tulisi pyytää neuvoja tietosuojavastaavalta muun muassa seuraavissa kysymyksissä:

- onko syytä tehdä tietosuojaa koskeva vaikutustenarviointi
- mitä menetelmiä tietosuojaa koskevaa vaikutustenarviointia tehtäessä olisi noudatettava
- kannattaako tietosuojaa koskeva vaikutustenarviointi toteuttaa organisaation sisäisesti vai ulkoistaa tehtävä
- mitä suojatoimia (mukaan lukien tekniset ja organisatoriset toimenpiteet) olisi toteutettava, jotta vähennetään rekisteröityjen oikeuksiin ja etuihin kohdistuvia riskejä
- onko tietosuojaa koskeva vaikutustenarviointi toteutettu oikein ja vastaavatko sen päätelmät (päätös siitä, aloitetaanko käsittely, ja käyttöön otettavat suojatoimet) yleisen tietosuoja-asetuksen vaatimuksia.

Lisätietoja on ohjeiden kohdassa 4.2.

Käsittelytoimia koskevan selosteen ylläpito on rekisterinpitäjän tai henkilötietojen käsittelijän – ei siis tietosuojavastaavan – tehtävä. Mikään ei kuitenkaan estä rekisterinpitäjää tai henkilötietojen käsittelijää antamasta tietosuojavastaavalle tehtäväksi ylläpitää selostetta rekisterinpitäjän vastuulla olevista käsittelytoimista. Tällaista selostetta olisi pidettävä yhtenä välineenä, jonka ansiosta tietosuojavastaava voi hoitaa niitä tehtäviään, jotka liittyvät sääntöjen noudattamisen seurantaan sekä tietojen ja neuvojen antamiseen rekisterinpitäjälle tai henkilötietojen käsittelijälle.

Lisätietoja on ohjeiden kohdassa 4.4.