TIETOSUOJATYÖRYHMÄ

17/FI

WP 248 rev.01

Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu "korkea riski"

Annettu 4. huhtikuuta 2017

Viimeksi tarkistettu ja hyväksytty 4. lokakuuta 2017

TIETOSUOJATYÖRYHMÄ, joka

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

ottaa huomioon mainitun direktiivin 29 ja 30 artiklan,

ottaa huomioon työjärjestyksensä,

ON ANTANUT SEURAAVAT OHJEET:

Sisällysluettelo

I. JOHDANTO 4

II. OHJEIDEN SOVELTAMISALA 5

III. TIETOSUOJAA KOSKEVA VAIKUTUSTENARVIOINTI: ASETUKSEN SELVENTÄMINEN 7

A. MITÄ TIETOSUOJAA KOSKEVASSA VAIKUTUSTENARVIOINNISSA KÄSITELLÄÄN? YHTÄ KÄSITTELYTOINTA TAI USEITA SAMANKALTAISIA KÄSITTELYTOIMIA. 8

B. MILLE KÄSITTELYTOIMILLE ON TEHTÄVÄ TIETOSUOJAA KOSKEVA VAIKUTUSTENARVIOINTI? LUKUUN OTTAMATTA POIKKEUKSIA ARVIOINTI ON TEHTÄVÄ SILLOIN, KUN KÄSITTELY ”*TODENNÄKÖISESTI AIHEUTTAA ... KORKEAN RISKIN*” 9

a) Milloin tietosuojaa koskeva vaikutustenarviointi on pakollinen? Se on pakollinen silloin, kun käsittely ”todennäköisesti aiheuttaa ... korkean riskin”. 9

b) Milloin tietosuojaa koskevaa vaikutustenarviointia ei vaadita? Sitä ei vaadita, kun ei katsota, että käsittely ”todennäköisesti aiheuttaa ... korkean riskin” tai kun samankaltainen vaikutustenarviointi on jo olemassa, käsittelylle on annettu hyväksyntä ennen toukokuuta 2018, käsittelyllä on oikeusperusta tai se sisältyy niiden käsittelytoimien luetteloon, joiden yhteydessä ei vaadita vaikutustenarviointia. 14

C. MITEN MENETELLÄÄN JO KÄYTÖSSÄ OLEVIEN KÄSITTELYTOIMIEN OSALTA? TIETOSUOJAA KOSKEVA VAIKUTUSTENARVIOINTI VAADITAAN TIETYISSÄ OLOSUHTEISSA. 15

D. MITEN TIETOSUOJAA KOSKEVA VAIKUTUSTENARVIOINTI TEHDÄÄN? 16

a) Milloin tietosuojaa koskeva vaikutustenarviointi olisi tehtävä? Se on tehtävä ennen tietojen käsittelyä. 16

b) Kenen on tehtävä tietosuojaa koskeva vaikutustenarviointi? Rekisterinpitäjän yhdessä tietosuojavastaavan ja henkilötietojen käsittelijöiden kanssa. 17

c) Mitä menetelmiä tietosuojaa koskevan vaikutustenarvioinnin tekemiseen käytetään? Erilaiset menetelmät, mutta yhteiset kriteerit. 18

d) Onko tietosuojaa koskeva vaikutustenarviointi julkaistava? Ei, mutta yhteenvedon julkaiseminen voi lisätä luottamusta, ja tietosuojaa koskeva vaikutustenarviointi on kokonaisuudessaan toimitettava valvontaviranomaiselle ennakkokuulemisen tapauksessa tai jos tietosuojaviranomainen sitä pyytää. 21

E. MILLOIN ON KUULTAVA VALVONTAVIRANOMAISTA? KUN JÄÄNNÖSRISKIT OVAT KORKEAT. 21

IV. JOHTOPÄÄTÖKSET JA SUOSITUKSET 22

LIITE 1 – ESIMERKKEJÄ OLEMASSA OLEVISTA EU:N TIETOSUOJAA KOSKEVAN VAIKUTUSTENARVIOINNIN KEHYKSISTÄ 24

LIITE 2 – TIETOSUOJAA KOSKEVAN VAIKUTUSTENARVIOINNIN HYVÄKSYMISKRITEERIT 26

I. Johdanto

Asetusta (EU) 2016/679[1] (yleinen tietosuoja-asetus) aletaan soveltaa 25. toukokuuta 2018. Yleisen tietosuoja-asetuksen 35 artiklassa[2] ja direktiivissä (EU) 2016/680[3] esitellään tietosuojaa koskevan vaikutustenarvioinnin käsite.

Tietosuojaa koskevan vaikutustenarvioinnin avulla on tarkoitus kuvata henkilötietojen käsittelyä, arvioida sen tarpeellisuutta ja oikeasuhteisuutta sekä tukea luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvien henkilötietojen käsittelystä[4] aiheutuvien riskien hallintaa arvioimalla riskit ja määrittelemällä toimenpiteet, joilla niihin puututaan. Tietosuojaa koskeva vaikutustenarviointi on osoitusvelvollisuuden kannalta tärkeä työkalu, koska se auttaa rekisterinpitäjiä paitsi noudattamaan yleisen tietosuoja-asetuksen vaatimuksia, myös osoittamaan, että asetuksen noudattaminen on varmistettu asianmukaisin toimenpitein (ks. myös 24 artikla)[5]. **Tietosuojaa koskeva vaikutustenarviointi on** toisin sanoen **menettely, jolla parannetaan vaatimusten noudattamista ja osoitetaan niiden noudattaminen**.

Yleisen tietosuoja-asetuksen mukaan toimivaltainen valvontaviranomainen voi määrätä sakkoja tietosuojaa koskevan vaikutustenarvioinnin vaatimusten noudattamatta jättämisestä. Tietosuojaa

---

[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).

[2] Muissa asiayhteyksissä käytetään samasta käsitteestä usein termiä ”yksityisyyden suojaa koskeva vaikutustenarviointi”.

[3] Myös 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 27 päivänä huhtikuuta 2016 annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/680 27 artiklassa todetaan, että yksityisyyden suojaa koskeva vaikutustenarviointi on toteutettava, jos käsittely ”*todennäköisesti aiheuttaa ... luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin*”.

[4] Yleisessä tietosuoja-asetuksessa ei virallisesti määritellä tietosuojaa koskevan vaikutustenarvioinnin käsitettä sinänsä, mutta

- sen vähimmäissisältö määritellään 35 artiklan 7 kohdassa seuraavasti:
    - ”a) *järjestelmällinen kuvaus suunnitelluista käsittelytoimista, ja käsittelyn tarkoituksista, mukaan lukien tarvittaessa rekisterinpitäjän oikeutetut edut;*
    - *b) arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta tarkoituksiin nähden;*
    - *c) arvio 1 kohdassa tarkoitetuista rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä; ja*
    - *d) suunnitellut toimenpiteet riskeihin puuttumiseksi, mukaan lukien suoja- ja turvallisuustoimet ja mekanismit, joilla varmistetaan henkilötietojen suoja ja osoitetaan, että tätä asetusta on noudatettu ottaen huomioon rekisteröityjen ja muiden asianomaisten oikeudet ja oikeutetut edut”*
- sen merkitys ja tehtävä täsmennetään johdanto-osan 84 kappaleessa seuraavasti: ”*Tämän asetuksen noudattamisen edesauttamiseksi tapauksissa, joissa käsittelytoimiin todennäköisesti liittyy luonnollisten henkilöiden oikeuksiin ja vapauksiin liittyvä korkea riski, rekisterinpitäjän olisi vastattava tietosuojaa koskevan vaikutustenarvioinnin suorittamisesta erityisesti kyseisen riskin alkuperän, luonteen, erityisluonteen ja vakavuuden arvioimiseksi*”.

[5] Ks. myös johdanto-osan 84 kappale: ”*Arvioinnin tulos olisi otettava huomioon määriteltäessä asianmukaisia toimia, jotka on toteutettava, jotta voidaan osoittaa, että henkilötietojen käsittely on tämän asetuksen säännösten mukaista*”.

koskevan vaikutustenarvioinnin toteuttamatta jättämisestä, kun käsittely edellyttää vaikutustenarvioinnin tekemistä (35 artiklan 1 kohta ja 3–4 kohta), vaikutustenarvioinnin tekemisestä väärällä tavalla (35 artiklan 2 kohta ja 7–9 kohta) tai toimivaltaisen valvontaviranomaisen kuulematta jättämisestä silloin, kun sitä vaaditaan (36 artiklan 3 kohdan e alakohta), voidaan määrätä enintään 10 miljoonan euron hallinnollinen sakko tai yritykselle sakko, joka on enintään kaksi prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

II. Ohjeiden soveltamisala

Näissä ohjeissa otetaan huomioon

- tietosuojatyöryhmän (WP29) lausunto 14/EN WP 218[6]
- Tietosuojavastaavaa koskevat tietosuojatyöryhmän ohjeet ”Guidelines on Data Protection Officer” 16/EN WP 243[7]
- Käyttötarkoituksen rajoittamista koskeva tietosuojatyöryhmän lausunto ”Opinion on purpose limitation” 13/EN WP 203[8]
- kansainväliset standardit[9].

Yleiseen tietosuoja-asetukseen sisältyvän riskiperusteisen lähestymistavan mukaisesti tietosuojaa koskevan vaikutustenarvioinnin suorittaminen ei ole pakollista kaikkien käsittelytoimien osalta. Vaikutustenarviointi vaaditaan vain, jos käsittely ”*todennäköisesti aiheuttaa ... luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin*” (35 artiklan 1 kohta). Jotta pakollista vaikutustenarviointia edellyttävät olosuhteet (35 artiklan 3 kohta) voidaan määritellä yhdenmukaisesti, näissä ohjeissa pyritään ensinnäkin täsmentämään tätä käsitettä ja tarjoamaan tietosuojaviranomaisille kriteerejä 35 artiklan 4 kohdassa tarkoitettujen luettelojen laatimista varten.

Euroopan tietosuojaneuvosto antaa 70 artiklan 1 kohdan e alakohdan mukaisesti suuntaviivoja, suosituksia ja parhaita käytänteitä, joiden tarkoituksena on tukea yleisen tietosuoja-asetuksen johdonmukaista soveltamista. Tämän asiakirjan tavoitteena on ennakoida Euroopan tietosuojaneuvoston edellä mainittua tulevaa työtä ja sen vuoksi selventää yleisen tietosuoja-asetuksen asiaan liittyviä säännöksiä. Näin rekisterinpitäjiä autetaan noudattamaan lainsäädäntöä ja turvataan oikeusvarmuus rekisterinpitäjille, joiden on tehtävä tietosuojaa koskeva vaikutustenarviointi.

---

[6] Tietosuojatyöryhmän lausunto tietosuojalainsäädännön riskiperusteisen lähestymistavan roolista ”Statement on the role of a risk-based approach in data protection legal frameworks” 14/EN WP 218, 30.5.2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] Tietosuojavastaavaa koskevat tietosuojatyöryhmän ohjeet ”Guidelines on Data Protection Officer” 16/EN WP 243, 13.12.2016. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] Käyttötarkoituksen rajoittamista koskeva tietosuojatyöryhmän lausunto ”Opinion 03/2013 on purpose limitation” 13/EN WP 203, 2.4.2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] esim. ISO 31000:2009, *Riskinhallinta. Periaatteet ja ohjeet*, Kansainvälinen standardisoimisjärjestö (ISO); ISO/IEC 29134 (valmistumassa), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, Kansainvälinen standardisoimisjärjestö (ISO).

Näillä ohjeilla pyritään myös edistämään seuraavien luetteloiden, perusteiden ja suositusten laatimista:

- Euroopan unionin yhteinen luettelo käsittelytoimista, joiden yhteydessä tietosuojaa koskeva vaikutustenarviointi on pakollinen (35 artiklan 4 kohta)
- EU:n yhteinen luettelo käsittelytoimista, joiden osalta ei vaadita tietosuojaa koskevaa vaikutustenarviointia (35 artiklan 5 kohta)
- yhteiset kriteerit tietosuojaa koskevan vaikutustenarvioinnin toteuttamismenetelmille (35 artiklan 5 kohta)
- yhteiset kriteerit valvontaviranomaisen kuulemistarpeen määrittelylle (36 artiklan 1 kohta)
- suositukset, jotka mahdollisuuksien mukaan perustuvat EU:n jäsenvaltioissa saatuihin kokemuksiin.

III. Tietosuojaa koskeva vaikutustenarviointi: asetuksen selventäminen

Yleisen tietosuoja-asetuksen mukaan rekisterinpitäjien on toteutettava tarvittavat toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan yleistä tietosuoja-asetusta, ottaen huomioon muun muassa ”luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit” (24 artiklan 1 kohta). Rekisterinpitäjien velvollisuutta laatia tietyissä olosuhteissa tietosuojaa koskeva vaikutustenarviointi olisi tarkasteltava ottaen huomioon niille asetettu yleinen velvoite, jonka mukaan niiden on hallittava asianmukaisesti henkilötietojen aiheuttamia riskejä[10].

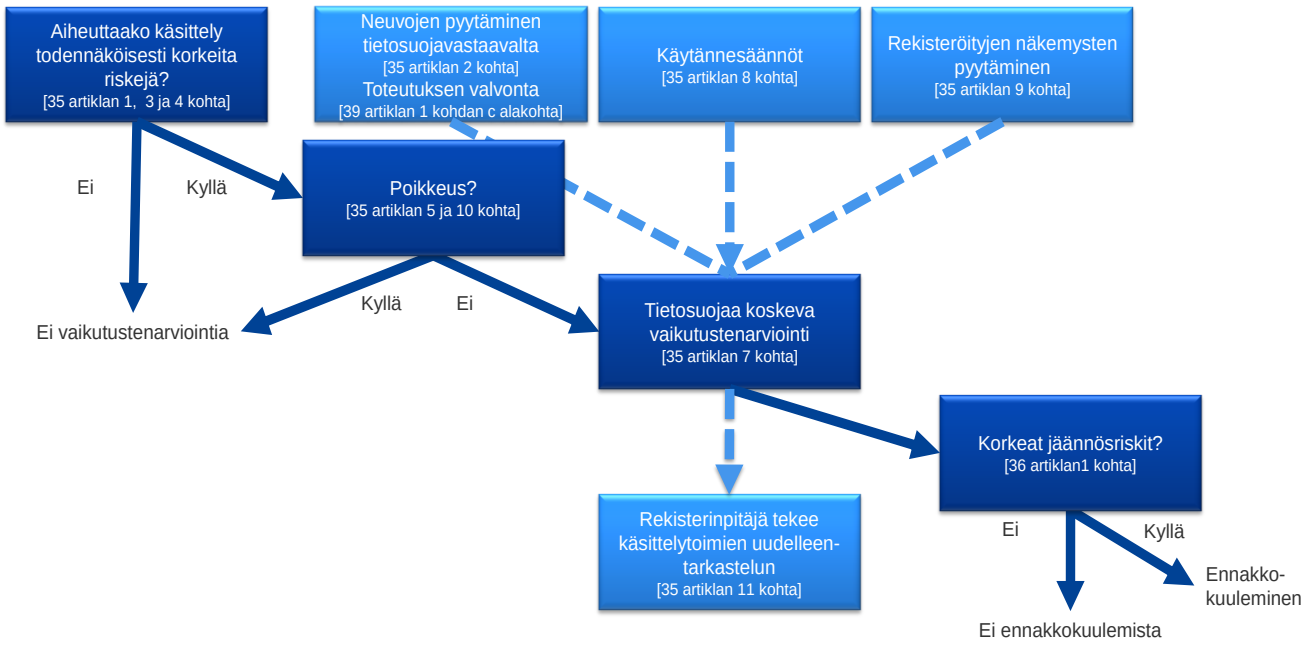
”Riskillä” tarkoitetaan skenaariota, jolla kuvataan tapahtumaa ja sen seurauksia ja arvioidaan niiden vakavuutta ja todennäköisyyttä. ”Riskinhallinta” voidaan puolestaan määritellä koordinoiduksi toiminnaksi, jolla ohjataan ja valvotaan organisaatiota riskien osalta.

Tietosuoja-asetuksen 35 artiklassa viitataan ”luonnollisen henkilön oikeuksien ja vapauksien kannalta” todennäköisesti korkeaan riskiin. Kuten tietosuojalainsäädännön riskiperusteisen lähestymistavan roolia koskevassa tietosuojatyöryhmän lausunnossa 14/EN WP 218 esitetään, viittaaminen rekisteröityjen ”oikeuksiin ja vapauksiin” koskee ensisijaisesti oikeutta tietosuojaan ja oikeutta yksityisyyteen mutta voi käsittää myös muita perusoikeuksia, kuten sananvapauden, ajatuksenvapauden, liikkumisvapauden, syrjintäkiellon, oikeuden vapauteen sekä omantunnon ja uskonnon vapauden.

Yleiseen tietosuoja-asetukseen sisältyvän riskiperusteisen lähestymistavan mukaisesti tietosuojaa koskevan vaikutustenarvioinnin suorittaminen ei ole pakollista kaikkien käsittelytoimien osalta. Vaikutustenarviointi vaaditaan vain, jos tietyntyyppinen käsittely ”todennäköisesti aiheuttaa ... luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin” (35 artiklan 1 kohta). Vaikka tietosuojaa koskevan vaikutustenarvioinnin tekemisen ehdot eivät täyttyisikään, rekisterinpitäjillä on edelleen yleinen velvollisuus toteuttaa toimenpiteitä, joilla hallitaan rekisteröityjen oikeuksiin ja vapauksiin kohdistuvia riskejä. Käytännössä tämä tarkoittaa, että rekisterinpitäjien on jatkuvasti arvioitava riskejä, joita niiden käsittelytoimet aiheuttavat. Näin voidaan tunnistaa, milloin tietyntyyppinen käsittely ”todennäköisesti aiheuttaa ... luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin”.

[10] On korostettava, että luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvien riskien hallitsemiseksi riskit on tunnistettava, analysoitava ja arvioitava. Niitä on myös käsiteltävä (esim. lievennettävä tms.) sekä tarkasteltava säännöllisesti uudelleen. Vakuutuksen ottaminen riskien varalta ei vapauta rekisterinpitäjiä vastuusta.

Seuraavassa kuvassa havainnollistetaan yleisen tietosuoja-asetuksen perusperiaatteita, jotka liittyvät tietosuojaa koskevaan vaikutustenarviointiin:



A. Mitä tietosuojaa koskevassa vaikutustenarvioinnissa käsitellään? Yhtä käsittelytointa tai useita samankaltaisia käsittelytoimia.

Tietosuojaa koskeva vaikutustenarviointi voi koskea vain yhtä tiedonkäsittelytointa. Asetuksen 35 artiklan 1 kohdassa todetaan kuitenkin, että ”*yhtä arviota voidaan käyttää samankaltaisiin vastaavia korkeita riskejä aiheuttaviin käsittelytoimiin*”. Johdanto-osan 92 kappaleessa todetaan lisäksi, että ”*joissain olosuhteissa voi olla järkevää ja taloudellista laatia tietosuojaa koskeva vaikutustenarviointi, jossa tarkastellaan asioita laajemmin kuin yhden projektin kannalta, esimerkiksi kun viranomaiset tai julkishallinnon elimet aikovat luoda yhteisen sovelluksen tai käsittelyalustan tai kun useat rekisterinpitäjät aikovat ottaa käyttöön yhteisen sovelluksen tai käsittely-ympäristön kokonaista teollisuuden alaa tai segmenttiä tai jotakin laajalti käytettävää horisontaalista toimintoa varten*”.

Yhtä yksittäistä tietosuojaa koskevaa vaikutustenarviointia voidaan käyttää useiden sellaisten käsittelytoimien arviointiin, joiden luonne, laajuus, asiayhteys, tarkoitus ja riskit ovat **samankaltaisia**. Tietosuojaa koskevien vaikutustenarviointien tavoitteena on tutkia järjestelmällisesti uusia tilanteita, jotka voivat aiheuttaa luonnollisten henkilöiden oikeuksien ja vapauksien kannalta korkean riskin. Vaikutustenarviointia ei tarvitse tehdä tapauksissa (eli tietyssä asiayhteydessä ja tiettyyn tarkoitukseen toteutettujen käsittelytoimien osalta), jotka on jo tutkittu. Näin voi olla silloin, kun samankaltaista tekniikkaa on käytetty samantyyppisten tietojen keräämiseen samoja tarkoituksia varten. Esimerkiksi ryhmälle kunnallisia viranomaisia, joista kukin perustaa samankaltaisen valvontakamerajärjestelmän (CCTV), riittää yhden tietosuojaa koskevan vaikutustenarvioinnin toteuttaminen. Sillä katetaan näiden erillisten rekisterinpitäjien suorittama käsittely. Vastaavasti rautatieliikenteen harjoittaja (yksi rekisterinpitäjä) voi kattaa videovalvonnan kaikilla rautatieasemillaan yhdellä vaikutustenarvioinnilla. Tätä voidaan soveltaa myös useiden eri rekisterinpitäjien toteuttamiin samankaltaisiin käsittelytoimiin. Näissä tapauksissa olisi jaettava tai saatettava julkisesti saataville ei-sitova tietosuojaa koskeva vaikutustenarviointi, toteutettava siinä kuvatut toimenpiteet ja esitettävä perustelut yhden vaikutustenarvioinnin tekemiselle.

Jos käsittelytoimeen osallistuu yhteisrekisterinpitäjiä, niiden on tarkasti määriteltävä kullekin erikseen kuuluvat velvollisuudet. Niiden laatimassa tietosuojaa koskevassa vaikutustenarvioinnissa olisi määriteltävä, mikä osapuoli vastaa erilaisista riskien käsittelyyn ja rekisteröityjen oikeuksien ja vapauksien suojeluun suunnitelluista toimenpiteistä. Kunkin rekisterinpitäjän olisi ilmoitettava tarpeensa ja jaettava hyödyllisiä tietoja vaarantamatta salaisuuksia (esim. liikesalaisuuksien, henkisen omaisuuden, luottamuksellisten liiketietojen suojelu) tai paljastamatta haavoittuvuuksia.

Tietosuojaa koskeva vaikutustenarviointi voi olla hyödyllinen myös teknisen tuotteen, esimerkiksi laitteen tai ohjelman, **aiheuttaman tietosuojaa koskevan vaikutuksen arvioinnin kannalta,** jos sitä käyttävät todennäköisesti eri rekisterinpitäjät eri käsittelytoimien suorittamiseen. Tuotetta käyttävällä rekisterinpitäjällä on luonnollisesti edelleen velvollisuus suorittaa oma tietosuojaa koskeva vaikutustenarviointi käsittelytoimintansa osalta. Tarvittaessa hän voi kuitenkin saada tietoa tuotteen toimittajan tekemästä vaikutustenarvioinnista. Esimerkkinä tästä voisi olla älymittareiden valmistajien ja kunnallisten yritysten välinen suhde. Kunkin tuotteen toimittajan tai henkilötietojen käsittelijän olisi jaettava hyödyllisiä tietoja vaarantamatta salaisuuksia ja aiheuttamatta turvallisuusriskejä paljastamalla haavoittuvuuksia.

B. Mille käsittelytoimille on tehtävä tietosuojaa koskeva vaikutustenarviointi? Lukuun ottamatta poikkeuksia arviointi on tehtävä silloin, kun käsittely ”*todennäköisesti aiheuttaa ... korkean riskin*”

Tässä luvussa kerrotaan, milloin tietosuojaa koskeva vaikutustenarviointi on pakollinen ja milloin sitä ei tarvitse tehdä.

Tietosuojaa koskeva vaikutustenarviointi on tehtävä silloin, kun käsittelytoimi ”*todennäköisesti aiheuttaa ... korkean riskin*” (ks. III.B.b) eikä täytä poikkeusmenettelyn (ks. III.B.a) edellytyksiä.

a) Milloin tietosuojaa koskeva vaikutustenarviointi on pakollinen? Se on pakollinen silloin, kun käsittely ”*todennäköisesti aiheuttaa ... korkean riskin*”.

Yleisessä tietosuoja-asetuksessa ei vaadita tietosuojaa koskevan vaikutustenarvioinnin suorittamista kaikkien sellaisten käsittelytoimien osalta, jotka voivat aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta riskin. Vaikutustenarviointi on pakollinen vain, jos käsittely ”*todennäköisesti aiheuttaa ... luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin*” (35 artiklan 1 kohta, josta annetaan esimerkkejä 35 artiklan 3 kohdassa ja jota täydentää 35 artiklan 4 kohta). Se on erityisen tärkeä silloin, kun otetaan käyttöön uutta henkilötietojen käsittelytekniikkaa[11].

Tapauksissa, joissa ei ole selvää, vaaditaanko tietosuojaa koskeva vaikutustenarviointi, tietosuojatyöryhmä suosittelee sen tekemistä joka tapauksessa, koska se auttaa rekisterinpitäjiä noudattamaan tietosuojalainsäädäntöä.

Vaikka tietosuojaa koskeva vaikutustenarviointi voidaan vaatia myös muissa olosuhteissa, 35 artiklan 3 kohdassa annetaan joitakin esimerkkejä tapauksista, joissa käsittelytoimi *”todennäköisesti aiheuttaa ... korkean riskin”:*

- ”*(a) luonnollisten henkilöiden henkilökohtaisten ominaisuuksien järjestelmällinen ja kattava arviointi, joka perustuu automaattiseen käsittelyyn, kuten profilointiin, ja johtaa päätöksiin,*

[11] Lisää esimerkkejä on johdanto-osan 89 ja 91 kappaleessa sekä 35 artiklan 1 ja 3 kohdassa.

joilla on luonnollista henkilöä koskevia oikeusvaikutuksia tai jotka vaikuttavat luonnolliseen henkilöön vastaavalla tavalla merkittävästi[12]*;*

- *b) laajamittainen käsittely, joka kohdistuu 1 artiklassa tarkoitettuihin erityisiin henkilötietoryhmiin tai 10 artiklassa tarkoitettuihin rikostuomioita tai rikkomuksia koskeviin tietoihin*[13]*; tai*
- *c) yleisölle avoimen alueen järjestelmällinen valvonta laajamittaisesti*".

Kuten yleisen tietosuoja-asetuksen 35 artiklan 3 kohdan johdantokappaleen sanasta "*erityisesti*" käy ilmi, luettelon ei ole tarkoitus olla tyhjentävä. Näiden esimerkkien lisäksi voi olla muita käsittelytoimia, joihin liittyy "korkea riski" ja jotka eivät sisälly tähän luetteloon, vaikka ne aiheuttavat vastaavia korkeita riskejä. Myös tällaisista käsittelytoimista olisi tehtävä tietosuojaa koskeva vaikutustenarviointi. Siksi jäljempänä käsiteltävissä kriteereissä selitetään, mitä yleisen tietosuoja-asetuksen 35 artiklan 3 kohdassa annetuilla kolmella esimerkillä tarkoitetaan, mutta esitellään myös muita tapauksia.

Jäljempänä olevissa yhdeksässä kriteerissä esitetään konkreettisempia esimerkkejä käsittelytoimista, joiden osalta vaaditaan tietosuojaa koskeva vaikutustenarviointi niihin liittyvän korkean riskin vuoksi ottaen huomioon 35 artiklan 1 kohdan ja 35 artiklan 3 kohdan a–c alakohdan tietyt osat, 35 artiklan 4 kohdan ja johdanto-osan 71, 75 ja 91 kappaleen mukaisesti kansallisella tasolla vahvistettava luettelo sekä muut yleiseen tietosuoja-asetukseen sisältyvät viittaukset käsittelyyn, joka "*todennäköisesti aiheuttaa ... korkean riskin*"[14].

1. Erityisesti *"rekisteröidyn työsuorituksen, taloudellisen tilanteen, terveyden, henkilökohtaisten mieltymysten tai kiinnostuksen kohteiden, luotettavuuden tai käyttäytymisen, sijainnin tai liikkumisen"* arviointi tai pisteytys, mukaan lukien profilointi ja ennakointi (johdanto-osan 71 ja 91 kappale). Esimerkkinä tästä voisi olla rahoituslaitos, joka arvioi asiakkaitaan luottotoimintaan liittyvän viitetietokannan tai rahanpesun ja terrorismin rahoituksen torjumiseen liittyvän tietokannan tai petoksia koskevan tietokannan valossa. Muita esimerkkejä ovat biotekniikka-alan yritys, joka tarjoaa geenitestejä suoraan kuluttajille voidakseen arvioida ja ennakoida sairauksien riskejä ja/tai terveysriskejä, sekä yritys, joka luo käyttäytymis- tai markkinointiprofiileja, jotka perustuvat sen verkkosivuston käyttöön tai verkkosivustolla liikkumiseen.
2. Automaattinen päätöksenteko, jolla on oikeusvaikutuksia tai vastaavia merkittäviä vaikutuksia: käsittely, jonka tavoitteena on tehdä rekisteröidyistä päätöksiä, joilla on "*luonnollista henkilöä koskevia oikeusvaikutuksia*" tai jotka "*vaikuttavat luonnolliseen henkilöön vastaavalla tavalla merkittävästi*" (35 artiklan 3 kohdan a alakohta). Tällainen käsittely voi esimerkiksi johtaa henkilöiden ulkopuolelle jättämiseen tai syrjintään. Tätä erityistä kriteeriä ei täytä käsittely, joka vaikuttaa luonnollisiin henkilöihin vain vähän tai ei

[12] Ks. johdanto-osan 71 kappale: "*erityisesti jos kyseessä on henkilöprofiilin luomista tai käyttämistä varten suoritettu analyysi tai ennakointi työsuorituksesta, taloudellisesta tilanteesta, terveydestä, henkilökohtaisista mieltymyksistä tai kiinnostuksen kohteista, luotettavuudesta tai käyttäytymisestä, sijainnista tai liikkeistä*".

[13] Ks. johdanto-osan 75 kappale: "*kun käsitellään sellaisia henkilötietoja, jotka koskevat rotua tai etnistä alkuperää, poliittisia mielipiteitä, uskonnollista tai filosofista vakaumusta ja ammattiliittoon kuulumista, tai käsitellään geneettisiä tietoja tai terveyttä ja seksuaalista käyttäytymistä tai rikostuomioita ja rikkomuksia tai niihin liittyviä turvaamistoimenpiteitä koskevia tietoja*".

[14] Ks. esim. johdanto-osan 75, 76, 92 ja 116 kappale.

ollenkaan. Näitä käsitteitä koskevia lisäselvityksiä annetaan tulevissa profilointia koskevissa tietosuojatyöryhmän ohjeissa.

3. Järjestelmällinen valvonta: rekisteröityjen tarkkailuun, seurantaan tai valvontaan käytettävä tietojenkäsittely sekä tietojen kerääminen verkkojen välityksellä tai ”*yleisölle avoimen alueen järjestelmällinen valvonta laajamittaisesti*” (35 artiklan 3 kohdan c alakohta)[15]. Tämäntyyppinen valvonta on yksi kriteereistä, koska henkilötietoja voidaan kerätä olosuhteissa, joissa rekisteröidyt eivät välttämättä ole tietoisia siitä, kuka kerää heidän tietojaan ja miten niitä tullaan käyttämään. Lisäksi yksittäisten henkilöiden voi olla mahdotonta välttyä joutumasta tällaisen tietojenkäsittelyn kohteeksi julkisessa tilassa (julkisissa tiloissa) tai yleisölle avoimessa tilassa (avoimissa tiloissa).
4. Arkaluontoiset tiedot tai luonteeltaan hyvin henkilökohtaiset tiedot: niihin kuuluvat 9 artiklassa määritellyt erityiset henkilötietoryhmät (esimerkiksi tiedot henkilöiden poliittisista mielipiteistä) sekä rikostuomioihin ja rikkomuksiin liittyvät henkilötiedot, jotka määritellään 10 artiklassa. Esimerkkinä tästä voisivat olla potilastiedostoja ylläpitävä yleinen sairaala tai rikoksentekijöiden tietoja säilyttävä yksityisetsivä. Näiden yleisen tietosuoja-asetuksen säännösten kattamien tietoryhmien lisäksi eräiden muiden tietoryhmien voidaan katsoa lisäävän mahdollista luonnollisten henkilöiden oikeuksiin ja vapauksiin liittyvää riskiä. Nämä henkilötiedot katsotaan arkaluontoisiksi (termin yleisessä merkityksessä), koska ne liittyvät kotitaloutta koskevaan ja yksityiseen toimintaan (esimerkiksi sähköinen viestintä, jonka luottamuksellisuus olisi suojattava), tai koska ne vaikuttavat perusoikeuden käyttämiseen (esimerkiksi paikannustiedot, joiden kerääminen kyseenalaistaa vapaan liikkuvuuden) tai koska niiden loukkaamiseen liittyy selvästi rekisteröidyn arkeen kohdistuvia vakavia vaikutuksia (esimerkiksi taloudelliset tiedot, joita saatetaan käyttää maksuvälinepetoksiin). Tässä yhteydessä voi olla merkitystä sillä, onko rekisteröity itse tai jokin kolmas osapuoli jo saattanut tiedot yleisesti saataville. Se, että henkilötiedot ovat yleisesti saatavilla, voidaan katsoa arvioinnin kannalta olennaiseksi, jos tietoja on odotettu käytettävän jatkossa tiettyihin tarkoituksiin. Tähän kriteeriin voi kuulua myös henkilökohtaisia asiakirjoja, kuten sähköposteja, päiväkirjoja, muistiinpanotoiminnolla varustetun e-kirjan lukulaitteen muistiinpanoja ja henkilökohtaisen elämän tallentamiseen tarkoitettujen lifelogging-sovellusten hyvin henkilökohtaisia tietoja.
5. Tietojen laajamittainen käsittely: yleisessä tietosuoja-asetuksessa ei määritellä laajamittaista käsittelyä, mutta johdanto-osan 91 kappaleessa annetaan joitakin siihen liittyviä ohjeita. Tietosuojaryhmä suosittelee joka tapauksessa, että seuraavat tekijät otetaan erityisesti huomioon määritettäessä, toteutetaanko käsittely laajamittaisesti[16]:
    a. asianomaisten rekisteröityjen lukumäärä, joko täsmällisenä lukuna tai osuutena kyseisestä väestöstä

[15] Tietosuojatyöryhmän tulkinnan mukaan termillä ”*järjestelmällinen*” tarkoitetaan yhtä tai useampaa seuraavista vaihtoehdoista (ks. Tietosuojavastaavaa koskevat tietosuojatyöryhmän ohjeet ”Guidelines on Data Protection Officer” 16/EN WP 243):

- jotain järjestelmää noudattaen tapahtuva
- ennalta järjestetty, organisoitu tai menetelmällinen
- osana tietojenkeruuta koskevaa yleissuunnitelmaa tapahtuva
- osana strategiaa toteutettava.

Tietosuojatyöryhmän tulkinnan mukaan ”*yleisölle avoimella alueella”* tarkoitetaan mitä tahansa paikkaa, joka on avoin kenelle tahansa yleisön jäsenelle, kuten aukio, ostoskeskus, katu, tori, rautatieasema tai yleinen kirjasto.

[16] Ks. tietosuojavastaavaa koskevat tietosuojatyöryhmän ohjeet ”Guidelines on Data Protection Officer” 16/EN WP 243.

b. käsiteltävien tietojen määrä ja/tai käsiteltävien erillisten tietoyksikköjen määrä
c. tietojenkäsittelytoimen kesto tai pysyvyys
d. käsittelytoimen maantieteellinen ulottuvuus.

6. Tietokokonaisuuksien sovittaminen yhteen tai yhdistäminen rekisteröidyn kohtuulliset odotukset ylittävällä tavalla, kun kyseessä ovat esimerkiksi kahdesta tai useammasta eri tarkoituksiin suoritetusta ja/tai eri rekisterinpitäjien suorittamasta tiedonkäsittelytoimesta peräisin olevat tietokokonaisuudet[17].
7. Heikossa asemassa olevia rekisteröityjä koskevat tiedot (johdanto-osan 75 kappale): tämäntyyppisten tietojen käsittely on yksi kriteereistä, koska sen taustalla on rekisteröityjen ja rekisterinpitäjän välisten voimasuhteiden epätasapainon lisääntyminen, jonka vuoksi yksittäisten henkilöiden ei välttämättä ole helppo antaa suostumusta tai vastustaa tietojensa käsittelyä tai käyttää oikeuksiaan. Heikossa asemassa olevilla rekisteröidyillä tarkoitetaan esimerkiksi lapsia (heidän voidaan katsoa olevan kykenemättömiä tietoisesti ja harkiten vastustamaan tietojensa käsittelyä tai antamaan suostumuksen siihen), työntekijöitä, muita heikommassa asemassa olevia ja erityistä suojelua tarvitsevia väestöryhmiä (mielenterveysongelmista kärsivät henkilöt, turvapaikanhakijat tai ikääntyneet ihmiset, potilaat jne.) sekä kaikkia muita rekisteröityjä, joiden suhteessa rekisterinpitäjään voidaan havaita epätasapaino.
8. Uusien teknisten tai organisatoristen ratkaisujen innovatiivinen käyttö tai soveltaminen, esimerkiksi sormenjälkien ja kasvojen tunnistuksen yhdistäminen kulunvalvonnan parantamiseksi jne. Yleisessä tietosuoja-asetuksessa (35 artiklan 1 kohta ja johdanto-osan 89 ja 91 kappale) tehdään selväksi, että uuden tekniikan käyttäminen ”*saavutetun teknologisen osaamistason mukaisesti*” (johdanto-osan 91 kappale) voi edellyttää tietosuojaa koskevan vaikutustenarvioinnin tekemistä. Tämä johtuu siitä, että tällaisen tekniikan käyttöön voi liittyä uudenlaisia tietojen keräämisen ja käytön muotoja, joihin mahdollisesti liittyy henkilöiden oikeuksiin ja vapauksiin kohdistuva korkea riski. Uuden tekniikan käytön henkilökohtaiset ja sosiaaliset seuraukset voivat olla hämärän peitossa. Tietosuojaa koskeva vaikutustenarviointi auttaa rekisterinpitäjää ymmärtämään ja käsittelemään tällaisia riskejä. Esimerkiksi tietyillä esineiden internet -sovelluksilla voi olla huomattava vaikutus yksittäisten henkilöiden arkielämään ja yksityisyyteen, joten ne edellyttävät tietosuojaa koskevan vaikutustenarvioinnin tekemistä.
9. Tapaukset, joissa itse käsittelytoimet *”estävät rekisteröityjä käyttämästä oikeutta tai palvelua tai sopimusta”* (22 artikla ja johdanto-osan 91 kappale). Tämä käsittää käsittelytoimet, joiden tavoitteena on sallia tai evätä rekisteröityjen oikeus käyttää palvelua tai tehdä sopimus tai muuttaa kyseistä oikeutta. Esimerkkinä tästä on tilanne, jossa pankki arvioi asiakkaitaan luottotoimintaan liittyvän viitetietokannan valossa tehdäkseen päätöksen lainan tarjoamisesta.

Rekisterinpitäjä voi useimmissa tapauksissa katsoa, että kaksi kriteeriä täyttävä käsittely edellyttää tietosuojaa koskevan vaikutustenarvioinnin tekemistä. Tietosuojatyöryhmä katsoo yleisesti ottaen, että mitä useampia kriteerejä käsittely täyttää, sitä todennäköisemmin se aiheuttaa korkean riskin rekisteröityjen oikeuksien ja vapauksien kannalta ja edellyttää sen vuoksi vaikutustenarviointia riippumatta rekisterinpitäjän kaavailemista toimenpiteistä.

[17] Ks. käyttötarkoituksen rajoittamista koskevan tietosuojatyöryhmän lausunnon ”Opinion 03/2013 on purpose limitation” 13/EN WP 203 sivulla 24 oleva selitys.

Rekisterinpitäjä voi kuitenkin eräissä tapauksissa **katsoa, että vain yhden näistä kriteereistä täyttävä käsittely edellyttää tietosuojaa koskevan vaikutustenarvioinnin tekemistä**.

Seuraavissa esimerkeissä havainnollistetaan, miten kriteerien avulla voidaan arvioida, edellyttääkö jokin tietty käsittelytoimi tietosuojaa koskevaa vaikutustenarviointia:

Esimerkkejä käsittelytoimista	**Mahdolliset olennaiset kriteerit**	**Vaaditaanko tietosuojaa koskeva vaikutustenarviointi todennäköisesti?**
Sairaala, joka käsittelee potilaiden geneettisiä ja terveystietoja (sairaalan tietojärjestelmässä).	- Arkaluontoiset tiedot tai luonteeltaan hyvin henkilökohtaiset tiedot - Heikossa asemassa olevia rekisteröityjä koskevat tiedot - Tietojen laajamittainen käsittely	Kyllä
Kamerajärjestelmän käyttö ajotavan seurantaan valtateillä. Rekisterinpitäjä suunnittelee käyttävänsä älykästä videoanalyysijärjestelmää autojen esiin poimintaan ja rekisterikilpien automaattiseen tunnistamiseen.	- Järjestelmällinen valvonta - Teknisten tai organisatoristen ratkaisujen innovatiivinen käyttö tai soveltaminen	
Yritys seuraa järjestelmällisesti työntekijöidensä toimintaa, esimerkiksi työntekijöiden työasemia ja toimintaa internetissä jne.	- Järjestelmällinen valvonta - Heikossa asemassa olevia rekisteröityjä koskevat tiedot	
Sosiaalisen median julkisten tietojen kerääminen profiilien laatimiseksi.	- Arviointi tai pisteytys - Tietojen laajamittainen käsittely - Tietokokonaisuuksien sovittaminen yhteen tai yhdistäminen - Arkaluontoiset tiedot tai luonteeltaan hyvin henkilökohtaiset tiedot	
Laitos laatii kansallisen tason luottoluokitus- tai petoksia koskevan tietokannan	- Arviointi tai pisteytys - Automaattinen päätöksenteko, jolla on oikeusvaikutuksia tai vastaavia merkittäviä vaikutuksia - Estää rekisteröityä käyttämästä oikeutta tai palvelua tai sopimusta - Arkaluontoiset tiedot tai luonteeltaan hyvin henkilökohtaiset tiedot	
Heikossa asemassa olevia rekisteröityjä koskevien ja peitenimellä tallennettujen, tutkimushankkeisiin tai kliinisiin tutkimuksiin liittyvien arkaluontoisten henkilötietojen tallentaminen arkistointitarkoituksiin.	- Arkaluontoiset tiedot - Heikossa asemassa olevia rekisteröityjä koskevat tiedot - Estää rekisteröityjä käyttämästä oikeutta tai palvelua tai sopimusta	
Käsittely, joka koskee ”yksittäisen lääkärin, muun terveydenhuollon ammattilaisen tai	- Arkaluontoiset tiedot tai luonteeltaan hyvin henkilökohtaiset tiedot	Ei

Esimerkkejä käsittelytoimista	Mahdolliset olennaiset kriteerit	Vaaditaanko tietosuojaa koskeva vaikutustenarviointi todennäköisesti?
lakimiehen asiakkaiden henkilötietoja" (johdanto-osan 91 kappale).	- Heikossa asemassa olevia rekisteröityjä koskevat tiedot	
Verkkolehti käyttää postituslistaa päivittäisen yleiskoosteen lähettämiseen tilaajilleen	- Tietojen laajamittainen käsittely	
Sähköisen kaupankäynnin verkkosivustolla esitetään museoajoneuvojen osia koskevia ilmoituksia, joihin liittyy kyseisellä verkkosivustolla katsottuihin tai hankittuihin tavaroihin perustuva rajoitettu profilointi.	- Arviointi tai pisteytys	

Käsittelytoimi voi toisaalta vastata edellä mainittuja tapauksia, ja rekisterinpitäjä voi silti katsoa, ettei se "todennäköisesti aiheuta ... korkeaa riskiä". Näissä tapauksissa rekisterinpitäjän olisi perusteltava ja dokumentoitava syyt, joiden vuoksi se ei tee tietosuojaa koskevaa vaikutustenarviointia. Lisäksi sen olisi sisällytettävä perusteluihin / kirjattava tietosuojavastaavan näkemykset.

Tilivelvollisuusperiaatteen mukaisesti jokaisen rekisterinpitäjän "*on ylläpidettävä selostetta vastuullaan olevista käsittelytoimista*", mukaan lukien muun muassa käsittelyn tarkoitukset, kuvaus tietoryhmistä ja henkilötietojen vastaanottajien ryhmistä sekä "*mahdollisuuksien mukaan yleinen kuvaus 32 artiklan 1 kohdassa tarkoitetuista teknisistä ja organisatorisista turvatoimista*" (30 artiklan 1 kohta). Rekisterinpitäjien on myös arvioitava, onko korkea riski todennäköinen, vaikka ne lopulta päättäisivät olla tekemättä tietosuojaa koskevaa vaikutustenarviointia.

Huomautus: valvontaviranomaisten on laadittava ja julkaistava luettelo käsittelytoimista, joiden yhteydessä vaaditaan tietosuojaa koskeva vaikutustenarviointi, sekä toimitettava se Euroopan tietosuojaneuvostolle (35 artiklan 4 kohta)[18]. Valvontaviranomaiset voivat saada apua edellä esitetyistä kriteereistä laatiessaan kyseistä luetteloa, johon voidaan tarvittaessa myöhemmin lisätä yksityiskohtaisempaa sisältöä. Esimerkiksi myös kaikentyyppisten biometristen tietojen tai lasten tietojen käsittelystä voidaan katsoa, että se on lisättävä 35 artiklan 4 kohdan nojalla laadittavaan luetteloon.

b) Milloin tietosuojaa koskevaa vaikutustenarviointia ei vaadita? Sitä ei vaadita, kun ei katsota, että käsittely "todennäköisesti aiheuttaa ... korkean riskin" tai kun samankaltainen vaikutustenarviointi on jo olemassa, käsittelylle on annettu hyväksyntä ennen toukokuuta 2018, käsittelyllä on oikeusperusta tai se sisältyy niiden käsittelytoimien luetteloon, joiden yhteydessä ei vaadita vaikutustenarviointia.

[18] Tältä osin on otettava huomioon, että "*jos ... luettelo sisältää käsittelytoimia, jotka liittyvät tavaroiden tai palvelujen tarjoamiseen rekisteröidyille tai näiden käyttäytymisen seurantaan useissa jäsenvaltioissa tai jos toimet voivat merkittävästi vaikuttaa henkilötietojen vapaaseen liikkuvuuteen unionissa, toimivaltaisen valvontaviranomaisen on sovellettava 63 artiklassa tarkoitettua yhdenmukaisuusmekanismia*" (35 artiklan 6 kohta).

Tietosuojatyöryhmä katsoo, ettei tietosuojaa koskevaa vaikutustenarviointia vaadita seuraavissa tapauksissa:

- **jos käsittelystä ei katsota, että se "*todennäköisesti aiheuttaa ... luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin*"** (35 artiklan 1 kohta)
- **jos käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset ovat hyvin samankaltaisia kuin sellaisen käsittelyn, jonka osalta vaikutustenarviointi on jo tehty**. Tällaisissa tapauksissa voidaan käyttää samankaltaisen käsittelyn yhteydessä tehdyn vaikutustenarvioinnin tuloksia (35 artiklan 1 kohta)[19]
- jos valvontaviranomainen on tarkastanut käsittelytoimet ennen toukokuuta 2018 tietyissä olosuhteissa, jotka eivät ole muuttuneet[20] (ks. III C kohta);
- **jos käsittelytoimella on** 6 artiklan 1 kohdan c tai e alakohdan nojalla **oikeusperuste** EU:n oikeudessa tai jäsenvaltion lainsäädännössä, joka säätelee siihen liittyvää käsittelytointa **ja jos tietosuojaa koskeva vaikutustenarviointi on jo tehty** kyseisen käsittelyn oikeusperusteen määrittämisen yhteydessä (35 artiklan 10 kohta)[21], paitsi jos jäsenvaltio katsoo tarpeelliseksi toteuttaa tällaisen arvioinnin ennen käsittelytoimien aloittamista;
- **jos käsittely sisältyy (valvontaviranomaisen laatimaan) vapaaehtoisuuden periaatteeseen perustuvaan luetteloon käsittelytoimista,** joiden osalta ei vaadita tietosuojaa koskevaa vaikutustenarviointia (35 artiklan 5 kohta). Tällainen luettelo voi sisältää kyseisen viranomaisen määrittelemien ehtojen mukaisia käsittelytoimia. Viranomainen voi määritellä ehdot erityisesti ohjeiden, tapauskohtaisten päätösten tai hyväksyntöjen, vaatimuksenmukaisuutta koskevien sääntöjen jne. (esim. Ranskassa muun muassa hyväksyntöjen, poikkeusten, yksinkertaistettujen sääntöjen tai vaatimustenmukaisuutta koskevien materiaalien) avulla. Tällaisissa tapauksissa ei vaadita tietosuojaa koskevaa vaikutustenarviointia edellyttäen, että toimivaltainen valvontaviranomainen toteuttaa uudelleenarvioinnin ja että käsittely kuuluu kiistattomasti luettelossa mainitun asiaan liittyvän menettelyn piiriin ja on jatkossakin kaikilta osin kaikkien yleisen tietosuoja-asetuksen olennaisten vaatimusten mukainen.

C. Miten menetellään jo käytössä olevien käsittelytoimien osalta? Tietosuojaa koskeva vaikutustenarviointi vaaditaan tietyissä olosuhteissa.

Tietosuojaa koskevan vaikutustenarvioinnin tekemistä koskevaa vaatimusta sovelletaan jo käytössä oleviin käsittelytoimiin, jotka todennäköisesti aiheuttavat luonnollisten henkilöiden oikeuksien ja vapauksien kannalta korkean riskin ja joiden sisältämä riski on muuttunut, ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset.

Tietosuojaa koskevaa vaikutustenarviointia ei tarvita käsittelytoimille, jotka valvontaviranomainen tai henkilötietojen suojaamisesta vastaava henkilö on tarkastanut direktiivin 95/46/EY 20 artiklan

[19] "*Yhtä arviota voidaan käyttää samankaltaisiin vastaavia korkeita riskejä aiheuttaviin käsittelytoimiin.*"

[20] "*Direktiiviin 95/46/EY perustuvat komission päätökset ja valvontaviranomaisten antamat hyväksynnät pysyvät voimassa, kunnes niitä muutetaan, ne korvataan tai kumotaan*" (johdanto-osan 171 kappale).

[21] Kun tietosuojaa koskeva vaikutustenarviointi tehdään käsittelyn oikeusperusteen muodostavan lainsäädännön laatimisvaiheessa, ennen toimien aloittamista edellytetään todennäköisesti uudelleentarkastelua, koska hyväksytty lainsäädäntö saattaa poiketa ehdotuksesta siten, että poikkeaminen vaikuttaa yksityisyyteen ja tietosuojaan liittyviin asioihin. Lainsäädännön antamisen yhteydessä ei välttämättä ole saatavilla riittävästi varsinaista käsittelyä koskevia teknisiä tietoja, vaikka säädösehdotuksen mukana olisikin ollut tietosuojaa koskeva vaikutustenarviointi. Tällaisissa tapauksissa voi olla tarpeen tehdä erityinen tietosuojaa koskeva vaikutustenarviointi ennen varsinaisten käsittelytoimien toteuttamista.

mukaisesti ja joiden suorittamistapa ei ole muuttunut ennakkotarkastuksen jälkeen. Tämä johtuu siitä, että ”*direktiiviin 95/46/EY perustuvat komission päätökset ja valvontaviranomaisten antamat hyväksynnät pysyvät voimassa, kunnes niitä muutetaan, ne korvataan tai kumotaan*” (johdanto-osan 171 kappale).

Tämä tarkoittaa toisaalta, että tietosuojaa koskeva vaikutustenarviointi olisi tehtävä kaikille käsittelytoimille, joiden täytäntöönpano-olosuhteet (laajuus, tarkoitus, kerätyt henkilötiedot, rekisterinpitäjien tai vastaanottajien henkilöllisyys, tietojen säilytysaika, tekniset ja organisatoriset toimenpiteet jne.) ovat muuttuneet valvontaviranomaisen tai henkilötietojen suojaamisesta vastaavan henkilön suorittaman ennakkotarkastuksen jälkeen ja jotka todennäköisesti aiheuttavat korkean riskin.

Tietosuojaa koskeva vaikutustenarviointi voidaan lisäksi vaatia sen jälkeen, kun käsittelytoimista aiheutuvat riskit ovat muuttuneet[22] esimerkiksi uuden tekniikan käyttöönoton tai henkilötietojen käyttötarkoituksen muuttumisen johdosta. Tiedonkäsittelytoimet voivat muuttua nopeasti ja uusia haavoittuvuuksia voi syntyä. Sen vuoksi on pantava merkille, että tietosuojaa koskevan vaikutustenarvioinnin tarkistaminen on paitsi hyödyllistä toiminnan jatkuvan parantamisen kannalta, myös ratkaisevaa tietosuojan tason säilyttämiseksi ajan mittaan muuttuvassa ympäristössä. Tietosuojaa koskeva vaikutustenarviointi voi tulla tarpeelliseksi myös käsittelytoiminnan organisatorisen tai yhteiskunnallisen asiayhteyden muuttumisen vuoksi esimerkiksi, kun tiettyjen automatisoitujen päätösten vaikutus on kasvanut tai uusista rekisteröityjen ryhmistä on tullut alttiita syrjinnälle. Kukin näistä esimerkeistä voisi olla asianomaisesta käsittelytoiminnasta aiheutuvan riskin muuttumiseen johtava tekijä.

Tietyt muutokset voivat toisaalta myös pienentää riskiä. Käsittelytoimi voi esimerkiksi muuttua siten, että päätökset eivät enää ole automatisoituja tai valvonta ei enää ole järjestelmällistä. Tässä tapauksessa jo tehdyn riskianalyysin uudelleentarkastelu voi osoittaa, ettei tietosuojaa koskevaa vaikutustenarviointia enää vaadita.

Hyvän käytännön noudattamiseksi **tietosuojaa koskevaa vaikutustenarviointia olisi tarkistettava jatkuvasti ja arvioitava säännöllisesti uudelleen**. Vaikka tietosuojaa koskevaa vaikutustenarviointia ei vaadita 25. toukokuuta 2018, rekisterinpitäjän on sen vuoksi tehtävä edellä mainittu vaikutustenarviointi yleiseen tilivelvollisuuteen liittyvien velvoitteiden täyttämiseksi.

D. Miten tietosuojaa koskeva vaikutustenarviointi tehdään?

a) Milloin tietosuojaa koskeva vaikutustenarviointi olisi tehtävä? Se on tehtävä ennen tietojen käsittelyä.

Tietosuojaa koskeva vaikutustenarviointi olisi toteutettava ”*ennen käsittelyä*” (35 artiklan 1 ja 10 kohta sekä johdanto-osan 90 ja 93 kappale)[23]. Tämä vastaa sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita (25 artikla ja johdanto-osan 78 kappale). Tietosuojaa

[22] Asiayhteyden, kerättyjen henkilötietojen, tarkoitusten, toimintojen, käsiteltävien henkilötietojen, vastaanottajien, tietojen yhdistämisen, riskien (käsittelyyn käytettävät varat, riskien alkuperä, mahdolliset vaikutukset, uhat jne.), turvatoimenpiteiden ja kansainvälisten siirtojen suhteen.

[23] Paitsi silloin, kun kyseessä on jo olemassa oleva käsittely, jonka valvontaviranomainen on ennakkotarkastanut. Tässä tapauksessa tietosuojaa koskeva vaikutustenarviointi olisi tehtävä ennen merkittävien muutosten toteuttamista.

koskevaa vaikutustenarviointia olisi pidettävä välineenä, jolla tuetaan käsittelyä koskevaa päätöksentekoa.

Tietosuojaa koskeva vaikutustenarviointi olisi aloitettava mahdollisimman aikaisin käsittelytoimen suunnitteluvaiheessa, vaikka kaikki toiminnan osat eivät vielä olisi tiedossa. Päivittämällä tietosuojaa koskevaa vaikutustenarviointia hankkeen koko elinkaaren aikana varmistetaan tietosuojan ja yksityisyyden huomioon ottaminen ja tuetaan vaatimusten noudattamista edistävien ratkaisujen luomista. Voi olla tarpeen myös kerrata arvioinnin yksittäisiä vaiheita sitä mukaa kun kehitysprosessi etenee, koska tiettyjen teknisten ja organisatoristen toimenpiteiden valinta voi vaikuttaa käsittelyn aiheuttamien riskien vakavuuteen tai todennäköisyyteen.

Tietosuojaa koskevan arvioinnin päivittämisen tarve sen jälkeen, kun varsinainen käsittely on alkanut, ei ole pätevä peruste arvioinnin lykkäämiselle tai tekemättä jättämiselle. Arviointi on jatkuva prosessi erityisesti, jos käsittelytoimi on dynaaminen ja sitä muutetaan jatkuvasti. **Tietosuojaa koskevan vaikutustenarvioinnin tekeminen on jatkuva prosessi, ei kertaluonteinen tehtävä.**

b) Kenen on tehtävä tietosuojaa koskeva vaikutustenarviointi? Rekisterinpitäjän yhdessä tietosuojavastaavan ja henkilötietojen käsittelijöiden kanssa.

Rekisterinpitäjän tehtävänä on varmistaa, että tietosuojaa koskeva vaikutustenarviointi on tehty (35 artiklan 2 kohta). Tietosuojaa koskevan vaikutustenarvioinnin voi tehdä joku muu organisaation sisällä tai sen ulkopuolella, mutta viime kädessä siitä vastaa rekisterinpitäjä.

Rekisterinpitäjän on myös pyydettävä neuvoja tietosuojavastaavalta, jos sellainen on nimitetty (35 artiklan 2 kohta) ja nämä neuvot sekä rekisterinpitäjän tekemät päätökset olisi dokumentoitava tietosuojaa koskevaan vaikutustenarviointiin. Tietosuojavastaavan olisi myös valvottava tietosuojaa koskevan vaikutustenarvioinnin toteutusta (39 artiklan 1 kohdan c alakohta). Lisäohjeita annetaan tietosuojavastaavaa koskevissa tietosuojatyöryhmän ohjeissa ”Guidelines on Data Protection Officer” 16/EN WP 243.

Jos käsittelyn suorittaa kokonaan tai osittain henkilötietojen käsittelijä, **tämän olisi autettava rekisterinpitäjää tietosuojaa koskevan vaikutustenarvioinnin tekemisessä** ja annettava kaikki tarpeelliset tiedot (28 artiklan 3 kohdan f alakohta).

Rekisterinpitäjän on ”*pyydettävä rekisteröityjen tai näiden edustajien näkemyksiä* ” (35 artiklan 9 kohta), ”*tapauksen mukaan*”. Tietosuojatyöryhmä katsoo, että

- näkemyksiä voidaan pyytää monin eri tavoin asiayhteydestä riippuen (esim. yleinen tutkimus, joka liittyy käsittelytoimen tarkoitukseen ja keinoihin, työntekijöiden edustajille osoitettu kysymys tai rekisterinpitäjän tuleville asiakkaille lähetetyt tavanomaiset kyselyt) varmistaen, että rekisterinpitäjällä on laillinen perusta tällaisten näkemysten pyytämiseen liittyvälle henkilötietojen käsittelylle. On kuitenkin huomattava, ettei käsittelyyn annettu suostumus ole ilman muuta suostumus näkemysten antamiseen.
- jos rekisterinpitäjän lopullinen päätös poikkeaa rekisteröityjen näkemyksistä, olisi dokumentoitava rekisterinpitäjän perustelut käsittelyn jatkamiselle tai lopettamiselle
- rekisterinpitäjän olisi myös dokumentoitava perustelunsa rekisteröityjen näkemysten pyytämättä jättämiselle, jos se päättää, ettei niiden pyytäminen ole aiheellista esimerkiksi, jos se vaarantaisi yrityksen liiketoimintasuunnitelmien luottamuksellisuuden tai olisi kohtuutonta tai mahdotonta.

Hyvän käytännön mukaista on määritellä ja dokumentoida muita erityisiä rooleja ja vastuualueita riippuen sisäisestä politiikasta, menettelyistä ja säännöistä. Tästä esitetään seuraavia esimerkkejä:

- jos tietyt liiketoimintayksiköt voivat ehdottaa tietosuojaa koskevan vaikutustenarvioinnin tekemistä, kyseisten yksikköjen olisi sen jälkeen annettava tietoja vaikutustenarviointiin ja ne olisi otettava mukaan vaikutustenarvioinnin kelpoisuustarkastukseen
- on suositeltavaa pyytää tarvittaessa neuvoja eri alojen riippumattomilta asiantuntijoilta[24] (lakimiehet, tietotekniikka-asiantuntijat, turvallisuusasiantuntijat, sosiologit, etiikan asiantuntijat jne.).
- henkilötietojen käsittelijöiden roolit ja vastuualueet on määriteltävä sopimusperusteisesti; lisäksi tietosuojaa koskeva vaikutustenarviointi on toteutettava henkilötietojen käsittelijän avustuksella ottaen huomioon käsittelyn luonne ja henkilötietojen käsittelijän saatavilla olevat tiedot (28 artiklan 3 kohdan f alakohta)
- tietojärjestelmien turvallisuusvastaava, jos sellainen on nimitetty, sekä tietosuojavastaava voivat ehdottaa, että rekisterinpitäjä tekee tiettyyn käsittelytoimeen liittyvän tietosuojaa koskevan vaikutustenarvioinnin; niiden olisi autettava sidosryhmiä käsittelemään menetelmiin liittyviä kysymyksiä, arvioimaan riskinarvioinnin laatua ja jäännösriskin hyväksyttävyyttä sekä kehittämään rekisterinpitäjän toimintaympäristössä tarvittavaa osaamista.
- tietojärjestelmien turvallisuusvastaavan, jos sellainen on nimitetty, ja/tai tietotekniikkayksikön, olisi annettava apua rekisterinpitäjälle; ne voivat ehdottaa tiettyyn käsittelytoimeen liittyvän tietosuojaa koskevan vaikutustenarvioinnin tekemistä turvallisuuteen tai toimintaan liittyvistä tarpeista riippuen.

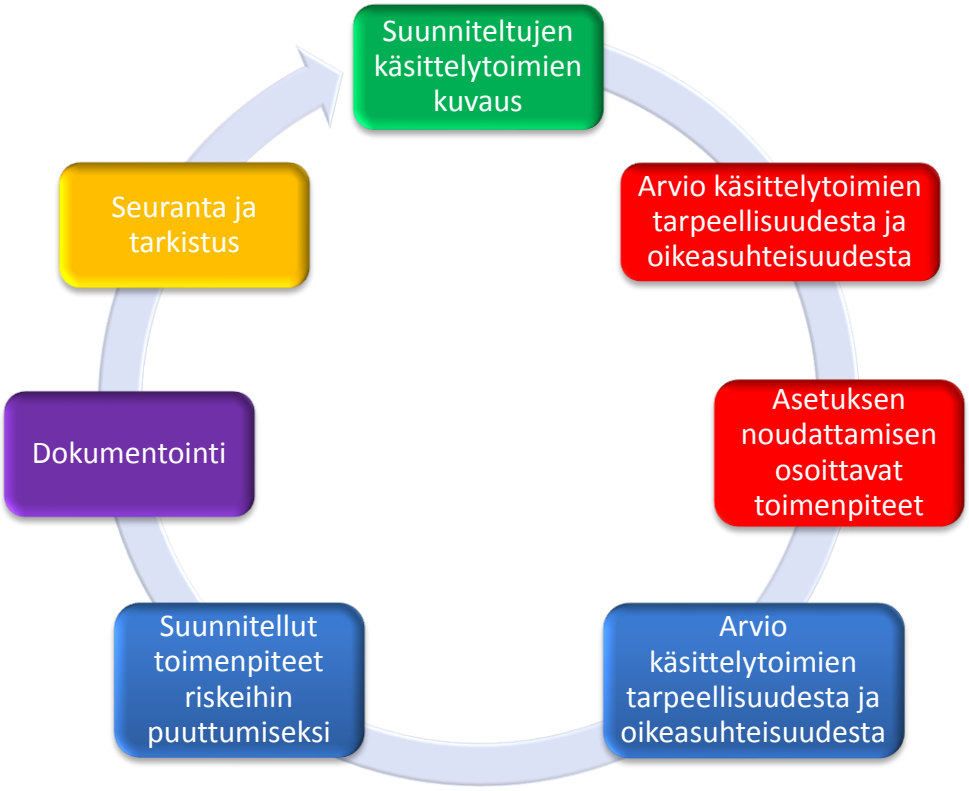
c) Mitä menetelmiä tietosuojaa koskevan vaikutustenarvioinnin tekemiseen käytetään? Erilaiset menetelmät, mutta yhteiset kriteerit.

[24] *Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

Yleisessä tietosuoja-asetuksessa määritellään vähimmäisvaatimukset tietosuojaa koskevalle vaikutustenarvioinnille (35 artiklan 7 kohta ja johdanto-osan 84 ja 90 kappale):

- ”kuvaus suunnitelluista käsittelytoimista ja käsittelyn tarkoituksista”
- ”arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta”
- ”arvio ... rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä”
- ”suunnitellut toimenpiteet
    - ”*riskeihin puuttumiseksi*”
    - sen osoittamiseksi, että ”*tätä asetusta on noudatettu*”.

Seuraava kuva esittää yleistä iteratiivista menettelyä tietosuojaa koskevan vaikutustenarvioinnin tekemiseksi[25]:



Käytännesääntöjen (40 artikla) noudattaminen on otettava huomioon (35 artiklan 8 kohta) arvioitaessa tiedonkäsittelytoimen vaikutusta. Näin voidaan osoittaa, että on valittu tai otettu käyttöön riittävät toimenpiteet edellyttäen, että käytännesäännöt ovat sovellettavissa kyseiseen käsittelytoimeen. Olisi myös otettava huomioon sertifioinnit, sinetit ja merkit, joiden tarkoituksena on osoittaa, että rekisterinpitäjät ja henkilötietojen käsittelijät noudattavat käsittelytoimia suorittaessaan yleistä tietosuoja-asetusta (42 artikla) ja yritystä koskevia sitovia sääntöjä.

Kaikki yleisen tietosuoja-asetuksen mukaiset asiaan liittyvät vaatimukset tarjoavat laajan yleisen kehyksen tietosuojaa koskevan vaikutustenarvioinnin tekemiselle. Vaikutustenarvioinnin käytännön

[25] On korostettava, että kuvassa esitetty menettely on iteratiivinen: käytännössä on todennäköistä, että kuhunkin vaiheeseen palataan useita kertoja, ennen kuin tietosuojaa koskeva vaikutustenarviointi saadaan valmiiksi.

toteutus määräytyy yleisessä tietosuoja-asetuksessa esitettyjen vaatimusten mukaan, joita voidaan täydentää yksityiskohtaisemmilla käytännön ohjeilla. Tietosuojaa koskevan vaikutustenarvioinnin toteuttaminen on näin ollen joustavaa. Tämä tarkoittaa, että myös pienimuotoista toimintaa harjoittava rekisterinpitäjä voi suunnitella ja toteuttaa vaikutustenarvioinnin, joka soveltuu sen käsittelytoimiin.

Yleisen tietosuoja-asetuksen johdanto-osan 90 kappaleessa mainitaan joitakin tietosuojaa koskevan vaikutustenarvioinnin osatekijöitä, jotka menevät päällekkäin riskinhallinnan tarkasti määriteltyjen osatekijöiden (esim. ISO 31000[26]) kanssa. Riskinhallinnan osalta tietosuojaa koskevalla vaikutustenarvioinnilla pyritään ”hallitsemaan riskejä”, jotka kohdistuvat luonnollisten henkilöiden oikeuksiin ja vapauksiin, käyttämällä seuraavia menettelyjä:

- asiayhteyden määrittely: ”*käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitusten sekä riskin alkuperän”* huomioon ottaminen
- riskien arviointi: korkean ”*riskin erityisen todennäköisyyden ja vakavuuden*” arviointi
- riskien käsittely: ”*lievennetään edellä mainittua riskiä*” ja ”*varmistetaan henkilötietojen suoja*” ja ”*osoitetaan, että tätä asetusta on noudatettu”.*

Huomautus: Yleisen tietosuoja-asetuksen mukaisella tietosuojaa koskevalla vaikutustenarvioinnilla pyritään hallitsemaan rekisteröityjen oikeuksiin kohdistuvia riskejä. Arvioinnissa otetaan näin ollen näkökulmaksi rekisteröityjen näkökulma tiettyjen muiden alojen tapaan (esim. yhteiskunnan turvallisuus). Muiden alojen (esim. tietoturva) riskinhallinnassa keskitytään sitä vastoin organisaatioon.

Yleisessä tietosuoja-asetuksessa jätetään rekisterinpitäjille joustovaraa tietosuojaa koskevan vaikutustenarvioinnin tarkan rakenteen ja muodon määrittelyyn. Näin se saadaan sovitettua yhteen käytössä olevien toimintatapojen kanssa. EU:ssa ja koko maailmassa on olemassa erilaisia vakiintuneita menettelyjä, joissa otetaan huomioon johdanto-osan 90 kappaleessa mainitut osatekijät. Tietosuojaa koskevan vaikutustenarvioinnin on muodosta riippumatta kuitenkin oltava riskien todellinen arviointi, joka antaa rekisterinpitäjille mahdollisuuden puuttua riskeihin.

Yleisessä tietosuoja-asetuksessa esitettyjen perusvaatimusten täyttämisessä voidaan käyttää apuna erilaisia menetelmiä (ks. liite 1, jossa annetaan esimerkkejä tietosuojaa ja yksityisyyden suojaa koskevan vaikutustenarvioinnin menetelmistä). Yhteisten kriteerien määrittelyn (ks. liite 2) ansiosta nämä erilaiset lähestymistavat ovat mahdollisia ja rekisterinpitäjät saavat tukea yleisen tietosuoja-asetuksen noudattamiseen. Kriteereillä täsmennetään asetuksen perusvaatimuksia ja tarjotaan toisaalta riittävästi mahdollisuuksia täytäntöönpanon eri muodoille. Näitä kriteerejä voidaan käyttää osoittamaan, että jokin tietty tietosuojaa koskevan vaikutustenarvioinnin tekemiseen käytetty menetelmä on yleisessä tietosuoja-asetuksessa esitettyjen vaatimusten mukainen. **Rekisterinpitäjän tehtävänä on valita menetelmä, jonka olisi kuitenkin oltava liitteessä 2 esitettyjen kriteerien mukainen**.

Tietosuojatyöryhmä kannustaa kehittämään tietosuojaa koskevan vaikutustenarvioinnin alakohtaisia kehyksiä. Ne voivat perustua alakohtaiseen erityisosaamiseen, jolloin tietosuojaa koskevassa vaikutustenarvioinnissa voidaan tarkastella tietyntyyppisen käsittelytoimen erityispiirteitä (esim. tietyntyyppisiä tietoja, yrityksen varoja, mahdollisia vaikutuksia, uhkia, toimenpiteitä). Tämä

[26] Riskinhallintamenettelyt: tiedottaminen ja kuuleminen, asiayhteyden määrittely, riskien arviointi, riskien käsittely, seuranta ja uudelleentarkastelu (ks. termit ja määritelmät sekä sisällysluettelo ISO 31000 -standardin esikatselusta: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

tarkoittaa, että tietosuojaa koskevassa vaikutustenarvioinnissa voidaan käsitellä asioita, jotka tulevat esiin tietyllä talouden alalla tai käytettäessä tiettyä tekniikkaa tai toteutettaessa tietyntyyppisiä käsittelytoimia.

Lisäksi ”*rekisterinpitäjän on tehtävä tarvittaessa uudelleentarkastelu arvioidakseen, tapahtuuko käsittely tietosuojaa koskevan vaikutustenarvioinnin mukaisesti, ainakin jos käsittelytoimien sisältämä riski muuttuu*” (35 artiklan 11 kohta[27]).

d) Onko tietosuojaa koskeva vaikutustenarviointi julkaistava? Ei, mutta yhteenvedon julkaiseminen voi lisätä luottamusta, ja tietosuojaa koskeva vaikutustenarviointi on kokonaisuudessaan toimitettava valvontaviranomaiselle ennakkokuulemisen tapauksessa tai jos tietosuojaviranomainen sitä pyytää.

Yleisessä tietosuoja-asetuksessa ei vaadita tietosuojaa koskevan vaikutustenarvioinnin julkaisemista, vaan siitä päättää rekisterinpitäjä. Rekisterinpitäjien olisi kuitenkin harkittava ainakin vaikutustenarvioinnin osien, esimerkiksi yhteenvedon tai päätelmien, julkaisemista.

Tällaisen menettelyn tarkoituksena on auttaa lisäämään luottamusta rekisterinpitäjän käsittelytoimia kohtaan ja osoittaa luotettavuus ja läpinäkyvyys. On erityisen hyvän käytännön mukaista julkistaa tietosuojaa koskeva vaikutustenarviointi silloin, kun käsittelytoimi vaikuttaa yksittäisiin kansalaisiin. Näin on erityisesti tapauksissa, joissa viranomainen tekee tietosuojaa koskevan vaikutustenarvioinnin.

Julkaistavan tietosuojaa koskevan vaikutustenarvioinnin ei tarvitse sisältää koko arviointia etenkään, jos arviointiin saattaa sisältyä rekisterinpitäjään kohdistuvia turvallisuusriskejä koskevia tietoja, liikesalaisuuksia tai kaupallisesti arkaluonteisia tietoja. Julkaistavana versiona voi tässä yhteydessä olla arvioinnin pääasiallisten tulosten yhteenveto tai pelkkä maininta siitä, että vaikutustenarviointi on tehty.

Jos tietosuojaa koskevasta vaikutustenarvioinnista käy ilmi korkeita jäännösriskejä, rekisterinpitäjän on pyydettävä valvontaviranomaiselta käsittelyä koskevaa ennakkokuulemista (36 artiklan 1 kohta). Tässä yhteydessä vaikutustenarviointi on toimitettava kokonaisuudessaan valvontaviranomaiselle (36 artiklan 3 kohdan e alakohta). Valvontaviranomainen voi antaa neuvojaan[28] vaarantamatta liikesalaisuuksia ja paljastamatta turvallisuutta vaarantavia tekijöitä, edellyttäen että se noudattaa kussakin jäsenvaltiossa sovellettavia virallisten asiakirjojen julkisuutta koskevia periaatteita.

E. <u>Milloin on kuultava valvontaviranomaista? Kun jäännösriskit ovat korkeat.</u>

Kuten edellä on esitetty,

- tietosuojaa koskeva vaikutustenarviointi vaaditaan, jos käsittelytoimi ”*todennäköisesti aiheuttaa ... luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin*” (35 artiklan 1 kohta, ks. III.B.a). Tästä on esimerkkinä terveystietojen laajamittainen käsittely, jonka katsotaan todennäköisesti aiheuttavan korkean riskin ja edellyttävän tietosuojaa koskevan vaikutustenarvioinnin tekemistä

[27] Asetuksen 35 artiklan 10 kohdassa nimenomaisesti suljetaan pois vain 35 artiklan 1–7 kohdan soveltaminen.

[28] Rekisterinpitäjälle on annettava ohjeet kirjallisina vain, jos valvontaviranomainen on sitä mieltä, että suunniteltu käsittely ei 36 artiklan 2 kohdan mukaan ole asetuksen mukaista.

- silloin rekisterinpitäjä vastaa rekisteröityjen oikeuksiin ja vapauksiin kohdistuvien riskien arvioinnista ja niiden toimenpiteiden[29] määrittelystä, jotka on suunniteltu lieventämään kyseisiä riskejä hyväksyttävälle tasolle, sekä sen osoittamisesta, että yleistä tietosuoja-asetusta on noudatettu (35 artiklan 7 kohta, ks. IIIC.c). Yhtenä esimerkkinä voisi olla asianmukaisten teknisten ja organisatoristen turvaamistoimien (tehokas koko levyn salaus, luotettava avaintenhallinta, asianmukainen pääsynvalvonta, suojatut varmuuskopiot jne.) käyttö henkilötietojen kannettaville tietokoneille tallentamisen yhteydessä, olemassa olevien toimintatapojen (ilmoitus, suostumus, pääsyoikeus, vastustusoikeus jne.) lisäksi.

Jos edellä esitetyssä kannettavaan tietokoneeseen liittyvässä esimerkissä katsotaan, että rekisterinpitäjä on lieventänyt riskejä riittävästi, ja kun on tulkittu 36 artiklan 1 kohtaa sekä johdanto-osan 84 ja 94 kappaletta, käsittely voidaan toteuttaa kuulematta valvontaviranomaista. Rekisterinpitäjän on kuultava valvontaviranomaista tapauksissa, joissa hän ei pysty riittävästi puuttumaan tunnistettuihin riskeihin (eli jäännösriskit pysyvät korkeina).

Esimerkkinä liian korkeasta jäännösriskistä ovat muun muassa tapaukset, joissa rekisteröidyt voivat joutua kärsimään huomattavista tai jopa peruuttamattomista seurauksista, joita he eivät välttämättä pysty torjumaan (esim. laiton tietoihin pääsy, joka johtaa rekisteröityjen henkeä uhkaavaan vaaraan, irtisanomiseen tai taloudelliseen uhkaan) ja/tai joissa riskin ilmeneminen näyttää selvältä (esim. kun ei pystytä vähentämään niiden henkilöiden lukumäärää, joilla on pääsy tietoihin tietojen jakamis-, käyttö- tai levitystapojen vuoksi tai kun tiedossa olevaa haavoittuvuutta ei pystytä korjaamaan).

Valvontaviranomaista on kuultava aina, kun rekisterinpitäjä ei pysty toteuttamaan riittäviä toimenpiteitä riskien lieventämiseksi hyväksyttävälle tasolle (eli kun jäännösriskit ovat edelleen korkeat)[30].

Lisäksi rekisterinpitäjän on kuultava valvontaviranomaista aina, kun jäsenvaltion lainsäädännössä vaaditaan rekisterinpitäjiä kuulemaan valvontaviranomaista ja/tai saamaan siltä ennakkolupa, jos rekisterinpitäjä suorittaa henkilötietojen käsittelyn yleiseen etuun liittyvän tehtävän suorittamiseksi, mukaan lukien käsittely sosiaaliturvan ja kansanterveyden alalla (36 artiklan 5 kohta).

On kuitenkin todettava, että riippumatta siitä, vaaditaanko valvontaviranomaisen kuulemista jäännösriskin tason perusteella vai ei, velvollisuudet säilyttää tiedot tietosuojaa koskevasta vaikutustenarvioinnista ja päivittää vaikutustenarviointia hyvissä ajoin pysyvät voimassa.

IV. Johtopäätökset ja suositukset

Tietosuojaa koskevien vaikutustenarviointien avulla rekisterinpitäjät voivat toteuttaa tietojenkäsittelyjärjestelmiä, jotka ovat yleisen tietosuoja-asetuksen mukaisia. Tällaiset vaikutustenarvioinnit voivat olla pakollisia tietyntyyppisten käsittelytoimien osalta. Ne ovat joustavia ja voivat olla eri muotoisia. Yleisessä tietosuoja-asetuksessa esitetään kuitenkin perusvaatimukset

[29] Mukaan lukien Euroopan tietosuojaneuvoston ja valvontaviranomaisten olemassa olevien ohjeiden huomioon ottaminen sekä uusimman tekniikan ja täytäntöönpanokustannusten huomioon ottaminen 35 artiklan 1 kohdassa säädetyllä tavalla.

[30] Huomautus: ”*henkilötietojen pseudonymisointi ja salaus*” (sekä tietojen minimointi, valvontamekanismit jne.) eivät välttämättä ole tarvittavia toimenpiteitä. Ne ovat vain esimerkkejä. Tarvittavat toimenpiteet määräytyvät käsittelytoimien asiayhteyden ja riskien mukaan.

tehokkaalle tietosuojaa koskevalle vaikutustenarvioinnille. Rekisterinpitäjien olisi pidettävä tietosuojaa koskevan vaikutustenarvioinnin tekemistä hyödyllisenä ja myönteisenä tehtävänä, joka tukee lainsäädännön noudattamista.

Asetuksen 24 artiklan 1 kohdassa määritellään rekisterinpitäjän vastuu yleisen tietosuoja-asetuksen noudattamisen osalta: ”*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”.*

Tietosuojaa koskeva vaikutustenarviointi on olennainen osa asetuksen noudattamista, jos suunnitellaan tai toteutetaan tiedonkäsittelyä, johon liittyy korkea riski. Tämä tarkoittaa, että rekisterinpitäjien olisi käytettävä tässä asiakirjassa esitettyjä kriteerejä määritelläkseen, onko tietosuojaa koskeva vaikutustenarviointi tehtävä. Rekisterinpitäjän sisäisissä toimintamenettelyissä tätä luetteloa voidaan laajentaa yleisen tietosuoja-asetuksen lakisääteisiä vaatimuksia laajemmalle. Näin voitaisiin lisätä rekisteröityjen ja muiden rekisterinpitäjien luottamusta.

Jos suunnitellaan tiedonkäsittelyä, johon todennäköisesti liittyy korkea riski, rekisterinpitäjän on

- valittava tietosuojaa koskevan vaikutustenarvioinnin tekemiseen käytettävä menetelmä (esimerkkejä on esitetty liitteessä 1), joka täyttää liitteessä 2 esitetyt kriteerit, tai määriteltävä ja pantava täytäntöön järjestelmällinen tietosuojaa koskeva vaikutustenarviointimenettely,
    - joka on liitteessä 2 esitettyjen kriteerien mukainen
    - joka sisällytetään olemassa oleviin suunnittelu-, kehitys-, muutos- ja riskimenettelyihin sekä operatiiviseen uudelleentarkastelumenettelyyn sisäisten menettelyjen sekä sisäisen toimintaympäristön ja kulttuurin mukaisesti
    - johon otetaan mukaan asianomaiset sidosryhmät ja jossa määritellään selkeästi niiden vastuut (rekisterinpitäjä, tietosuojavastaava, rekisteröidyt tai heidän edustajansa, yritykset, tekniset palvelut, henkilötietojen käsittelijät, tietoturvasta vastaava henkilö jne.)
- annettava toimivaltaiselle valvontaviranomaiselle pyynnöstä tietosuojaa koskevan vaikutustenarvioinnin raportti
- kuultava valvontaviranomaista, jos se ei ole määritellyt riittävästi toimenpiteitä korkeiden riskien lieventämiseksi
- tarkasteltava määräajoin uudelleen tietosuojaa koskevaa vaikutustenarviointia ja siinä arvioitua käsittelyä, vähintään silloin, kun käsittelytoimen aiheuttama riski muuttuu
- dokumentoitava tehdyt päätökset.

Liite 1 – Esimerkkejä olemassa olevista EU:n tietosuojaa koskevan vaikutustenarvioinnin kehyksistä

Tietosuoja-asetuksessa ei määritellä, mitä menettelyä on käytettävä tietosuojaa koskevan vaikutustenarvioinnin tekemiseen. Sen sijaan siinä annetaan rekisterinpitäjille mahdollisuus ottaa käyttöön kehys, jolla täydennetään niiden olemassa olevia toimintatapoja edellyttäen, että niissä otetaan huomioon 35 artiklan 7 kohdassa mainitut osatekijät. Tällainen kehys voi olla rekisterinpitäjän tarpeisiin suunniteltu tai tietylle toimialalle yhteinen. EU:n tietosuojaviranomaisten kehittämiä aiemmin julkaistuja kehyksiä ja EU:n alakohtaisia kehyksiä ovat muun muassa seuraavat:

Esimerkkejä EU:n yleisistä kehyksistä:

- DE: Standardoitu tietosuojamalli V.1.0 – Testiversio, 2016[31].
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014.
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/node/15798
- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014.
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Esimerkkejä EU:n alakohtaisista kehyksistä:

- Kehys RFID-sovellusten yksityisyyden suojaa koskevien ja tietosuojavaikutusten arvioinnille[32].
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_fi.pdf
- Älykkäiden verkkojen ja älykkäiden mittausjärjestelmien tietosuojaa koskevan vaikutustenarvioinnin laadintamalli[33]
  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

---

[31] Yksimielisesti ja vahvistetusti tunnustettu liittovaltion ja osavaltioiden Kühlungsbornissa 9.–10. marraskuuta 2016 pitämässä riippumattomien tietosuojaviranomaisten 92. konferenssissa (Baijerin äänestettyä tyhjää).

[32] Katso myös:

- Komission suositus, annettu 12 päivänä toukokuuta 2009, yksityisyyden suojaa ja tietosuojaa koskevien periaatteiden toteuttamisesta radiotaajuustunnistusta käyttävissä sovelluksissa.
  https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Lausunto 9/2011 elinkeinoelämän ehdottamasta tarkistetusta kehyksestä RFID-sovellusten yksityisyyden suojaa ja tietosuojaa koskeville vaikutustenarvioinneille.
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_fi.pdf

[33] Ks. myös lausunto 07/2013 komission älykkäitä verkkoja käsittelevän erityisryhmän alaisen asiantuntijaryhmän 2 kehittämästä älykkäiden verkkojen ja älykkäiden mittausjärjestelmien tietosuojaa koskevan vaikutustenarvioinnin laadintamallista. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_fi.pdf

Ohjeita tietosuojaa koskevan vaikutustenarvioinnin tekemiseen käytettävistä menetelmistä annetaan myös kansainvälisessä standardissa (ISO/IEC 29134[34]).

[34] ISO/IEC 29134 (valmistumassa), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, Kansainvälinen standardisoimisjärjestö (ISO).

Liite 2 – Tietosuojaa koskevan vaikutustenarvioinnin hyväksymiskriteerit

Tietosuojatyöryhmä ehdottaa seuraavia kriteerejä, joita rekisterinpitäjät voivat käyttää arvioidessaan, onko tietosuojaa koskeva vaikutustenarviointi tai sen tekemiseen käytettävä menetelmä riittävän kattava yleisen tietosuoja-asetuksen noudattamiseksi:

- ☐ järjestelmällinen kuvaus käsittelystä annetaan (35 artiklan 7 kohdan a alakohta):
  - ☐ käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset otetaan huomioon (johdanto-osan 90 kappale)
  - ☐ henkilötiedoista, vastaanottajista ja henkilötietojen säilytysajasta pidetään kirjaa
  - ☐ toiminnallinen kuvaus käsittelytoimesta esitetään
  - ☐ henkilötietojen käsittelyyn käytettävät resurssit (laitteistot, ohjelmistot, verkostot, ihmiset, asiakirjat tai asiakirjojen välittämiseen käytettävät kanavat) yksilöidään
  - ☐ hyväksyttyjen käytännesääntöjen noudattaminen otetaan huomioon (35 artiklan 8 kohta)
- ☐ tarpeellisuus ja oikeasuhteisuus arvioidaan (35 artiklan 7 kohdan b alakohta):
  - ☐ suunnitellut toimenpiteet asetuksen noudattamiseksi määritellään (35 artiklan 7 kohdan d alakohta ja johdanto-osan 90 kappale) ottaen huomioon
    - ☐ käsittelyn oikeasuhteisuutta ja tarpeellisuutta edistävät toimenpiteet, joiden perustana on/ovat
      - ☐ yksi tai useampi tietty, nimenomainen ja laillinen tarkoitus (5 artiklan 1 kohdan b alakohta)
      - ☐ käsittelyn lainmukaisuus (6 artikla)
      - ☐ tiedot, jotka ovat asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista (5 artiklan 1 kohdan c alakohta)
      - ☐ rajoitettu säilytysaika (5 artiklan 1 kohdan e alakohta)
    - ☐ rekisteröityjen oikeuksia edistävät toimenpiteet:
      - ☐ rekisteröidylle annettavat tiedot (12, 13 ja 14 artikla)
      - ☐ oikeus saada pääsy tietoihin ja siirtää tiedot järjestelmästä toiseen (15 ja 20 artikla)
      - ☐ oikeus tietojen oikaisemiseen ja poistamiseen (16, 17 ja 19 artikla)
      - ☐ vastustamisoikeus ja oikeus käsittelyn rajoittamiseen (18, 19 ja 21 artikla)
      - ☐ suhteet henkilötietojen käsittelijöihin (28 artikla)
      - ☐ kansainvälisiin henkilötietojen siirtoihin liittyvät suojatoimet (V luku)
      - ☐ ennakkokuuleminen (36 artikla).
- ☐ rekisteröityjen oikeuksiin ja vapauksiin kohdistuvia riskejä hallitaan (35 artiklan 7 kohdan c alakohta):
  - ☐ riskien alkuperä, luonne, erityisluonne ja vakavuus arvioidaan (ks. johdanto-osan 84 kappale) tai tarkemmin ottaen kunkin riskin (laiton tietoihin pääsy, tietojen asiaton muuttaminen ja tietojen katoaminen) osalta erikseen rekisteröityjen näkökulmasta:
    - ☐ riskien alkuperä otetaan huomioon (johdanto-osan 90 kappale)
    - ☐ rekisteröityjen oikeuksiin ja vapauksiin kohdistuvat mahdolliset vaikutukset tunnistetaan sellaisten tapahtumien osalta, joihin kuuluu laiton tietoihin pääsy, asiaton muuttaminen ja tietojen katoaminen
    - ☐ tunnistetaan uhat, jotka voivat johtaa laittomaan tietoihin pääsyyn, asiattomaan muuttamiseen ja tietojen katoamiseen
    - ☐ todennäköisyys ja vakavuus arvioidaan (johdanto-osan 90 kappale)
  - ☐ riskien käsittelyyn suunnitellut toimenpiteet määritellään (35 artiklan 7 kohdan d alakohta ja johdanto-osan 90 kappale)
- ☐ Sidosryhmät otetaan mukaan seuraavasti:
  - ☐ pyydetään tietosuojavastaavalta neuvoja (35 artiklan 2 kohta)
  - ☐ tarvittaessa pyydetään rekisteröityjen tai heidän edustajiensa näkemyksiä (35 artiklan 9 kohta).