TIETOSUOJATYÖRYHMÄ

16/FI
WP 243 rev.01

Tietosuojavastaavia koskevat ohjeet

Annettu 13. joulukuuta 2016

Viimeksi tarkistettu ja hyväksytty 5. huhtikuuta 2017

Työryhmä on perustettu direktiivin 95/46/EY 29 artiklalla. Se on riippumaton EU:n neuvoa-antava elin, joka käsittelee tietosuojaan ja yksityisyyden suojaan liittyviä kysymyksiä. Sen tehtävät määritellään direktiivin 95/46/EY 30 artiklassa ja direktiivin 2002/58/EY 15 artiklassa.

Työryhmän sihteeristön tehtävistä huolehtii Euroopan komission oikeus- ja kuluttaja-asioiden pääosaston linja C (perusoikeudet ja oikeusvaltioperiaate), toimisto MO59 05/35, B-1049 Bryssel, Belgia.

Verkkosivusto: http://ec.europa.eu/justice/data-protection/index_en.htm

TIETOSUOJATYÖRYHMÄ, joka

on perustettu 24 päivänä lokakuuta 1995 annetulla Euroopan parlamentin ja neuvoston direktiivillä 95/46/EY,

ottaa huomioon kyseisen direktiivin 29 ja 30 artiklan,

ottaa huomioon työjärjestyksensä,

ON ANTANUT SEURAAVAT OHJEET:

Sisällysluettelo

1 Johdanto

Yleisessä tietosuoja-asetuksessa[1], jonka on määrä tulla voimaan 25. toukokuuta 2018, säädetään nykyaikaistetusta, tilivelvollisuuteen perustuvasta tietosuojakehyksestä Euroopassa. Uuden lainsäädäntökehyksen keskeisiä toimijoita ovat tietosuojavastaavat, joiden tarkoituksena on helpottaa yleisen tietosuoja-asetuksen säännösten noudattamista useissa organisaatioissa.

Yleisen tietosuoja-asetuksen mukaan tiettyjen rekisterinpitäjien ja henkilötietojen käsittelijöiden on nimitettävä tietosuojavastaava.[2] Tämä velvoite koskee kaikkia viranomaisia ja julkishallinnon elimiä (riippumatta siitä, mitä tietoja ne käsittelevät) sekä sellaisia muita organisaatioita, joiden ydintehtäviin sisältyy henkilöiden järjestelmällinen ja laajamittainen seuranta tai erityisiin henkilötietoryhmiin kohdistuva laajamittainen käsittely.

Myös silloin, kun yleisessä tietosuoja-asetuksessa ei nimenomaisesti vaadita tietosuojavastaavan nimittämistä, organisaatioiden voi olla hyödyllistä nimittää tietosuojavastaava vapaaehtoisesti. Tietosuojatyöryhmä kannustaa tällaista vapaaehtoista nimittämistä.

Tietosuojavastaava ei ole käsitteenä uusi. Vaikka direktiivissä 95/46/EY[3] ei vaadita organisaatioita nimittämään tietosuojavastaavaa, tällainen käytäntö on vakiintunut useissa jäsenvaltioissa vuosien kuluessa.

Tietosuojatyöryhmä totesi jo ennen yleisen tietosuoja-asetuksen hyväksymistä, että tietosuojavastaava on tilivelvollisuuden kulmakivi ja että tietosuojavastaavan nimittäminen voi helpottaa säännösten noudattamista ja tuoda kilpailuetua yrityksille.[4] Sen lisäksi, että tietosuojavastaavat helpottavat säännösten noudattamista panemalla täytäntöön tilivelvollisuuden täyttämistä edistäviä välineitä (kuten tukemalla tietosuojaa koskevien vaikutustenarviointien tekemistä tai tekemällä tarkastuksia tai avustamalla niissä), he toimivat välittäjinä sidosryhmien (esim. valvontaviranomaisten, rekisteröityjen ja organisaation liiketoimintayksiköiden) välillä.

Tietosuojavastaavat eivät ole henkilökohtaisesti vastuussa yleisen tietosuoja-asetuksen noudattamatta jättämisestä, jos asetusta ei ole noudatettu. Yleisessä tietosuoja-asetuksessa todetaan selvästi, että

---

[1] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EUVL L 119, 4.5.2016, s. 1). Yleinen tietosuoja-asetus on merkityksellinen ETA:n kannalta, ja asetusta sovelletaan sen jälkeen, kun se on otettu osaksi ETA-sopimusta.

[2] Tietosuojavastaavan nimittäminen on pakollista myös toimivaltaisille viranomaisille luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta 27 päivänä huhtikuuta 2016 annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/680 (EUVL L 119, 4.5.2016, s. 89–131) 32 artiklan nojalla sekä kansallisen täytäntöönpanolainsäädännön nojalla. Vaikka näissä ohjeissa käsitellään ensisijaisesti yleisen tietosuoja-asetuksen mukaisia tietosuojavastaavia, ohjeet koskevat myös direktiivin (EU) 2016/680 mukaisia tietosuojavastaavia siinä määrin, kuin säännökset ovat samankaltaisia.

[3] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (EYVL L 281, 23.11.1995, s. 31).

[4] Ks. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

rekisterinpitäjän tai henkilötietojen käsittelijän on voitava varmistaa ja osoittaa, että käsittelyssä noudatetaan asetuksen säännöksiä (24 artiklan 1 kohta). Tietosuojasäännösten noudattaminen on näin rekisterinpitäjän tai henkilötietojen käsittelijän vastuulla.

Rekisterinpitäjä tai henkilötietojen käsittelijä luo myös edellytykset sille, että tietosuojavastaava voi hoitaa tehtävänsä. Tietosuojavastaavan nimittäminen on ensimmäinen askel, mutta tietosuojavastaavalle on annettava asianmukainen riippumattomuus ja asianmukaiset resurssit, jotta hän voi hoitaa tehtävänsä.

Yleisessä tietosuoja-asetuksessa todetaan tietosuojavastaavan olevan keskeinen toimija uudessa tietohallintojärjestelmässä ja vahvistetaan tietosuojavastaavan nimittämistä, asemaa ja tehtäviä koskevat ehdot. Näiden ohjeiden tarkoituksena on selventää kyseeseen tulevia yleisen tietosuoja-asetuksen säännöksiä ja auttaa siten rekisterinpitäjiä ja henkilötietojen käsittelijöitä noudattamaan lainsäädäntöä ja tietosuojavastaavia hoitamaan tehtäviään. Ohjeissa annetaan hyviä käytäntöjä koskevia suosituksia, jotka perustuvat joidenkin EU:n jäsenvaltioiden saamiin kokemuksiin. Tietosuojatyöryhmä seuraa ohjeiden noudattamista ja voi tarvittaessa täydentää niitä myöhemmin.

2 Tietosuojavastaavan nimittäminen

2.1. Pakollinen nimittäminen

Yleisen tietosuoja-asetuksen 37 artiklan 1 kohdan mukaan tietosuojavastaavan nimittäminen on pakollista kolmessa tapauksessa[5]:

a) tietojenkäsittelyä suorittaa viranomainen tai julkishallinnon elin[6]
b) rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa, tai
c) rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu erityisiin henkilötietoryhmiin[7] tai[8] rikostuomioita tai rikkomuksia koskeviin tietoihin[9].

Tietosuojatyöryhmä antaa seuraavissa alakohdissa ohjeita 37 artiklan 1 kohdassa käytetyistä kriteereistä ja termeistä.

Ellei ole selvää, että organisaation ei tarvitse nimittää tietosuojavastaavaa, tietosuojatyöryhmä suosittelee, että rekisterinpitäjät ja henkilötietojen käsittelijät dokumentoivat toteutetun sisäisen analyysin, joka on tehty sen selvittämiseksi, pitäisikö organisaatiossa nimittää tietosuojavastaava. Näin ne voivat osoittaa, että olennaiset tekijät on otettu asianmukaisesti huomioon.[10] Tämä analyysi on osa

[5] Yleisen tietosuoja-asetuksen 37 artiklan 4 kohdan mukaan unionin tai jäsenvaltion lainsäädännössä voidaan vaatia tietosuojavastaavan nimittämistä myös muissa tilanteissa.

[6] Lukuun ottamatta lainkäyttötehtäviään hoitavia tuomioistuimia. Ks. direktiivin (EU) 2016/680 32 artikla.

[7] Asetuksen 9 artiklan mukaan näihin kuuluvat sellaiset henkilötiedot, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys, sekä geneettiset tai biometriset tiedot henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevat tiedot taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot.

[8] Asetuksen 37 artiklan 1 kohdan c alakohdassa käytetään ”ja”-sanaa. Ks. jäljempänä kohta 2.1.5, jossa selitetään ”tai”-sanan käyttöä ”ja”-sanan sijaan.

[9] 10 artikla.

[10] Ks. 24 artiklan 1 kohta.

tilivelvollisuusperiaatteen mukaista dokumentaatiota. Valvontaviranomainen voi edellyttää analyysia, ja sitä olisi tarvittaessa päivitettävä, jos esimerkiksi rekisterinpitäjät tai henkilötietojen käsittelijät ottavat suorittaakseen sellaisia uusia toimintoja tai tarjoavat sellaisia uusia palveluja, jotka voivat kuulua 37 artiklan 1 kohdassa lueteltuihin tapauksiin.

Jos organisaatio nimittää tietosuojavastaavan vapaaehtoisesti, tietosuojavastaavan nimittämiseen, asemaan ja tehtäviin sovelletaan 37–39 artiklan vaatimuksia samalla tavoin kuin tilanteessa, jossa nimittäminen on pakollista.

Organisaatio, jolla ei ole lakisääteistä velvoitetta nimittää tietosuojavastaavaa ja joka ei halua tehdä nimitystä vapaaehtoisesti, voi kuitenkin vapaasti palkata henkilöstöä tai ulkopuolisia konsultteja hoitamaan henkilötietojen suojaan liittyviä tehtäviä. Tällöin on kuitenkin tärkeää varmistaa, ettei kyseisten henkilöiden tehtävänimikkeestä, toimesta, asemasta ja tehtävistä ole epäselvyyttä. Näin ollen kaikessa yrityksen sisäisessä viestinnässä sekä viestinnässä tietosuojaviranomaisten, rekisteröityjen ja suuren yleisön kanssa on selvennettävä, että kyseisen henkilön tai konsultin tehtävänimike ei ole tietosuojavastaava.[11]

Tietosuojavastaavan toimialaan kuuluvat kaikki rekisterinpitäjän tai henkilötietojen käsittelijän suorittamat käsittelytoimet riippumatta siitä, onko nimitys ollut pakollinen vai vapaaehtoinen.

2.1.1 VIRANOMAINEN TAI JULKISHALLINNON ELIN

Yleisessä tietosuoja-asetuksessa ei määritellä, mitä tarkoitetaan ’viranomaisella tai julkishallinnon elimellä’. Tietosuojatyöryhmä katsoo, että käsite on määriteltävä kansallisen lainsäädännön perusteella. Viranomaisiin ja julkishallinnon elimiin kuuluvat näin ollen kansalliset, alueelliset ja paikalliset viranomaiset, mutta yleensä käsite kattaa sovellettavan kansallisen lainsäädännön nojalla myös joukon muita julkisoikeudellisia elimiä[12]. Näissä tapauksissa tietosuojavastaavan nimittäminen on pakollista.

Julkista tehtävää voivat hoitaa ja julkista valtaa käyttää[13] viranomaisten ja julkishallinnon elinten lisäksi myös muut julkis- tai yksityisoikeudelliset luonnolliset tai oikeushenkilöt, jotka toimivat esimerkiksi joukkoliikennepalvelujen, vesi- ja energiahuollon, tieinfrastruktuurin, yleisradiotoiminnan tai julkisen asuntotuotannon aloilla taikka säänneltyä ammattitoimintaa koskevissa kurinpitoelimissä, sen mukaan mitä kunkin jäsenvaltion kansallisessa lainsäädännössä säädetään.

Rekisteröidyt saattavat olla edellä mainitun kaltaisten organisaatioiden suhteen hyvin samanlaisessa tilanteessa kuin silloin, kun tietoja käsittelee viranomainen tai julkishallinnon elin. Tietojenkäsittelyn tarkoitukset voivat olla samanlaisia, ja henkilöillä on usein samalla tavoin joko vähän tai ei lainkaan vaikutusvaltaa siihen, käsitelläänkö heidän tietojaan ja millä tavoin. Tämän vuoksi henkilöitä, joiden tietoja käsitellään, voi olla tarpeen suojata tavallista enemmän, minkä tietosuojavastaavan nimittäminen mahdollistaa.

---

[11] Näin on tehtävä myös silloin kun on kyse yksityisyyden suojasta vastaavista toimihenkilöistä tai muista alan ammattilaisista, joita jotkin yritykset ovat jo palkanneet. Nämä henkilöt eivät välttämättä täytä yleisen tietosuoja-asetuksen kriteerejä esimerkiksi käytössään olevien resurssien tai riippumattomuutensa osalta, jolloin heitä ei voida pitää tietosuojavastaavina eikä kutsua tietosuojavastaaviksi.

[12] Ks. esimerkiksi julkisen sektorin hallussa olevien tietojen uudelleenkäytöstä 17 päivänä marraskuuta 2003 annetun Euroopan parlamentin ja neuvoston direktiivin 2003/98/EY 2 artiklan 1 ja 2 kohdassa (EUVL L 345, 31.12.2003, s. 90) annettu ’julkisen sektorin elimen’ ja ’julkisoikeudellisen laitoksen’ määritelmä.

[13] 6 artiklan 1 kohdan e alakohta.

Vaikka nimittämistä ei tällaisissa tapauksissa vaadita, tietosuojatyöryhmä suosittelee hyvänä käytäntönä, että julkista tehtävää hoitavat tai julkista valtaa käyttävät yksityiset organisaatiot nimittävät tietosuojavastaavan. Tietosuojavastaavan toiminta kattaa tällöin kaikki suoritetut käsittelytoimet, mukaan lukien ne, jotka eivät liity julkisen tehtävän hoitamiseen tai virkavelvollisuuden täyttämiseen (esim. työntekijöitä koskevan tietokannan hallinta).

2.1.2 YDINTEHTÄVÄT

Yleisen tietosuoja-asetuksen 37 artiklan 1 kohdan b ja c alakohdassa viitataan rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtäviin. Johdanto-osan 97 kappaleessa täsmennetään, että rekisterinpitäjän keskeinen toiminta liittyy tämän ”ensisijaisiin toimintoihin, eikä se liity oheistoimintona tapahtuvaan henkilötietojen käsittelyyn”. ’Ydintehtäviä’ tai ’keskeistä toimintaa’ voidaan siten pitää avaintoimina, joita rekisterinpitäjän tai henkilötietojen käsittelijän tavoitteiden saavuttaminen edellyttää.

Ydintehtäviä ei kuitenkaan pitäisi tulkita siten, että niihin eivät kuulu toiminnot, joissa tietojenkäsittely on erottamaton osa rekisterinpitäjän tai henkilötietojen käsittelijän toimintaa. Esimerkiksi sairaalan ydintehtävä on tarjota sairaanhoitoa. Sairaala ei kuitenkaan voi tarjota sairaanhoitoa turvallisesti ja tehokkaasti ilman terveystietojen, kuten potilaskertomusten, käsittelyä. Sen vuoksi näiden tietojen käsittelyn pitäisi katsoa kuuluvan sairaalan ydintehtäviin, ja sairaaloiden on näin ollen nimitettävä tietosuojavastaava.

Toisena esimerkkinä on yksityinen turvallisuusalan yritys, joka vastaa useiden yksityisten kauppakeskusten ja julkisten tilojen valvonnasta. Valvonta on näin yrityksen ydintehtävä. Tähän ydintehtävään liittyy kuitenkin erottamattomasti henkilötietojen käsittely. Näin ollen myös tämän yrityksen on nimitettävä tietosuojavastaava.

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

2.1.3 LAAJAMITTAINEN

Yleisen tietosuoja-asetuksen 37 artiklan 1 kohdan b ja c alakohdan mukaan henkilötietojen käsittelyn on oltava laajamittaista, jotta tietosuojavastaavan nimittämisestä tulee pakollista. Asetuksessa ei määritellä laajamittaista käsittelyä, mutta johdanto-osan 91 kappaleessa annetaan joitakin ohjeita.[14]

[14] Kyseisen kappaleen mukaan laajamittaiseen käsittelyyn kuuluvat etenkin laajat käsittelytoimet, ”joissa on tarkoitus käsitellä huomattavia määriä henkilötietoja alueellisella, kansallisella tai ylikansallisella tasolla, jotka voivat vaikuttaa suureen määrään rekisteröityjä ja joihin todennäköisesti liittyy suuri riski”. Toisaalta kyseisessä johdanto-osan kappaleessa täsmennetään, että ”henkilötietojen käsittelyä ei saisi pitää laaja-alaisena, jos käsittely koskee yksittäisen lääkärin, muun terveydenhuollon ammattilaisen tai lakimiehen asiakkaiden henkilötietoja”. On tärkeää ottaa huomioon, että vaikka johdanto-osan kappaleessa annetaan esimerkkejä asteikon ääripäistä (yksittäisen lääkärin suorittama käsittely verrattuna koko maan tai Euroopan kattavaan tietojenkäsittelyyn), niiden välillä on suuri harmaa alue. Lisäksi olisi pidettävä mielessä, että tässä johdanto-osan kappaleessa

On mahdotonta antaa sellaista käsiteltyjen tietojen tarkkaa määrää tai asianomaisten henkilöiden tarkkaa lukumäärää, joka sopisi kaikkiin tilanteisiin. Siitä huolimatta on mahdollista, että ajan kuluessa kehitetään vakiokäytäntö, jonka pohjalta määritetään nykyistä täsmällisemmin ja/tai määrällisesti se, mitä 'laajamittaisella' tarkoitetaan tietyntyyppisten yleisten käsittelytoimien yhteydessä. Tietosuojatyöryhmä aikoo osallistua tähän kehitystyöhön jakamalla ja julkaisemalla esimerkkejä kynnysarvoista, joiden ylittyminen edellyttää tietosuojavastaavan nimittämistä.

Joka tapauksessa 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 tällaisten palvelujen tarjontaan
- 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.

2.1.4 SÄÄNNÖLLINEN JA JÄRJESTELMÄLLINEN SEURANTA

Yleisessä tietosuoja-asetuksessa ei määritellä rekisteröityjen säännöllisen ja järjestelmällisen seurannan käsitettä, mutta johdanto-osan 24 kappaleessa mainitaan rekisteröityjen käyttäytymisen seuranta[15]. Tähän sisältyvät selvästi kaikenlainen seuraaminen ja profilointi internetissä, myös käyttötottumuksia seuraavaa mainontaa varten.

---

viitataan tietosuojaa koskeviin vaikutustenarviointeihin. Näin ollen jotkin kyseisen kappaleen osat saattavat liittyä juuri tähän asiayhteyteen, eivätkä ne välttämättä sovellu samalla tavoin tietosuojavastaavan nimittämiseen.

[15] "Jotta voidaan määrittää, voidaanko käsittelytoiminta katsoa rekisteröityjen käyttäytymisen seuraamiseksi, olisi varmistettava, seurataanko luonnollisia henkilöitä internetissä, mukaan lukien sellaisten henkilötietojen käsittelytekniikoiden mahdollinen myöhempi käyttö, jotka käsittävät tietyn yksilön profiloinnin erityisesti häntä koskevien päätösten tekemistä varten tai hänen henkilökohtaisten mieltymystensä, käyttäytymisensä ja asenteidensa analysointia tai ennakoimista varten."

Seurannan käsite ei kuitenkaan rajoitu pelkästään verkkoympäristöön, ja internetissä tapahtuvaa seurantaa olisi pidettävä vain yhtenä esimerkkinä rekisteröityjen käyttäytymisen seurannasta[16].

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.

Seuraavat ovat esimerkkejä toiminnoista, jotka voivat olla rekisteröityjen säännöllistä ja järjestelmällistä seurantaa: 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.

2.1.5 ERITYISET HENKILÖTIETORYHMÄT JA RIKOSTUOMIOITA TAI RIKKOMUKSIA KOSKEVAT TIEDOT

Yleisen tietosuoja-asetuksen 37 artiklan 1 kohdan c alakohdassa käsitellään 9 artiklan mukaisiin erityisiin henkilötietoryhmiin ja 10 artiklassa tarkoitettuihin rikostuomioita tai rikkomuksia koskeviin tietoihin kohdistuvaa käsittelyä. Vaikka säännöksessä käytetään ”ja”-sanaa, olemassa ei ole mitään poliittista perustetta, jonka vuoksi molempia kriteerejä olisi sovellettava samanaikaisesti. Näin ollen tekstiä olisi luettava ikään kuin siinä käytettäisiin ”tai”-sanaa.

2.2. Henkilötietojen käsittelijän tietosuojavastaava

Yleisen tietosuoja-asetuksen 37 artiklaa sovelletaan tietosuojavastaavan nimittämisen osalta sekä rekisterinpitäjiin[17] että henkilötietojen käsittelijöihin[18]. Joissain tapauksissa ainoastaan rekisterinpitäjän tai ainoastaan henkilötietojen käsittelijän on nimitettävä tietosuojavastaava, ja joissain

[16] On pantava merkille, että johdanto-osan 24 kappaleessa keskitytään yleisen tietosuoja-asetuksen ekstraterritoriaaliseen soveltamiseen. Lisäksi ilmaisujen ”rekisteröityjen käyttäytymisen seuranta” (3 artiklan 2 kohdan b alakohta) ja ”rekisteröityjen säännöllinen ja järjestelmällinen seuranta” (37 artiklan 1 kohdan b alakohta) välillä on ero, joten niiden voidaan katsoa viittaavaan eri käsitteisiin.

[17] Rekisterinpitäjä määritellään 4 artiklan 7 kohdassa henkilöksi tai elimeksi, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

[18] Henkilötietojen käsittelijä määritellään 4 artiklan 8 kohdassa henkilöksi tai elimeksi, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

tapauksissa vaatimus koskee molempia (jolloin niiden olisi tehtävä yhteistyötä). Nimittämisvelvollisuus riippuu siitä, täyttyvätkö pakollisen nimittämisen kriteerit.

On tärkeää korostaa, että vaikka rekisterinpitäjä täyttäisi pakollisen nimittämisen kriteerit, henkilötietojen käsittelijän ei välttämättä tarvitse nimittää tietosuojavastaavaa. Tällaisessa tilanteessa vapaaehtoinen nimittäminen voi kuitenkin olla hyvän käytännön mukaista.

Esimerkkejä:

- Kodinkoneiden jakelua yhdessä kaupungissa harjoittava pieni perheyritys käyttää henkilötietojen käsittelijän palveluja. Kyseisen henkilötietojen käsittelijän ydintehtävänä on tarjota verkkosivujen analytiikkapalveluja sekä kohdennettua mainontaa ja markkinointia koskevaa apua. Perheyrityksen toiminta ja asiakkaat eivät edellytä laajamittaista tietojenkäsittelyä, sillä asiakkaita on vähän ja toiminta on suhteellisen pienimuotoista. Henkilötietojen käsittelijällä on kuitenkin useita tämän pienyrityksen kaltaisia asiakkaita, joten kokonaisuutena tarkasteltuna käsittely on laajamittaista. Näin ollen henkilötietojen käsittelijän on nimitettävä tietosuojavastaava 37 artiklan 1 kohdan b alakohdan nojalla. Itse perheyrityksen ei tarvitse nimittää tietosuojavastaavaa.

- Keskisuuri laattoja valmistava yritys hankkii työterveyspalvelunsa ulkopuoliselta henkilötietojen käsittelijältä, jolla on paljon samanlaisia asiakkaita. Henkilötietojen käsittelijän on nimitettävä tietosuojavastaava 37 artiklan 1 kohdan c alakohdan nojalla, jos käsittely on laajamittaista. Laattayrityksen ei kuitenkaan välttämättä tarvitse nimittää tietosuojavastaavaa.

Henkilötietojen käsittelijän nimittämä tietosuojavastaava valvoo henkilötietoja käsittelevän organisaation toimintoja myös silloin, kun kyseinen organisaatio toimii itse rekisterinpitäjänä (esim. henkilöstöresurssit, tietotekniikka, logistiikka).

2.3. Yhden tietosuojavastaavan nimittäminen usealle organisaatiolle

Yleisen tietosuoja-asetuksen 37 artiklan 2 kohdan mukaan konserni voi nimittää yhden ainoan tietosuojavastaavan edellyttäen, että ”tietosuojavastaavaan voidaan ottaa helposti yhteyttä jokaisesta toimipaikasta”. Tällä saavutettavuuden käsitteellä viitataan tietosuojavastaavan toimintaan rekisteröityjen[19] ja valvontaviranomaisen[20] yhteyspisteenä ja myös organisaation sisäisenä yhteyspisteenä ottaen huomioon, että tietosuojavastaavan tehtävänä on muun muassa ”antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle sekä henkilötietoja käsitteleville työntekijöille tietoja ja neuvoja, jotka koskevat niiden tämän asetuksen ... mukaisia velvollisuuksia”.[21]

Riippumatta siitä, onko tietosuojavastaavana organisaation sisäinen vai ulkopuolinen henkilö, saavutettavuuden takaamiseksi on tärkeää varmistaa, että tietosuojavastaavan yhteystiedot ovat

[19] 38 artiklan 4 kohta: ”Rekisteröidyt voivat ottaa yhteyttä tietosuojavastaavaan kaikissa asioissa, jotka liittyvät heidän henkilötietojensa käsittelyyn ja tähän asetukseen perustuvien oikeuksiensa käyttöön.”

[20] 39 artiklan 1 kohdan e alakohta: ”... toimia valvontaviranomaisen yhteyspisteenä käsittelyyn liittyvissä kysymyksissä, mukaan lukien 36 artiklan mukainen ennakkokuuleminen ja tarvittaessa kuuleminen muista mahdollisista kysymyksistä”.

[21] 39 artiklan 1 kohdan a alakohta.

saatavilla yleisen tietosuoja-asetuksen vaatimusten mukaisesti.[22]

Tietosuojavastaavalla on – tarvittaessa tiimin avustuksella – oltava edellytykset olla tehokkaasti yhteydessä rekisteröityihin[23] ja tehdä yhteistyötä[24] asianomaisten valvontaviranomaisten kanssa. Tämä tarkoittaa myös sitä, että yhteyttä on pidettävä valvontaviranomaisten ja rekisteröityjen käyttämällä kielellä tai käyttämillä kielillä. Tietosuojavastaavan 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.

Yleisen tietosuoja-asetuksen 37 artiklan 3 kohdan mukaan myös usealle viranomaiselle tai julkishallinnon elimelle voidaan niiden organisaation rakenne ja koko huomioon ottaen nimittää yksi ainoa tietosuojavastaava. Tällöin sovelletaan samoja resurssi- ja yhteydenpitovaatimuksia kuin muissakin tapauksissa. Koska yhdellä tietosuojavastaavalla on tässä tapauksessa useita eri tehtäviä, rekisterinpitäjän tai henkilötietojen käsittelijän on varmistettava, että kyseinen tietosuojavastaava voi – tarvittaessa tiimin avustuksella – hoitaa tehtävänsä tehokkaasti, vaikka hänet on nimitetty useampaa viranomaista tai julkishallinnon elintä varten.

2.4. Tietosuojavastaavan saavutettavuus ja sijainti

Yleisen tietosuoja-asetuksen 4 jakson mukaan tietosuojavastaavaan on tosiasiassa voitava ottaa yhteyttä.

Tietosuojavastaavan saavutettavuuden varmistamiseksi tietosuojatyöryhmä suosittelee, että tietosuojavastaava sijaitsee Euroopan unionissa riippumatta siitä, onko rekisterinpitäjä tai henkilötietojen käsittelijä sijoittautunut EU:hun.

Joissain tilanteissa, joissa rekisterinpitäjällä tai henkilötietojen käsittelijällä ei ole toimipaikkaa EU:ssa[25], on kuitenkin mahdollista, että tietosuojavastaava voi hoitaa tehtäviään tehokkaammin EU:n ulkopuolelta.

2.5. Tietosuojavastaavan asiantuntemus ja ammattitaito

Yleisen tietosuoja-asetuksen 37 artiklan 5 kohdan mukaan ”tietosuojavastaavaa nimitettäessä otetaan huomioon henkilön ammattipätevyys ja erityisesti asiantuntemus tietosuojalainsäädännöstä ja alan käytänteistä sekä valmiudet suorittaa 39 artiklassa tarkoitetut tehtävät”. Johdanto-osan 97 kappaleen mukaan tarvittavan erityisasiantuntemuksen taso olisi määriteltävä suoritettujen tietojenkäsittelytoimien ja käsiteltävien henkilötietojen edellyttämän suojan perusteella.

[22] Ks. myös kohta 2.6 jäljempänä.

[23] 12 artiklan 1 kohta: ”Rekisterinpitäjän on toteutettava asianmukaiset toimenpiteet toimittaakseen rekisteröidylle 13 ja 14 artiklan mukaiset tiedot ja 15–22 artiklan ja 34 artiklan mukaiset kaikki käsittelyä koskevat tiedot tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä varsinkin silloin, kun tiedot on tarkoitettu erityisesti lapselle.”

[24] 39 artiklan 1 kohdan d alakohta: ”... tehdä yhteistyötä valvontaviranomaisen kanssa”.

[25] Ks. alueellista soveltamisalaa koskeva 3 artikla.

- **Asiantuntemuksen taso**

Asiantuntemuksen vaadittua tasoa ei määritellä täsmällisesti, mutta tason on oltava asianmukainen suhteessa organisaation käsittelemien tietojen arkaluonteisuuteen, monimutkaisuuteen ja määrään. Jos esimerkiksi tietojenkäsittelytoiminta on erityisen monimutkaista tai siihen liittyy suuri määrä arkaluonteisia tietoja, tietosuojavastaava voi tarvita tavallista enemmän asiantuntemusta ja tukea. Lisäksi vaadittavaan asiantuntemukseen vaikuttaa myös se, siirtääkö organisaatio henkilötietoja järjestelmällisesti Euroopan unionin ulkopuolelle vai ovatko tällaiset siirrot satunnaisia. Tietosuojavastaava olisi näin ollen valittava huolellisesti ottaen asianmukaisesti huomioon organisaation sisäiset tietosuojanäkökohdat.

- **Ammattipätevyys**

Vaikka yleisen tietosuoja-asetuksen 37 artiklan 5 kohdassa ei nimenomaisesti täsmennetä ammattipätevyyttä, joka olisi otettava huomioon tietosuojavastaavaa nimitettäessä, on olennaista, että tietosuojavastaavalla on asiantuntemusta kansallisesta ja EU:n tietosuojalainsäädännöstä ja alan käytänteistä ja että hän tuntee yleisen tietosuoja-asetuksen perusteellisesti. Lisäksi on hyödyllistä, jos valvontaviranomaiset edistävät tietosuojavastaavien riittävää ja säännöllistä koulutusta.

Asianomaisen toimialan ja rekisterinpitäjän organisaation tuntemuksesta on hyötyä. Tietosuojavastaavalla olisi lisäksi oltava hyvä käsitys kyseeseen tulevista käsittelytoimista ja tietojärjestelmistä sekä rekisterinpitäjän tietoturva- ja tietosuojatarpeista.

Viranomaisen tai julkishallinnon elimen nimittämällä tietosuojavastaavalla olisi oltava hyvä tietämys myös organisaation hallinnollisista säännöistä ja menettelyistä.

- **Valmiudet tehtävien hoitamiseen**

Valmiuksia hoitaa tietosuojavastaavalle kuuluvat tehtävät olisi tulkittava siten, että niillä viitataan sekä tietosuojavastaavan henkilökohtaisiin ominaisuuksiin ja tietämykseen että hänen asemaansa organisaatiossa. Henkilökohtaisia ominaisuuksia ovat esimerkiksi rehellisyys ja korkea ammattietiikka, sillä tietosuojavastaavan ensisijaisena päämääränä tulisi olla yleisen tietosuoja-asetuksen noudattamisen edistäminen. Tietosuojavastaavalla on keskeinen asema organisaation tietosuojakulttuurin vahvistamisessa ja yleisen tietosuoja-asetuksen olennaisten osien täytäntöönpanon varmistamisessa. Tällaisia osia ovat esimerkiksi tietojenkäsittelyn periaatteet[26], rekisteröityjen oikeudet[27], sisäänrakennettu ja oletusarvoinen tietosuoja[28], seloste käsittelytoimista[29], käsittelyn turvallisuus[30] sekä tietoturvaloukkauksista ilmoittaminen[31].

[26] II luku.
[27] III luku.
[28] 25 artikla.
[29] 30 artikla.
[30] 32 artikla.
[31] 33 ja 34 artikla.

- **Palvelusopimuksen perusteella toimiva tietosuojavastaava**

Tietosuojavastaavan tehtävän hoitaminen voi perustua myös palvelusopimukseen, joka tehdään rekisterinpitäjän tai henkilötietojen käsittelijän organisaation ulkopuolisen henkilön tai organisaation kanssa. Jos sopimus tehdään organisaation kanssa, on välttämätöntä, että jokainen tietosuojavastaavan tehtäviä hoitava organisaation jäsen täyttää kaikki yleisen tietosuoja-asetuksen 4 jakson sovellettavat vaatimukset (on esimerkiksi tärkeää, ettei kenelläkään ole eturistiriitaa). Yhtä lailla on tärkeää, että jokaisella tällaisella jäsenellä on yleisen tietosuoja-asetuksen säännösten mukainen suoja (esim. tietosuojavastaavan tehtäviä koskevaa palvelusopimusta ei saa päättää perusteettomasti eikä kyseisiä tehtäviä hoitavaa organisaation jäsentä saa perusteettomasti erottaa). Toisaalta eri työntekijöiden taitoja ja vahvuuksia voidaan yhdistää siten, että useat henkilöt voivat tiiminä palvella asiakkaitaan tehokkaammin.

Oikeusvarmuuden ja hyvän organisoinnin varmistamiseksi sekä tiimin jäsenten eturistiriitojen ehkäisemiseksi on suositeltavaa, että tehtävät jaetaan tietosuojavastaavan tiimissä selkeästi ja että kullekin asiakkaalle nimetään yksi henkilö ensisijaiseksi yhteyshenkilöksi ja vastuuhenkilöksi. Nämä näkökohdat olisi yleisesti ottaen hyvä täsmentää palvelusopimuksessa.

2.6. Tietosuojavastaavan yhteystietojen julkistaminen ja ilmoittaminen

Yleisen tietosuoja-asetuksen 37 artiklan 7 kohdassa vaaditaan rekisterinpitäjää tai henkilötietojen käsittelijää

- julkistamaan tietosuojavastaavan henkilötiedot ja
- ilmoittamaan ne asianomaisille valvontaviranomaisille.

Näiden vaatimusten tarkoituksena on varmistaa, että rekisteröidyt (sekä organisaatiossa että sen ulkopuolella) ja valvontaviranomaiset voivat ottaa helposti suoraan yhteyttä tietosuojavastaavaan ilman yhteydenottoa organisaation muuhun osaan. Luottamuksellisuus on yhtä tärkeää: esimerkiksi työntekijät eivät välttämättä halua tehdä valitusta tietosuojavastaavalle, jos ilmoituksen luottamuksellisuutta ei taata.
Tietosuojavastaavaa sitoo tietosuojavastaavan tehtävien hoitamista koskeva salassapitovelvollisuus unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti (38 artiklan 5 kohta).

Tietosuojavastaavan yhteystietojen olisi sisällettävä tiedot, joiden avulla rekisteröidyt ja valvontaviranomainen voivat helposti tavoittaa tietosuojavastaavan (tietosuojavastaavan postiosoite, puhelinnumero ja/tai sähköpostiosoite). Yleisön kanssa viestimiseen voidaan tarvittaessa käyttää myös muita viestintäkanavia, kuten erityistä palvelupuhelinta tai organisaation verkkosivulla olevaa tietosuojavastaavalle osoitettua yhteydenottolomaketta.

Asetuksen 37 artiklan 7 kohdassa ei edellytetä, että julkistettavissa yhteystiedoissa ilmoitetaan tietosuojavastaavan nimi. Vaikka nimen ilmoittaminen voi olla hyvän käytännön mukaista, rekisterinpitäjä tai henkilötietojen käsittelijä sekä tietosuojavastaava päättävät, onko tämä tarpeellista tai hyödyllistä asianomaisissa olosuhteissa.[32]

[32] Olisi huomattava, että toisin kuin 37 artiklan 7 kohdassa, 33 artiklan 3 kohdan b alakohdassa, jossa kuvataan valvontaviranomaiselle ja rekisteröidyille henkilötietojen tietoturvaloukkauksen sattuessa annettavia tietoja, vaaditaan nimenomaisesti ilmoittamaan myös tietosuojavastaavan nimi (eikä pelkästään yhteystietoja).

Tietosuojavastaavan nimi on kuitenkin välttämätöntä ilmoittaa valvontaviranomaiselle, jotta tietosuojavastaava voi toimia organisaation ja valvontaviranomaisen välisenä yhteyspisteenä (39 artiklan 1 kohdan e alakohta).

Lisäksi tietosuojatyöryhmä suosittelee hyvänä käytäntönä, että organisaatio ilmoittaa työntekijöilleen tietosuojavastaavan nimen ja yhteystiedot. Nämä tiedot voidaan julkistaa organisaatiossa esimerkiksi intranetissä, sisäisessä puhelinluettelossa ja organisaatiokaaviossa.

3 Tietosuojavastaavan asema

3.1. Tietosuojavastaavan osallistuminen kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn

Yleisen tietosuoja-asetuksen 38 artiklan mukaan rekisterinpitäjän ja henkilötietojen käsittelijän on varmistettava, että tietosuojavastaava ”otetaan asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn”.

On ratkaisevan tärkeää, että tietosuojavastaava tai hänen tiiminsä otetaan mahdollisimman aikaisessa vaiheessa mukaan kaikkien tietosuojakysymysten käsittelyyn. Tietosuojaa koskevien vaikutustenarviointien osalta yleisessä tietosuoja-asetuksessa säädetään nimenomaisesti tietosuojavastaavan varhaisesta mukanaolosta ja täsmennetään, että tällaista vaikutustenarviointia tehdessään rekisterinpitäjän on pyydettävä neuvoja tietosuojavastaavalta.[33] Varmistamalla, että tietosuojavastaava pidetään ajan tasalla ja että häneltä pyydetään neuvoja alusta lähtien, helpotetaan yleisen tietosuoja-asetuksen noudattamista ja edistetään sisäänrakennettua yksityisyyden suojaa koskevaa lähestymistapaa. Tällaisen käytännön olisi näin ollen oltava vakiomenettely organisaation hallinnossa. Lisäksi on tärkeää nähdä tietosuojavastaava keskustelukumppanina organisaatiossa ja varmistaa, että hän kuuluu työryhmiin, jotka käsittelevät organisaation tietojenkäsittelytoimia.

Näin ollen organisaation olisi noudatettava muun muassa seuraavia toimintatapoja:

- Tietosuojavastaava kutsutaan säännöllisesti ylemmän tai keskitason johdon kokouksiin.
- Hänen läsnäolonsa on suositeltavaa tehtäessä päätöksiä, joilla on vaikutusta tietosuojaan. Kaikki olennaiset tiedot toimitetaan tietosuojavastaavalle viipymättä, jotta hän voi antaa asianmukaisia neuvoja.
- Tietosuojavastaavan näkemykselle annetaan aina asianmukainen painoarvo. Erimielisyystilanteessa tietosuojatyöryhmä suosittelee hyvänä käytäntönä dokumentoimaan perusteet, joiden vuoksi tietosuojavastaavan neuvoa ei noudateta.
- Tietosuojavastaavaa kuullaan nopeasti, jos ilmenee tietoturvaloukkaus tai muu ongelma.

Rekisterinpitäjä tai henkilötietojen käsittelijä voi tarvittaessa laatia tietosuojaa koskevia ohjeita tai ohjelmia, joissa ilmoitetaan, milloin tietosuojavastaavaa on kuultava.

[33] 35 artiklan 2 kohta.

3.2. Tarvittavat resurssit

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”. Erityisesti on otettava huomioon seuraavat näkökohdat:

- Ylempi johto (esim. yhtiön hallitus) tukee aktiivisesti tietosuojavastaavan tehtävää.
- Tietosuojavastaavalle varataan riittävästi aikaa tehtävien hoitamiseen. Tämä on erityisen tärkeää silloin, kun nimitetään osa-aikainen sisäinen tietosuojavastaava tai kun ulkoinen tietosuojavastaava hoitaa tietosuojatehtäviä muiden tehtäviensä ohella. Vastakkaiset prioriteetit voivat muutoin johtaa tietosuojavastaavan tehtävien laiminlyöntiin. Tietosuojavastaavan tehtäville on ensisijaisen tärkeää varata riittävästi aikaa. Jos tietosuojavastaava ei hoida tehtäviään kokoaikaisesti, on hyvän käytännön mukaista määrittää prosenttiosuus ajasta, joka käytetään tietosuojavastaavan tehtävän hoitamiseen. Lisäksi on hyvän käytännön mukaista määrittää tehtävän hoitamiseen tarvittava aika ja tietosuojavastaavan tehtävien asianmukainen prioriteettitaso, minkä lisäksi tietosuojavastaavan (tai organisaation) on hyvä laatia työsuunnitelma.
- Tietosuojavastaavalle järjestetään riittävästi tukea eli varoja, infrastruktuuri (tilat, palvelut, laitteet) ja tarvittaessa henkilöstö.
- Tietosuojavastaavan nimittämisestä ilmoitetaan virallisesti koko henkilöstölle, jotta varmistetaan, että tietosuojavastaavan olemassaolo ja tehtävä ovat organisaation tiedossa.
- Tietosuojavastaavalle järjestetään tarvittaessa pääsy muihin palveluihin (esim. henkilöstöresurssit, oikeudellinen neuvonta, tietotekniikka ja turvallisuus), jotta hän voi saada niiltä olennaista tukea ja tietoa.
- Tietosuojavastaavalle tarjotaan jatkuvasti koulutusta. Tietosuojavastaavalle on annettava mahdollisuus pysyä ajan tasalla tietosuoja-alan kehityksestä. Tavoitteena tulisi olla tietosuojavastaavan asiantuntemuksen jatkuva lisääminen, ja tietosuojavastaavaa olisi kannustettava osallistumaan tietosuojaa koskeville kursseille ja muunlaiseen ammatilliseen kehittämiseen, kuten yksityisyyttä käsitteleviin foorumeihin ja työpajoihin.
- Organisaation koosta ja rakenteesta riippuen voi olla tarpeen perustaa tietosuojavastaavan tiimi (eli tietosuojavastaava ja hänen henkilöstönsä). Tällöin tiimin sisäinen rakenne sekä kunkin jäsenen tehtävät ja vastuualueet olisi määriteltävä selkeästi. Vastaavasti jos tietosuojavastaavan tehtävää hoitaa ulkoinen palveluntarjoaja, kyseiselle palveluntarjoajalle työskentelevien henkilöiden ryhmä voi käytännössä hoitaa tietosuojavastaavan tehtävää tiiminä asiakkaalle nimetyn ensisijaisen yhteyshenkilön alaisuudessa.

Yleisesti ottaen mitä monimutkaisempia ja/tai arkaluonteisempia käsittelytoimet ovat, sitä enemmän tietosuojavastaavalle on varattava resursseja. Tietosuojavastaavan tehtävän on oltava vaikutuksiltaan tehokas ja riittävästi resursoitu suhteessa suoritettavaan tietojenkäsittelyyn.

3.3. Ohjeet ja valmiudet ”suorittaa velvollisuutensa ja tehtävänsä riippumattomasti”

Yleisen tietosuoja-asetuksen 38 artiklan 3 kohdassa vahvistetaan joitakin perustakeita, joiden avulla varmistetaan, että tietosuojavastaava voi hoitaa tehtävänsä organisaatiossa riittävän riippumattomasti. Rekisterinpitäjien tai henkilötietojen käsittelijöiden on erityisesti varmistettava, ettei tietosuojavastaava ”ota vastaan ohjeita [tehtäviensä] hoitamisen yhteydessä”. Johdanto-osan

97 kappaleessa lisätään, että tietosuojavastaavan ”olisi voitava suorittaa velvollisuutensa ja tehtävänsä riippumattomasti, olipa hän palvelussuhteessa rekisterinpitäjään tai ei”.

Tämä tarkoittaa, että tietosuojavastaavan hoitaessa 39 artiklan mukaisia tehtäviään hänelle ei saa antaa ohjeita asian käsittelystä, kuten siitä, mitä tuloksia olisi saavutettava, miten valitus olisi tutkittava tai onko syytä kuulla valvontaviranomaista. Tietosuojavastaavaa ei myöskään saa ohjeistaa suhtautumaan tietosuojalainsäädäntöön liittyvään kysymykseen tietyllä tavalla, kuten tulkitsemaan lainsäädäntöä tietyllä tavalla.

Tietosuojavastaavan riippumattomuus ei kuitenkaan tarkoita sitä, että hänellä on laajemmat päätöksentekovaltuudet kuin on tarpeen 39 artiklassa tarkoitettujen tehtävien hoitamiseksi.

Rekisterinpitäjä tai henkilötietojen käsittelijä vastaa edelleen tietosuojalainsäädännön noudattamisesta, ja sen on voitava osoittaa lainsäädännön noudattaminen.[34] Jos rekisterinpitäjä tai henkilötietojen käsittelijä tekee päätöksiä, jotka eivät ole yleisen tietosuoja-asetuksen ja tietosuojavastaavan neuvojen mukaisia, tietosuojavastaavalle olisi annettava tilaisuus esittää eriävä mielipiteensä ylimmälle johdolle ja päätöksentekijöille. Tältä osin 38 artiklan 3 kohdassa säädetään, että tietosuojavastaava ”raportoi suoraan rekisterinpitäjän tai henkilötietojen käsittelijän ylimmälle johdolle”. Suoralla raportoinnilla varmistetaan, että ylempi johto (esim. yhtiön hallitus) on tietoinen neuvoista ja suosituksista, jotka tietosuojavastaava on antanut osana tehtäväänsä antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle tietoja ja neuvoja. Toinen esimerkki suorasta raportoinnista on ylimmälle johdolle laadittava tietosuojavastaavan vuotuinen toimintakertomus.

3.4. Tietosuojavastaavan erottaminen tai rankaiseminen tehtävien hoitamisen vuoksi

Yleisen tietosuoja-asetuksen 38 artiklan 3 kohdan mukaan ”rekisterinpitäjä tai henkilötietojen käsittelijä ei saa erottaa tai rangaista tietosuojavastaavaa sen vuoksi, että hän on hoitanut tehtäviään”.

Tämä vaatimus vahvistaa tietosuojavastaavan riippumattomuutta ja auttaa varmistamaan, että tietosuojavastaava toimii itsenäisesti ja että hänellä on riittävä suoja tietosuojatehtäviä hoitaessaan.

Rangaistukset kielletään yleisen tietosuoja-asetuksen nojalla ainoastaan silloin, kun ne määrätään sen vuoksi, että tietosuojavastaava on hoitanut tehtäviään. Tietosuojavastaava voi esimerkiksi katsoa, että tietty käsittely aiheuttaa todennäköisesti suuren riskin, ja neuvoa rekisterinpitäjää tai henkilötietojen käsittelijää tekemään tietosuojaa koskevan vaikutustenarvioinnin, mutta rekisterinpitäjä tai henkilötietojen käsittelijä on asiasta eri mieltä. Tällaisessa tilanteessa tietosuojavastaavaa ei saa erottaa sen vuoksi, että hän on antanut kyseisen neuvon.

Rangaistukset voivat olla erilaisia, ja ne voivat olla suoria tai välillisiä. Rangaistus voi olla esimerkiksi ylennyksen tekemättä jättäminen tai viivästyminen, urakehityksen estäminen tai sellaisten etuuksien epääminen, joita muut työntekijät saavat. Näiden rangaistusten ei tarvitse tosiasiallisesti toteutua, vaan pelkkä uhka riittää edellyttäen, että sitä käytetään rankaisemaan tietosuojavastaavaa tehtäviensä hoitamisesta.

[34] 5 artiklan 2 kohta.

Jos erottaminen toteutetaan tavanomaisena johdon määräyksenä ja ehdoin, jotka kansallisen sopimuslainsäädännön tai työ- tai rikoslainsäädännön nojalla koskevat myös kaikkia muita työntekijöitä tai toimeksisaajia, tietosuojavastaava voidaan erottaa lainmukaisesti perustein, jotka eivät liity hänen tehtäviensä hoitamiseen (esim. varkauden, fyysisen, psyykkisen tai seksuaalisen häirinnän tai vastaavan vakavan rikkomuksen vuoksi).

Tässä yhteydessä on pantava merkille, että yleisessä tietosuoja-asetuksessa ei täsmennetä, miten ja milloin tietosuojavastaava voidaan erottaa tai korvata toisella henkilöllä. Mitä pysyvämpi tietosuojavastaavan sopimus on ja mitä enemmän perusteetonta erottamista vastaan on olemassa takeita, sitä todennäköisemmin tietosuojavastaava voi toimia riippumattomasti. Näin ollen tietosuojatyöryhmä kannustaa organisaatioita pyrkimään tällaiseen tilanteeseen.

3.5. Eturistiriidat

Yleisen tietosuoja-asetuksen 38 artiklan 6 kohdan mukaan tietosuojavastaava voi ”suorittaa muita tehtäviä ja velvollisuuksia”. Organisaation on tällöin kuitenkin varmistettava, että ”tällaiset tehtävät ja velvollisuudet eivät aiheuta eturistiriitoja”.

Eturistiriitojen välttäminen liittyy läheisesti vaatimukseen toimia riippumattomasti. Vaikka tietosuojavastaava voi hoitaa myös muita tehtäviä, hänelle voidaan antaa tällaisia muita tehtäviä ja velvollisuuksia ainoastaan edellyttäen, etteivät ne aiheuta eturistiriitoja. Tämä tarkoittaa erityisesti sitä, että 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 organisaatiossa, mutta sama koskee myös muita tehtäviä organisaatiorakenteen alemmilla tasoilla, jos näissä tehtävissä on määritettävä tietojenkäsittelyn tarkoitukset ja keinot. Lisäksi eturistiriita voi syntyä esimerkiksi silloin, kun ulkoista tietosuojavastaavaa pyydetään edustamaan rekisterinpitäjää tai henkilötietojen käsittelijää tuomioistuimessa tietosuojaa koskevissa kysymyksissä.

Organisaation toiminnasta, koosta ja rakenteesta riippuen rekisterinpitäjien tai henkilötietojen käsittelijöiden voi olla hyvän käytännön mukaista

- yksilöidä ne toimet, jotka eivät sovi yhteen tietosuojavastaavan tehtävien kanssa
- laatia asiaa koskevia sisäisiä sääntöjä eturistiriitojen välttämiseksi
- laatia yleinen selitys eturistiriidoista
- lisätä tietoisuutta tästä vaatimuksesta ilmoittamalla, ettei organisaation tietosuojavastaavalla ole tehtäviensä osalta eturistiriitaa
- sisällyttää organisaation sisäisiin sääntöihin suojatoimia ja varmistaa, että tietosuojavastaavan tointa koskeva työpaikkailmoitus tai palvelusopimus on riittävän tarkka ja yksityiskohtainen, jotta vältetään eturistiriidat. Tässä yhteydessä olisi lisäksi muistettava, että eturistiriitojen luonne voi vaihdella sen mukaan, rekrytoidaanko tietosuojavastaava organisaation sisältä vai ulkopuolelta.

4 Tietosuojavastaavan tehtävät

4.1. Yleisen tietosuoja-asetuksen noudattamisen seuraaminen

Yleisen tietosuoja-asetuksen 39 artiklan 1 kohdan b alakohdan mukaan tietosuojavastaavan tehtäviin kuuluu muun muassa asetuksen noudattamisen seuraaminen. Johdanto-osan 97 kappaleessa täsmennetään, että ”rekisterinpitäjällä tai henkilötietojen käsittelijällä on oltava apunaan [tietosuojavastaava], ... joka valvoo tämän asetuksen noudattamista”.

Osana asetuksen noudattamisen seuraamista tietosuojavastaava voi erityisesti

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

Noudattamisen seuraaminen ei kuitenkaan tarkoita sitä, että tietosuojavastaava olisi henkilökohtaisesti vastuussa asetuksen noudattamatta jättämisestä. Yleisessä tietosuoja-asetuksessa todetaan selvästi, että rekisterinpitäjän – ei siis tietosuojavastaavan – ”on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tätä asetusta” (24 artiklan 1 kohta). Tietosuojasääntöjen noudattaminen on näin rekisterinpitäjän organisaation eikä tietosuojavastaavan vastuulla.

4.2. Tietosuojavastaavan rooli tietosuojaa koskevissa vaikutustenarvioinneissa

Yleisen tietosuoja-asetuksen 35 artiklan 1 kohdan mukaan rekisterinpitäjän – ei siis tietosuojavastaavan – tehtävänä on tarvittaessa tehdä tietosuojaa koskeva vaikutustenarviointi. Tietosuojavastaava voi kuitenkin avustaa rekisterinpitäjää erittäin tärkeällä ja hyödyllisellä tavalla. Sisäänrakennettua tietosuojaa koskevan periaatteen mukaisesti 35 artiklan 2 kohdassa vaaditaan erityisesti, että tietosuojaa koskevaa vaikutustenarviointia tehdessään rekisterinpitäjän ”on pyydettävä neuvoja” tietosuojavastaavalta. Asetuksen 39 artiklan 1 kohdan c alakohdassa puolestaan annetaan tietosuojavastaavalle tehtäväksi ”antaa pyydettäessä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoa sen toteutusta 35 artiklan mukaisesti”.

Tietosuojatyöryhmä suosittelee, että rekisterinpitäjä pyytää tietosuojavastaavalta neuvoja muun muassa seuraavissa kysymyksissä[35]:

- 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

[35] Asetuksen 39 artiklan 1 kohdassa luetellaan tietosuojavastaavan tehtävät ja todetaan, että tietosuojavastaavalla on oltava ”*ainakin*” luetellut tehtävät. Näin ollen rekisterinpitäjä voi antaa tietosuojavastaavalle muita tehtäviä, joita ei nimenomaisesti mainita 39 artiklan 1 kohdassa, tai täsmentää tehtäviä tarkemmin.

- onko tietosuojaa koskeva vaikutustenarviointi toteutettu oikein ja vastaavatko sen päätelmät (päätös siitä, aloitetaanko käsittely, ja käyttöön otettavat suojatoimet) yleisen tietosuoja-asetuksen vaatimuksia.

Jos rekisterinpitäjä on eri mieltä tietosuojavastaavan antamista neuvoista, tietosuojaa koskevan vaikutustenarvioinnin asiakirjoissa olisi perusteltava kirjallisesti, miksi neuvoja ei ole noudatettu.[36]

Tietosuojatyöryhmä suosittelee lisäksi, että rekisterinpitäjä ilmoittaa selvästi – esimerkiksi tietosuojavastaavan sopimuksessa sekä työntekijöille ja johdolle (sekä tarvittaessa muille sidosryhmille) annetuissa tiedoissa – tietosuojavastaavan täsmälliset tehtävät ja niiden laajuuden, erityisesti tietosuojaa koskevan vaikutustenarvioinnin toteutuksen osalta.

4.3. Yhteistyö valvontaviranomaisen kanssa ja yhteyspisteenä toimiminen

Yleisen tietosuoja-asetuksen 39 artiklan 1 kohdan d ja e alakohdan mukaan tietosuojavastaavan tehtävänä on ”tehdä yhteistyötä valvontaviranomaisen kanssa” ja ”toimia valvontaviranomaisen yhteyspisteenä käsittelyyn liittyvissä kysymyksissä, mukaan lukien 36 artiklan mukainen ennakkokuuleminen ja tarvittaessa kuuleminen muista mahdollisista kysymyksistä”.

Näissä tehtävissä viitataan tietosuojavastaavan rooliin ”välittäjänä”, joka mainitaan näiden ohjeiden johdannossa. Tietosuojavastaava toimii yhteyshenkilönä, joka auttaa valvontaviranomaista saamaan käyttöönsä asiakirjoja ja tietoja, jotta valvontaviranomainen voi hoitaa 57 artiklassa mainitut tehtävät ja käyttää 58 artiklassa mainittuja tutkintavaltuuksia, korjaavia toimivaltuuksia sekä hyväksymis- ja neuvontavaltuuksia. Kuten edellä on todettu, tietosuojavastaavaa sitoo tietosuojavastaavan tehtävien hoitamista koskeva salassapitovelvollisuus unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti (38 artiklan 5 kohta). Salassapitovelvollisuus ei kuitenkaan estä tietosuojavastaavaa ottamasta yhteyttä valvontaviranomaiseen ja pyytämästä tältä neuvoja. Asetuksen 39 artiklan 1 kohdan e alakohdassa säädetään, että tietosuojavastaava voi tarvittaessa kuulla valvontaviranomaista muista mahdollisista kysymyksistä.

[36] Asetuksen 24 artiklan 1 kohdassa säädetään seuraavaa: ”Ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja **osoittaa**, että käsittelyssä noudatetaan tätä asetusta. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa.”

4.4. Riskiperusteinen lähestymistapa

Yleisen tietosuoja-asetuksen 39 artiklan 2 kohdan mukaan tietosuojavastaavan on ”otettava asianmukaisesti huomioon käsittelytoimiin liittyvä riski ottaen samalla huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset”.

Tässä artiklassa muistutetaan yleisestä ja järkevästä periaatteesta, jolla voi olla merkitystä tietosuojavastaavan päivittäisen työn useilla osa-alueilla. Pohjimmiltaan siinä vaaditaan, että tietosuojavastaava priorisoi toimiaan ja keskittyy työssään kysymyksiin, jotka aiheuttavat tavallista suurempia tietosuojariskejä. Tämä ei tarkoita sitä, että tietosuojavastaavan tulisi laiminlyödä säännösten noudattamisen seuraaminen sellaisissa tietojenkäsittelytoimissa, jotka aiheuttavat verrattain pieniä riskejä, vaan se tarkoittaa sitä, että tietosuojavastaavan tulisi keskittyä ensisijaisesti suuririskisiin osa-alueisiin.

Tämän valikoivan ja käytännönläheisen lähestymistavan on tarkoitus auttaa tietosuojavastaavaa antamaan rekisterinpitäjälle neuvoja siitä, mitä menetelmiä tietosuojaa koskevaa vaikutustenarviointia tehtäessä olisi käytettävä, millä aloilla olisi toteutettava sisäinen tai ulkoinen tietosuojaa koskeva tarkastus, mitä sisäistä koulutusta olisi tarjottava tietojenkäsittelystä vastaavalle henkilöstölle tai johdolle ja mihin käsittelytoimiin on syytä varata tavallista enemmän tietosuojavastaavan aikaa ja resursseja.

4.5. Tietosuojavastaavan rooli selosteen ylläpidossa

Yleisen tietosuoja-asetuksen 30 artiklan 1 ja 2 kohdan nojalla rekisterinpitäjän tai henkilötietojen käsittelijän – ei siis tietosuojavastaavan – on ”ylläpidettävä selostetta vastuullaan olevista käsittelytoimista” tai ”ylläpidettävä selostetta kaikista rekisterinpitäjän lukuun suoritettavista käsittelytoimista”.

Käytännössä tietosuojavastaava laatii usein luetteloita ja pitää rekisteriä käsittelytoimista niiden tietojen perusteella, joita henkilötietojen käsittelystä vastaavat organisaation eri osastot hänelle toimittavat. Tämä käytäntö on vahvistettu useissa voimassa olevissa kansallisissa säädöksissä sekä EU:n toimielimiin ja elimiin sovellettavissa tietosuojasäännöissä[37].

Yleisen tietosuoja-asetuksen 39 artiklan 1 kohdassa annetaan luettelo tehtävistä, jotka tietosuojavastaavalla on vähintään oltava. Mikään ei näin ollen estä rekisterinpitäjää tai henkilötietojen käsittelijää antamasta tietosuojavastaavalle tehtäväksi ylläpitää selostetta rekisterinpitäjän tai henkilötietojen käsittelijän 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.

Asetuksen 30 artiklan nojalla ylläpidettävää selostetta olisi kuitenkin pidettävä myös työkaluna, jonka ansiosta rekisterinpitäjä ja valvontaviranomainen voivat pyynnöstä saada yleiskatsauksen kaikista organisaation suorittamista henkilötietojen käsittelytoimista. Sitä tarvitaan näin säännösten noudattamiseksi, ja sillä edistetään sen vuoksi tehokkaasti tilivelvollisuuden noudattamista.

[37] Asetuksen (EY) N:o 45/2001 24 artiklan 1 kohdan d alakohta.

5 LIITE – TIETOSUOJAVASTAAVAA KOSKEVAT OHJEET: TÄRKEITÄ TIETOJA

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

1 Minkä organisaatioiden on nimitettävä tietosuojavastaava?

Tietosuojavastaavan nimittäminen on pakollista, jos

- 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. Vaikka tietosuojavastaavan nimittäminen ei olisi pakollista, organisaatioiden voi olla hyödyllistä nimittää tietosuojavastaava vapaaehtoisesti. Tietosuojatyöryhmä kannustaa tällaista vapaaehtoista nimittämistä. Jos organisaatio nimittää tietosuojavastaavan vapaaehtoisesti, tietosuojavastaavan nimittämiseen, asemaan ja tehtäviin sovelletaan samoja vaatimuksia kuin tilanteessa, jossa nimittäminen on pakollista.

Lähde: Yleisen tietosuoja-asetuksen 37 artiklan 1 kohta

2 Mitä ’ydintehtävillä’ tarkoitetaan?

’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 esimerkkejä organisaation ydintehtävien tai keskeisen liiketoiminnan tarpeellisista tukitoiminnoista. Vaikka nämä toiminnot ovat tarpeellisia tai välttämättömiä, niitä pidetään yleensä ydintehtävien sijaan oheistoimintoina.

Lähde: Yleisen tietosuoja-asetuksen 37 artiklan 1 kohdan b ja c alakohta

3 Mitä ’laajamittaisella’ tarkoitetaan?

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.

Lähde: Yleisen tietosuoja-asetuksen 37 artiklan 1 kohdan b ja c alakohta

4 Mitä ’säännöllisellä ja järjestelmällisellä seurannalla’ tarkoitetaan?

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.

Seuraavat ovat esimerkkejä toiminnoista, jotka voivat olla rekisteröityjen säännöllistä ja järjestelmällistä seurantaa: 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.

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.

Lähde: Yleisen tietosuoja-asetuksen 37 artiklan 1 kohdan b alakohta

5 Voivatko organisaatiot nimittää yhteisen tietosuojavastaavan? Jos voivat, millä edellytyksin?

Kyllä. 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 tietosuojavastaavana organisaation sisäinen vai ulkopuolinen henkilö, saavutettavuuden takaamiseksi on tärkeää varmistaa, että tietosuojavastaavan yhteystiedot ovat saatavilla. Tietosuojavastaavalla on – tarvittaessa tiimin avustuksella – 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 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.

Myös usealle viranomaiselle tai julkishallinnon elimelle voidaan niiden organisaation rakenne ja koko huomioon ottaen nimittää yksi ainoa tietosuojavastaava. Tällöin sovelletaan samoja resurssi- ja yhteydenpitovaatimuksia kuin muissakin tapauksissa. Koska yhdellä tietosuojavastaavalla on tässä tapauksessa useita eri tehtäviä, rekisterinpitäjän tai henkilötietojen käsittelijän on varmistettava, että kyseinen tietosuojavastaava voi – tarvittaessa tiimin avustuksella – hoitaa tehtävänsä tehokkaasti, vaikka hänet on nimitetty useampaa viranomaista tai julkishallinnon elintä varten.

Lähde: Yleisen tietosuoja-asetuksen 37 artiklan 2 ja 3 kohta

6 Missä tietosuojavastaan pitäisi sijaita?

Tietosuojavastaavan saavutettavuuden varmistamiseksi tietosuojatyöryhmä suosittelee, että tietosuojavastaava sijaitsee Euroopan unionissa riippumatta siitä, onko rekisterinpitäjä tai henkilötietojen käsittelijä sijoittautunut EU:hun. Joissain tilanteissa, joissa rekisterinpitäjällä tai henkilötietojen käsittelijällä ei ole toimipaikkaa EU:ssa, on kuitenkin mahdollista, että tietosuojavastaava voi hoitaa tehtäviään tehokkaammin EU:n ulkopuolelta.

7 Onko mahdollista nimittää ulkoinen tietosuojavastaava?

Kyllä. 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.

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 sovellettavat vaatimukset.

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

Lähde: Yleisen tietosuoja-asetuksen 37 artiklan 6 kohta

8 Millainen ammattipätevyys tietosuojavastaavalla tulisi olla?

Tietosuojavastaavaa nimitettäessä on otettava huomioon henkilön ammattipätevyys ja erityisesti asiantuntemus tietosuojalainsäädännöstä ja alan käytänteistä sekä valmiudet hoitaa hänelle osoitetut 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.

Tietosuojavastaavan 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.

Lähde: Yleisen tietosuoja-asetuksen 37 artiklan 5 kohta

9 Mitä resursseja rekisterinpitäjän tai henkilötietojen käsittelijän olisi järjestettävä tietosuojavastaavalle?

Tietosuojavastaavalla on oltava tarvittavat resurssit tehtäviensä hoitamiseen.

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.

Lähde: Yleisen tietosuoja-asetuksen 38 artiklan 2 kohta

10 Millä suojatoimilla voidaan varmistaa, että tietosuojavastaava hoitaa tehtävänsä riippumattomasti? Mitä 'eturistiriidalla' tarkoitetaan?

Olemassa on useita suojatoimia, joilla varmistetaan, että tietosuojavastaava voi toimia riippumattomasti:

- 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.

Tietosuojavastaavan muut tehtävät ja velvollisuudet eivät saa aiheuttaa eturistiriitaa. Tämä tarkoittaa ensinnäkin sitä, että 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 organisaatiossa, mutta sama koskee myös muita tehtäviä organisaatiorakenteen alemmilla tasoilla, jos näissä tehtävissä on määritettävä tietojenkäsittelyn tarkoitukset ja keinot. Lisäksi eturistiriita voi syntyä esimerkiksi silloin, jos ulkoista tietosuojavastaavaa pyydetään edustamaan rekisterinpitäjää tai henkilötietojen käsittelijää tuomioistuimessa tietosuojaa koskevissa kysymyksissä.

Lähde: Yleisen tietosuoja-asetuksen 38 artiklan 3 ja 6 kohta

11 Mitä ’noudattamisen seuraamisella’ tarkoitetaan?

Osana asetuksen noudattamisen seuraamista tietosuojavastaava voi erityisesti

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

Lähde: Yleisen tietosuoja-asetuksen 39 artiklan 1 kohdan b alakohta

12 Onko tietosuojavastaava henkilökohtaisesti vastuussa tietosuojavaatimusten noudattamatta jättämisestä?

Ei. Tietosuojavastaava ei vastaa henkilökohtaisesti siitä, että tietosuojavaatimuksia ei noudateta. Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava varmistaa ja osoittaa, että käsittelyssä noudatetaan asetuksen säännöksiä. Tietosuojasääntöjen noudattaminen on näin rekisterinpitäjän tai henkilötietojen käsittelijän vastuulla.

13 Mikä rooli tietosuojavastaavalla on tietosuojaa koskevien vaikutustenarviointien ja käsittelytoimia koskevan selosteen 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) tietosuojavaatimuksia.

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 tai henkilötietojen käsittelijän 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.

Lähde: Yleisen tietosuoja-asetuksen 39 artiklan 1 kohdan c alakohta ja 30 artikla

Tehty Brysselissä 13. joulukuuta 2016

Tietosuojatyöryhmän puolesta
Puheenjohtaja

Isabelle FALQUE-PIERROTIN

Viimeksi tarkistettu ja hyväksytty 5. huhtikuuta 2017

Tietosuojatyöryhmän puolesta
Puheenjohtaja

Isabelle FALQUE-PIERROTIN