Potilasrekisteri ja EU:n tietosuoja-asetus

Yleistä

EU:n tietosuoja-asetus tuli voimaan 24.5.2016. Sen edellyttämät toimenpiteet tulee olla tehtynä siirtymäajan kuluttua viimeistään 25.5.2018, josta eteenpäin tietosuoja-asetusta on noudatettava. Tietosuoja-asetus vastaa monin paikoin nykyistä henkilötietolakiamme. Tietosuoja-asetukseen sisältyy tietosuojan kannalta kuitenkin myös uutta asiaa.

Tietosuoja-asetus on suoraan sovellettavaa oikeutta Suomessa. Sitä ei muunneta erikseen kansalliseksi laiksi. Tietosuoja-asetus jättää jonkin verran kansallista liikkumavaraa. Tätä liikkumavaraa varten säädetään uusi tietosuojalaki. Nyt voimassa oleva henkilötietolaki kumotaan tietosuoja-asetuksen tullessa sovellettavaksi.

Tietosuoja-asetus asettaa varsin ankarat sanktiot asetuksen rikkomisesta. Asetuksen säännösten rikkomisesta voidaan määrätä hallinnollinen sakko, jonka enimmäismäärä on 20 miljoonaa euroa tai 4 % yrityksen vuotuisesta maailmanlaajuisesta liikevaihdosta. Tietosuojavaltuutetun toimisto tulee muuttumaan tietosuoja-asetuksen noudattamista valvovaksi valvontaviranomaiseksi.

Tässä ohjeessa on käsitelty tietosuoja-asioita laajasti. Kaikki tieto ei ole relevanttia jokaisen toimijan osalta, mutta ohjeeseen on hyvä tutustua kokonaisuuden hahmottamiseksi.

Dokumentointivelvollisuus (tietosuojaselvitys)

Uutena asiana tietosuoja-asetuksessa on rekisterinpitäjän *dokumentointivelvollisuus*. Rekisterinpitäjän on pystyttävä osoittamaan se, että tietosuoja-asetuksen tietosuojaperiaatteita on noudatettu. Tämä tarkoittaa esim. sitä, että rekisterinpitäjän on käytävä läpi tietovarantonsa, arvioitava niihin kohdistuvat riskit, omaksuttava tarvittavat käytännöt ja toimenpiteet riskien vuoksi ja selvitettävä miten näiden asioiden koulutus on järjestetty henkilökunnalle. Kaikki tämä on dokumentoitava ja tarvittaessa esitettävä valvontaviranomaiselle. *Tämä on mahdollisesti merkittävin käytännön uudistus tietosuoja-asetuksessa ja teettää rekisterinpitäjille työtä.*

Tietojen käsittelyn on oltava läpinäkyvää. Rekisteröidylle on annettava kaikki käsittelyä koskevat tiedot tiiviisti esitetyssä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Rekisterinpitäjän on helpotettava rekisteröidyn oikeuksien toteutumista sekä neuvottava ja opastettava rekisteröityä.

Dokumentointivelvollisuus on hyvä aloittaa hahmottamalla vastaanoton tietovirrat. Mistä tietoa saadaan, mitä tietoa saadaan ja mihin tietoa luovutetaan? Enimmäkseen vastaanoton tieto on potilastietoa, jota saadaan hoidon yhteydessä potilaalta. Erilaisten tietojen osalta on selvitettävä käsittelyn tarkoitus. Tarpeetonta tietoa ei saa käsitellä ja tietoa saadaan käsitellä vain siinä tarkoituksessa, johon se on kerätty. Potilastiedon osalta käsittelyn tarkoitus on hoidon mahdollistaminen ja edistäminen. Mikäli potilastiedon osalta käsitellään myös muuta tietoa, on tämän osalta selvitettävä mikä ko. tiedon käsittelyn tarkoitus on.

Vastaanotolla voi olla erilaisia henkilörekisterejä. Jokaisella vastaanotolla on potilasrekisteri. Tämän lisäksi voi olla erillinen asiakasrekisteri ja esim. työntekijöitä koskeva rekisteri. Kunkin henkilötietotyypin osalta on selvitettävä käsittelyn peruste. Potilastiedon osalta käsittely perustuu lakiin. Käsiteltävä henkilötieto on hyvä kuvata. Samalla on hyvä todeta, että kysymys on ns. erityisestä henkilötiedosta, jolla tarkoitetaan

arkaluonteista tietoa. Tämän suojaamiseen on kiinnitettävä erityistä huomiota. Tiedon sijainti on kirjattava ylös; sijaitseeko tieto sähköisessä järjestelmässä palvelimella, Kanta-järjestelmässä tai paperisessa arkistossa?

Potilastiedon luovuttamisesta on tarkemmat säännökset potilaslaissa: https://www.finlex.fi/fi/laki/ajantasa/1992/19920785. Yleensä vastaanotolta ei luovuteta tietoa kolmansiin maihin, eli EU:n ulkopuolelle. Mikäli näin kuitenkin tapahtuu, on huomioitava, että tällöin on varmistuttava siitä, että kolmannessa maassa sijaitseva rekisterinpitäjä on toteuttanut tietosuoja-asetuksessa määritellyt riittävät suojatoimet. On myös mahdollista, että EU-komissio on todennut kohdemaan toteuttavan riittävän tietosuojan tason. Tietosuoja-asetusta edeltäneen tietosuojadirektiivin perusteella on tehty joukko päätöksiä kolmansien maiden tietosuojan tasosta. Nämä päätökset pysyvät voimassa tietosuoja-asetuksen tultua voimaan, kunnes niitä muutetaan, ne korvataan tai kumotaan. Lisätietoa löytyy täältä: http://www.tietosuoja.fi/fi/index/rekisterinpitajalle/ilmoitusvelvollisuus/henkilotietojenulkomailleluovutus.html

On syytä huomata, että tiedon luovuttamista kolmanteen maahan on myös sen siirtäminen kolmannessa maassa sijaitsevalle palvelimelle, esim. pilvipalvelimelle. Mikäli suojatoimille asetetut kriteerit eivät täyty, edellyttää tiedon luovuttaminen ulkomaille rekisteröidyn lupaa. Tiedon luovuttaminen kolmansiin maihin on syytä mainita tietosuojaselvityksessä.

Potilastiedon säilytysaika on säädetty STM:n asetuksessa 298/2009: https://www.finlex.fi/fi/laki/alkup/2009/20090298. Yleensä säilytysaika on 12 vuotta potilaan kuolemasta, mutta tästä on poikkeuksia. Säilytysajan päätyttyä tieto on hävitettävä. Jos tietoa tarvitaan esim. tilastointia varten, on se säilytysajan päätyttyä pseudonymisoitava, eli siitä on poistettava sellainen tieto, jolla se voidaan yhdistää yksittäiseen henkilöön. Mikäli näin toimitaan, asia on hyvä kirjata. Tiedon hävittämiseksi olisi oltava säännöllinen mekanismi, joka on dokumentoitava. Jos tietoa käsittelee rekisterinpitäjän lukuun ulkopuolinen käsittelijä, on tästä tehtävä sopimus ja asia on syytä dokumentoida.

Tietosuojavastaavan nimittämistä ja vaikutusarvioinnin laatimista käsitellään tarkemmin alla. Mikäli vastaanotolla arvioidaan, että näitä ei tarvitse tehdä, on tämä arviointi ja sen perusteet kirjattava. Toiminta tietoturvahäiriöiden varalta on dokumentoitava. Tämä tarkoittaa käytännön toimenpiteitä tietoturvahäiriön korjaamiseksi ja mahdollisia ilmoituksia rekisteröidylle ja valvontaviranomaiselle.

Tiedon suojaaminen on kuvattava. Tämä voi tarkoittaa fyysistä suojaamista kuten tilojen lukitsemista tai teknistä suojaamista, kuten pääsyä tietojärjestelmiin ja sellaisen rekisteriarkkitehtuurin järjestämistä, joka sallii kullekin työntekijälle pääsyn vain hänelle tarpeellisiin tietoihin. Tiedonsiirron suojaus ja tietojärjestelmän käytön seuranta lokitietojen avulla dokumentoidaan.

Henkilöstö on koulutettava ja perehdytettävä tietosuoja-asetuksen noudattamiseen. Koulutuksen toteuttaminen on hyvä dokumentoida. Henkilöstön osalta ydinasioita lienevät tiedon käsitteleminen vastaanotolla ja rekisteröidyn oikeuksien toteuttaminen. Vastuuhenkilöille on koulutettava toiminta tietoturvahäiriötilanteissa.

Rekisteröidyn oikeuksien toteuttamiseksi olisi luotava prosessit ja nämä prosessit on syytä dokumentoida. Erityisesti tämä koskee tietojen tarkastus- ja korjauspyyntöjä ja tietojen luovutusta.

Käsittelyn peruste

Tietosuoja-asetuksen soveltamisen kannalta on tärkeää selvittää henkilötiedon käsittelyperuste. Tämä on se tekijä, joka oikeuttaa käsittelemään, eli esim. keräämään ja katselemaan tietoa. Jos käsittelylle ei ole perustetta, käsittely on kielletty. Potilasrekisterin osalta käsittelyn peruste on tietosuoja-asetuksen 6.1.a artikla: käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Potilasrekisterin ylläpitäminen perustuu potilaslakiin ja potilasasiakirjoja käsittelevään STM:n asetukseen. Henkilötiedon käsittelyperuste on oleellinen tekijä, koska rekisteröidyn oikeudet ovat erilaiset eri käsittelyperusteissa. Muut tietosuoja-asetuksen mukaiset käsittelyperusteet ovat:

- rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten;
- käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä;
- käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi;
- käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi;
- käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.

Nämä vaihtoehtoiset käsittelyperusteet tulevat kysymykseen, jos vastaanotolla on muita henkilörekistereitä kuin potilasrekisteri. Potilasrekisterin ulkopuolisen asiakasrekisterin käsittelyperuste voisi esim. olla sopimuksen täytäntöön paneminen. Usein vastaanotoilla on työnantajana työntekijöihin liittyviä tietoja, jotka muodostavat oman rekisterinsä.

On huomattava, että suostumus voi olla käsittelyperuste joissain tilanteissa myös potilastiedon kohdalla kuten nykyisin. Jos esim. potilastietoa on kerätty yhteisesti ylläpidettyyn potilastietojärjestelmään, sisältää tällainen tietojärjestelmä kunkin erillisen rekisterinpitäjän potilasrekisterin. Potilaan luvalla potilastietoa voidaan tietojärjestelmässä tai Kannassa katsoa ilman potilaan yksittäistapauksessa erikseen antamaa suostumusta myös muiden hoitoon osallistuvien henkilöiden toimesta kuin rekisterinpitäjän. Käsittelyn täytyy tällöinkin tapahtua hoitoon liittyen. Käsittely tältä osin perustuu potilaan suostumukseen. Lyhyesti sanottuna siis potilastiedon käsitteleminen on lakisääteistä silloin kun rekisterinpitäjä on itse tuottanut tiedon. Muiden tuottaman potilastiedon käsitteleminen perustuu suostumukseen.

Potilasrekisterin sisältämä tieto kuuluu EU:n tietosuoja-asetuksessa ns. *erityiseen henkilötietoryhmään*. Näistä tietoista on henkilötietolaissa käytetty termiä *arkaluonteiset tiedot*. Arkaluonteisen tiedon käsitteleminen on lähtökohtaisesti kielletty. Kiellosta on kuitenkin säädetty poikkeuksia. Kuten henkilötietolaissakin, terveydenhuoltoa koskee tietosuoja-asetuksessa poikkeus: ” …käsittely on tarpeen ennalta ehkäisevää tai työterveydenhuoltoa koskevia tarkoituksia varten, työntekijän työkyvyn arvioimiseksi, lääketieteellisiä diagnooseja varten, terveys- tai sosiaalihuollollisen hoidon tai käsittelyn suorittamiseksi…”

Rekisteröidyn oikeudet

Rekisteröidyn oikeudet ovat eräs tietosuoja-asetuksen ydinkohtia. Rekisteröidyllä on tietoon ja henkilörekisteriin liittyviä oikeuksia. Jos rekisteröity tekee näihin oikeuksiin perustuvan pyynnön rekisterinpitäjälle, rekisteröidylle on annettava viipymättä tieto niistä toimenpiteistä, joihin tämän pyynnön johdosta on ryhdytty. Tieto on annettava viimeistään kuukauden kuluttua pyynnön saamisesta. Määräaikaa voidaan jatkaa erityisestä syystä kahdella kuukaudella. Jos rekisterinpitäjä kieltäytyy toteuttamasta pyyntöä, tästä on ilmoitettava rekisteröidylle kuukauden kuluessa. Samalla on ilmoitettava rekisteröidyn oikeussuojakeinoista.

Tiedot on annettava maksutta, ellei pyyntö ole ilmeisen perusteeton tai kohtuuton. Tällöin rekisterinpitäjä voi periä kohtuullisen maksun tai kieltäytyä toteuttamasta pyyntöä. Tämä on muutos henkilötietolakiin verrattuna. Henkilötietolain mukaan pyynnön toteuttamisesta sai periä vain kohtuullisen maksun, jos edellisestä pyynnöstä oli vähemmän kuin vuosi aikaa. Tätä voitaneen paremman ohjeistuksen puutteessa pitää suuntaa antavana ohjeena tietosuoja-asetustakin sovellettaessa.

Rekisteröidylle on edelleen *annettava tarpeellinen informaatio* tietoja kerättäessä **(liite 1)**. Käytännössä tämä tapahtunee antamalla potilaalle informaatiolomake joko anamneesikaavakkeen osana tai sen mukana. Aiempaan informaatioon nähden velvollisuus on laajentunut. Esim. rekisteröidyn oikeuksista täytyy tiedottaa laajasti. Tietosisältö poikkeaa jonkin verran silloin kun tietoja ei saada rekisteröidyltä itseltään **(liite 2)**. Kuten aiemminkin tietoja ei tarvitse antaa, jos rekisteröity on saanut ne jo aiemmin.

Rekisteröidyllä on nykyisen käytännön mukaisesti *oikeus päästä tietoihinsa*. Rekisterinpitäjän on toimitettava pyynnöstä jäljennös käsiteltävistä henkilötiedoista. Jos rekisteröity pyytää useampia jäljennöksiä, rekisterinpitäjä voi periä niistä hallinnollisiin kustannuksiin perustuvan kohtuullisen maksun. Jos rekisteröity esittää pyynnön sähköisesti, tiedot on toimitettava yleisesti käytetyssä sähköisessä muodossa, paitsi jos rekisteröity toisin pyytää. Sähköinen muoto voi tarkoittaa esim. tiedon polttamista levylle tai tallentamista muistitikulle. Suojaamatonta sähköpostia ei saa käyttää potilastiedon välittämiseen (ks. tarkemmin Lääkäriliiton suositus: sähköinen viestinvaihto potilas-lääkärisuhteessa). Tämän lisäksi rekisteröidylle on annettava muita tietoja **(liite 3)**.

Rekisteröidyllä on nykyisen käytännön mukaisesti *oikeus saada epätarkka ja virheellinen tieto oikaistuksi*. Tämä ei tarkoita sitä, että rekisteröidyllä olisi oikeus päättää siitä mitä hänestä rekisteröidään tai oikeus päättää siitä mikä tieto on virheellistä. Jos tieto on kuitenkin havaittavissa virheelliseksi, se on korjattava. Rekisteröidyllä on myös *oikeus saada puutteelliset henkilötiedot täydennettyä*.

Tietosuoja-asetuksessa rekisteröidyllä on tietyin edellytyksin **(liite 4)** *oikeus tietojen poistamiseen*, eli oikeus tulla unohdetuksi. On huomattava, että tämä oikeus ei päde silloin kun tietoja käsitellään lakisääteisen velvollisuuden noudattamiseksi, kuten potilastiedon kohdalla. Jos vastaanotolla on muita rekistereitä, on tämä oikeus kuitenkin voimassa niihin nähden.

Rekisteröidyllä on *oikeus vaatia käsittelyn rajoittamista.* Tämä käytännössä lähinnä, jos rekisteröity kiistää henkilötietojen paikkansapitävyyden tai käsittely on lainvastaista ja rekisteröity henkilötietojen poistamisen sijaan vaatii niiden käsittelyn rajoittamista. Jos käsittelyä rajoitetaan, näitä henkilötietoja saa, säilyttämistä lukuun ottamatta, käsitellä ainoastaan rekisteröidyn suostumuksella taikka oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi tai toisen luonnollisen henkilön tai oikeushenkilön oikeuksien

suojaamiseksi tai tärkeää unionin tai jäsenvaltion yleistä etua koskevista syistä. Käsittelyn rajoittaminen koskee siis aktiivista käsittelemistä.

Rekisteröity voi myös *vaatia tietojen siirtoa järjestelmästä toiseen*. Tämä koskee kuitenkin vain sellaista tietoa, jota käsitellään rekisteröidyn suostumuksen perusteella tai sellaisen sopimuksen täyttämiseksi, jossa rekisteröity on osapuolena. Siirtovaatimus ei siis pääsääntöisesti koske potilastietoa, jota käsitellään lakisääteisen velvoitteen noudattamiseksi.

Rekisteröidyllä on *oikeus vastustaa tiedon käsittelemistä*, jos käsittely perustuu yleistä etua koskevan tehtävän suorittamiseen tai rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi. Oikeus ei näin ollen koske potilastietoa.

Tietosuoja-asetuksessa on säännöksiä automaattista päätöksentekoa ja profilointia koskien. Näitä ei käsitellä tässä, koska lähtökohtaisesti tällaisia toimintoja ei käytetä potilasrekisterissä. Mikäli esim. asiakasviestintää kohdennetaan profiloinnin avulla, on sitä koskeviin säännöksiin perehdyttävä.

Rekisterinpitäjän yleiset velvollisuudet

Rekisterinpitäjän on noudatettava tietosuoja-asetuksen yleisiä velvollisuuksia. Tietosuoja-asetuksessa käytetään tässä yhteydessä paljon käsitettä ”tekniset ja organisatoriset toimenpiteet”, joihin rekisterinpitäjän on ryhdyttävä. Tekniset toimenpiteet voivat olla esim. käyttöoikeuksia, ohjelmistoarkkitehtuuria ja sen kaltaisia asioita koskevia ratkaisuja. Organisatoriset toimenpiteet voinevat olla esim. henkilökunnan kouluttamista, tietoturvan vastuuttamista ja toimenpideprotokollien luomista.

Rekisterinpitäjän on toteutettava teknisiä ja organisatorisia toimenpiteitä:

- tietosuoja-asetuksen noudattamiseksi
- tietosuojaperiaatteiden, kuten tietojen minimoinnin, täytäntöönpanoa varten
    - kerätään vain tarpeellisia tietoja
    - hävitetään tarpeeton tieto
    - käsitellään tietoa vain kun se on tarpeellista
- sen varmistamiseksi, että käsitellään vain kulloinkin tarpeellisia tietoja
    - määrä
    - käsittelyn laajuus
    - säilytysaika
    - saatavilla olo.

Tietojen käsittelyn turvallisuuden varmistamiseksi rekisterinpitäjän on lisäksi toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet:

- henkilötietojen pseudonymisointi ja salaus; pseudonymisointi tarkoittaa tiedon muokkaamista siten, että sitä ei voida yhdistää yksittäiseen henkilöön
    - tämä voi olla tarpeen, jos tietoa tarvitaan esim. tilastointia varten, mutta sen liittäminen yksittäiseen henkilöön ei ole enää tarpeellista
    - salauksella estetään ulkopuolisten pääsy tietoon
- kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;
    - luottamuksellisuus: pääsy koneelle aina salasanalla, ei jätetä konetta auki käytön jälkeen, päivitykset, virustorjunta, palomuuri

  - eheys: enemmänkin ohjelmistotoimittajan asia, jos käytät sähköistä potilastietojärjestelmää, tiedon muuttumattomuus, säilyvyys
  - käytettävyys: ohjelmisto ja laite toimii
- kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;
  - varmuuskopiointi
- menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

Rekisterinpitäjän on varmistettava, että sen palveluksessa olevat henkilöt käsittelevät tietoa vain rekisterinpitäjän ohjeiden mukaisesti. Tämä tarkoittaa henkilökunnan kouluttamista tietoturva-asioissa ja mahdollisesti sellaista rekisteriarkkitehtuuria, missä pääsy eri tietoryhmiin on rajattu henkilön tehtävien mukaan.

Rekisterinpitäjän ja tarvittaessa rekisterinpitäjän edustajan on ylläpidettävä selostetta vastuullaan olevista käsittelytoimista. Kyseessä on nykyistä rekisteriselostetta vastaava asiakirja, joka tosin on aiempaa laajempi **(liite 5)**.

Tietoturvaloukkaukset ja niistä ilmoittaminen

Tietoturvaloukkaus voi tarkoittaa tiedon tuhoutumista, jolloin tieto on hävinnyt tai se ei ole enää sellaisessa muodossa, jossa sitä voidaan käyttää. Tietoturvaloukkaus voi tarkoittaa myös tiedon vahingoittumista, jolloin tietoa on muutettu tai se ei ole enää täydellistä. Tieto voi myös kadota, jolloin tieto sinällään voi olla olemassa, mutta se ei ole enää rekisterinpitäjän hallinnassa. Lisäksi tietoturvaloukkaus voi tarkoittaa tiedon oikeudetonta luovuttamista tai oikeudetonta pääsyä tietoon, esim. tietomurto.

Tietoturvaloukkauksista on ilmoitettava sekä valvontaviranomaiselle että rekisteröidylle **(liite 6a-b)**. Ilmoitusta valvontaviranomaiselle ei tarvitse tehdä, jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa *riskiä*. Rekisteröidylle ilmoitus on tehtävä, jos tietoturvaloukkaus aiheuttaa *korkean riskin* henkilön oikeuksille ja vapauksille. Ilmoitukset valvontaviranomaiselle ja rekisteröidylle tehdään siis osittain eri perustein.

Riskiä arvioitaessa on otettava huomioon

- millaisesta loukkauksesta on kysymys
- millaisesta tiedosta on kysymys
  - terveydenhuollon arkaluonteinen tieto aiheuttaa herkemmin korkean riskin
  - ilmoitus rekisteröidylle lienee näin ollen lähtökohtaisesti aiheellinen
- henkilöiden tunnistamisen helppous
- tietoturvaloukkauksen vaikutukset henkilölle
- onko henkilö erityisen suojan tarpeessa

Valvontaviranomaiselle ilmoitus on tehtävä 72 tunnin kuluessa loukkauksen ilmitulosta. Rekisteröidylle ilmoitus on tehtävä ilman aiheetonta viivytystä. Rekisterinpitäjän on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset, mukaan lukien henkilötietojen tietoturvaloukkaukseen liittyvät seikat, sen vaikutukset ja toteutetut korjaavat toimet.

Ilmoitusta rekisteröidylle ei vaadita, jos jokin seuraavista edellytyksistä täyttyy:

a) rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet ja henkilötietojen tietoturvaloukkauksen kohteena oleviin henkilötietoihin on sovellettu kyseisiä toimenpiteitä, erityisesti niitä, joiden avulla henkilötiedot muutetaan muotoon, jossa ne eivät ole sellaisten henkilöiden ymmärrettävissä, joilla ei ole lupaa päästä tietoihin, kuten salausta;

- käytännössä siis korjaavat toimenpiteet on kohdistettu tietoturvaloukkauksen kohteena olleen henkilön henkilötietoon

b) rekisterinpitäjä on toteuttanut jatkotoimenpiteitä, joilla varmistetaan, että 1 kohdassa tarkoitettu rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu;

- liittynee edelliseen kohtaan, varmistetaan ettei jatkossa vastaavaa pääse tapahtumaan

c) se vaatisi kohtuutonta vaivaa. Tällaisissa tapauksissa on käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröidyille tiedotetaan yhtä tehokkaalla tavalla.

- harvinainen poikkeus

Vaikutustenarviointi

Tietosuoja-asetus velvoittaa rekisterinpitäjän tekemään tietyin edellytyksin tietosuojaa koskevan vaikutustenarvioinnin. Vaikutustenarviointi vaaditaan, mikäli henkilötietojen käsittely todennäköisesti aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin. Rekisterinpitäjän on siis arvioitava näiden tunnusmerkkien täyttymistä.

EU:n tietosuojatyöryhmä on kirjannut 9 kriteeriä korkean riskin toteutumisen arvioimiseen. Näistä kriteereistä yleisimmin terveydenhuollossa toteutuvat kohta 4. arkaluonteisten tietojen käsittely ja kohta 7. heikossa asemassa olevien rekisteröityjen, eli esim. lapsien, mielenterveysongelmaisten ja ikääntyneiden tietojen käsitteleminen.

Tietosuojatyöryhmän näkemyksen mukaan kaksi kriteeriä täyttävä käsittely edellyttäisi tietosuojaa koskevan vaikutustenarvioinnin tekemisen. Työryhmän ohjeessa kuitenkin on katsottu, että yksittäisen lääkärin tai muun terveydenhuollon ammattilaisen käsittely ei edellyttäisi vaikutustenarviointia. Sen sijaan sairaalan olisi vaikutustenarviointi tehtävä.

Ohjetta voitaneen tulkita siten, että siinä on annettu huomattava paino sille miten laajamittaista käsittely on. Sairaalan tietojenkäsittely on laajamittaista, mutta yksittäisen lääkärin käsittely koskee varsin rajattua henkilöpiiriä. Ohjeessa ei oteta kantaa siihen missä vaiheessa vaikutustenarviointi tulee pakolliseksi. Miten on esim. arvosteltava pienen ryhmävastaanoton tietojenkäsittelyä? Toistaiseksi on mahdotonta antaa tähän varmaa vastausta, mutta mitä suurempi vastaanotto on kyseessä, sitä laajamittaisempaa käsittely on ja sitä todennäköisemmin vaikutustenarviointi tulee tehtäväksi. Epäselvässä tilanteessa suositellaan vaikutustenarvioinnin tekemistä.

Jos rekisterinpitäjä katsoo, että kriteerien täyttymisestä huolimatta tietojen käsittely ei aiheuta korkeaa riskiä, se voi jättää vaikutustenarvioinnin tekemättä. Tällöin on syytä huolella perustella ja dokumentoida ne syyt, minkä vuoksi katsoo, että korkea riski ei täyty. Olosuhteiden muuttuminen toiminnan aikana on myös otettava huomioon. Velvollisuus vaikutustenarvioinnin tekemiseen voi syntyä myös toiminnan aikana.

Vaikutustenarviointi sisältää vähintään

- kuvauksen suunnitelluista käsittelytoimista ja käsittelyn tarkoituksesta
- arvion käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta
- arvion rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä
- suunnitellut toimenpiteet riskeihin puuttumiseksi ja sen osoittamiseksi, että tietosuoja-asetusta on noudatettu

Tarkemmat ohjeet:
http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/ibVehxmcp/Ohjeet_tietosuojaa_koskevasta_vaikutustenarvioinnista.pdf

Tietosuojavastaava

Rekisterinpitäjien ja henkilötietojen käsittelijöiden on varmistuttava siitä, onko organisaatioon asetuksen mukaan nimettävä tietosuojavastaava. Tietosuojavastaavan tehtävänä on muun muassa seurata henkilötietojen käsittelyn lainmukaisuutta ja auttaa organisaatiota toteuttamaan lainsäädännön asettamat velvoitteet. Tietosuojavastaavan tehtävänä on myös toimia valvontaviranomaisen sekä rekisteröityjen yhteyspisteenä henkilötietojen käsittelyyn liittyvissä kysymyksissä. Tästä johtuen organisaation on julkistettava tietosuojavastaavan yhteystiedot ja ilmoitettava ne valvontaviranomaiselle.

Tietosuojavastaava on nimitettävä, jos

a) tietojenkäsittelyä suorittaa viranomainen tai julkishallinnon elin
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 tai rikostuomioita tai rikkomuksia koskeviin tietoihin.

Yksityisten lääkärivastaanottojen kohdalla kyseeseen tulee lähinnä kohta c). Terveydenhuollossa tiedon käsittely on sillä tavoin kiinteässä yhteydessä ydintoimintaan, että kriteeri voi täyttyä. Tällöinkin oleellista on se, onko käsittelyä pidettävä laajamittaisena. Tähän vaikuttavat potilaiden lukumäärä, käsiteltävä tietomäärä, käsittelyn kesto ja maantieteellinen laajuus.

Kuten vaikutustenarvioinninkin kohdalla EU:n tietosuojatyöryhmä on katsonut, että pääsääntöisesti yksittäisen lääkärin suorittama potilastietojen käsittely ei ole sillä tavoin laajamittaista, että tietosuojavastaavan nimittäminen olisi pakollista. Sen sijaan sairaalan tietojenkäsittely todennäköisesti on laajamittaista. Näiden välillä arvion tekemisessä viitataan vaikutustenarvioinnin yhteydessä esitettyyn.

Tietosuojavastaavaksi voidaan haluttaessa nimittää organisaation ulkopuolinen henkilö tai tehtävä voidaan ulkoistaa ulkopuoliselle organisaatiolle. Tietosuojavastaavan tehtävien suorittamisen jouhevuuden kannalta lienee kuitenkin ensisijainen vaihtoehto nimittää tehtävään henkilö organisaation sisältä. Pienellä vastaanotolla tähän ei kuitenkaan aina ole mahdollisuutta. Pienen vastaanoton ei toisaalta yleensä ole pakko nimittää tietosuojavastaavaa. Tietosuojavastaavan yhteystiedot on oltava saatavilla vastaanotolla. Tietosuojavastaavaan on myös tosiasiallisesti voitava ottaa yhteyttä.

Tietosuojavastaavalle ei ole määritelty kelpoisuusehtoja. Tietosuojavastaavalla on oltava tehtävän suorittamisen kannalta riittävä asiantuntemus esim. tietosuojalainsäädännöstä ja alan käytänteistä. Toimialan ja rekisterinpitäjän organisaation tuntemus ovat eduksi.

Mikäli vastaanotolla katsotaan, että tietosuojavastaavan nimittäminen ei ole tarpeen, on syytä dokumentoida miten ja millä perusteilla tähän johtopäätökseen on päädytty.

Tarkemmat ohjeet:

http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/UvreCmOiN/Tietosuojavastaavia_koskevat_ohjeet_wp243rev01_fi.pdf

Yhteisrekisterinpitäjät

Kaksi tai useampi rekisterinpitäjä, jotka määrittelevät yhdessä käsittelyn tavoitteet ja keinot, voivat toimia yhteisrekisterinpitäjinä. Tällöin yhteisrekisterinpitäjien on sovittava keskenään tietosuoja-asetuksen velvoitteiden jaosta. Tällainen järjestely voi tulla kyseeseen useamman erillisen yrityksen ryhmävastaanotolla. Velvoitteiden jaossa on huolehdittava siitä, että kaikki velvoitteet tulevat varmasti katetuksi ja että vastuunjako on selkeä. Velvoitteiden jako on dokumentoitava ja se on voitava tarvittaessa esittää rekisteröidylle.

Käsittelijä

Rekisterinpitäjä voi käyttää henkilötietojen käsittelijää, joka käsittelee tietoa rekisterinpitäjän lukuun. Näin voi olla vuokrasuhteessa. Vuokralaisen potilasrekisteristä tai ainakin joistakin siihen liittyvistä tehtävistä huolehtii vuokralaisen puolesta vuokranantaja. Vuokranantaja on tällöin henkilötietojen käsittelijä suhteessa vuokralaisen potilastietoon. Käsittelijän toiminnan täytyy täyttää tietosuoja-asetuksen vaatimukset.

Rekisterinpitäjä ei voi kuitenkaan välttyä omalta vastuultaan käyttämällä henkilötiedon käsittelijää. Rekisterinpitäjän on näin ollen huolehdittava myös siitä, että sen oma toiminta tietoa käsiteltäessä täyttää tietosuoja-asetuksen vaatimukset. Näin ollen rekisterinpitäjä ei välty esim. dokumentointivelvollisuudeltaan käyttämällä käsittelijää.

Rekisterinpitäjän ja käsittelijän on tehtävä keskenään sopimus tiedon käsittelystä. Tietosuoja-asetus määrää sopimuksen minimisisällön **(liite 7)**.

liite 1 rekisteröidylle annettavat tiedot kun tiedot kerätään rekisteröidyltä

a) rekisterinpitäjän ja tapauksen mukaan tämän mahdollisen edustajan identiteetti ja yhteystiedot;

b) tapauksen mukaan tietosuojavastaavan yhteystiedot (jos on nimetty);

c) henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste;

d) rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut, jos käsittely perustuu näihin etuihin;

e) henkilötietojen vastaanottajat tai vastaanottajaryhmät;

f) tapauksen mukaan tieto siitä, että rekisterinpitäjä aikoo siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle

g) henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit (määritellään STM:n asetuksessa);

h) rekisteröidyn oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten tietojen oikaisemista tai poistamista (ei koske lakisääteisesti käsiteltävää tietoa) taikka käsittelyn rajoittamista tai vastustaa käsittelyä (sekä oikeutta siirtää tiedot järjestelmästä toiseen);

i) oikeus peruuttaa suostumus milloin tahansa tämän vaikuttamatta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen, jos käsittely perustuu rekisteröidyn suostumukseen;

j) oikeus tehdä valitus valvontaviranomaiselle;

k) onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus taikka sopimuksen tekemisen edellyttämä vaatimus sekä onko rekisteröidyn pakko toimittaa henkilötiedot ja tällaisten tietojen antamatta jättämisen mahdolliset seuraukset;

l) automaattisen päätöksenteon, muun muassa profiloinnin olemassaolo, sekä ainakin näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle.

Jos rekisterinpitäjä aikoo käsitellä henkilötietoja muuhun tarkoitukseen kuin siihen, johon henkilötiedot kerättiin, rekisterinpitäjän on ilmoitettava rekisteröidylle ennen kyseistä jatkokäsittelyä tästä muusta tarkoituksesta ja annettava kaikki asiaankuuluvat lisätiedot yllä olevan mukaisesti.

liite 2 rekisteröidylle annettavat tiedot kun tiedot kerätään muulta kuin rekisteröidyltä

a) rekisterinpitäjän ja tämän mahdollisen edustajan identiteetti ja yhteystiedot;

b) tapauksen mukaan mahdollisen tietosuojavastaavan yhteystiedot (jos on nimetty);

c) henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste;

d) kyseessä olevat henkilötietoryhmät;

e) mahdolliset henkilötietojen vastaanottajat tai vastaanottajaryhmät;

f) tarvittaessa tieto siitä, että rekisterinpitäjä aikoo siirtää henkilötietoja kolmannessa maassa olevalle vastaanottajalle tai kansainväliselle järjestölle

a) henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit;

b) rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut, jos käsittely perustuu näihin etuihin;

c) rekisteröidyn oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten tietojen oikaisemista tai poistamista (ei koske lakisääteisesti käsiteltävää tietoa) taikka käsittelyn rajoittamista ja vastustaa käsittelyä (sekä oikeutta siirtää tiedot järjestelmästä toiseen);

d) oikeus peruuttaa suostumus milloin tahansa tämän vaikuttamatta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen, jos käsittely perustuu rekisteröidyn suostumukseen;

e) oikeus tehdä valitus valvontaviranomaiselle;

f) mistä henkilötiedot on saatu sekä tarvittaessa se, onko tiedot saatu yleisesti saatavilla olevista lähteistä;

g) automaattisen päätöksenteon, muun muassa profiloinnin olemassaolo, sekä ainakin näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle.

Jos rekisterinpitäjä aikoo käsitellä henkilötietoja muuhun tarkoitukseen kuin siihen, johon henkilötiedot kerättiin, rekisterinpitäjän on ilmoitettava rekisteröidylle ennen kyseistä jatkokäsittelyä tästä muusta tarkoituksesta ja annettava kaikki asiaankuuluvat lisätiedot yllä olevan mukaisesti.

liite 3 rekisteröidylle tarkastusoikeuden toteuttamisen yhteydessä annettavat tiedot

a) käsittelyn tarkoitukset;

b) kyseessä olevat henkilötietoryhmät;

c) vastaanottajat tai vastaanottajaryhmät, erityisesti kolmansissa maissa olevat vastaanottajat tai kansainväliset järjestöt, joille henkilötietoja on luovutettu tai on tarkoitus luovuttaa;

d) mahdollisuuksien mukaan henkilötietojen suunniteltu säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit (määritellään STM:n potilasasiakirja-asetuksessa);

e) rekisteröidyn oikeus pyytää rekisterinpitäjältä häntä itseään koskevien henkilötietojen oikaisemista tai poistamista (ei koske lakisääteisesti käsiteltävää tietoa) taikka henkilötietojen käsittelyn rajoittamista tai vastustaa tällaista käsittelyä;

f) oikeus tehdä valitus valvontaviranomaiselle;

g) jos henkilötietoja ei kerätä rekisteröidyltä, kaikki tietojen alkuperästä käytettävissä olevat tiedot;

h) automaattisen päätöksenteon, muun muassa profiloinnin olemassaolo, sekä ainakin näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle

liite 4 kriteerit, joilla rekisteröity saa vaatia tietojen poistamista rekisteristä

a) henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä muutoin käsiteltiin;

b) rekisteröity peruuttaa suostumuksen, johon käsittely on perustunut, eikä käsittelyyn ole muuta laillista perustetta;

c) rekisteröity vastustaa käsittelyä vastustamisoikeuden nojalla eikä käsittelyyn ole olemassa perusteltua syytä tai rekisteröity vastustaa käsittelyä suoramarkkinointitarkoituksiin;

d) henkilötietoja on käsitelty lainvastaisesti;

e) henkilötiedot on poistettava unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan rekisterinpitäjään sovellettavan lakisääteisen velvoitteen noudattamiseksi;

f) henkilötiedot on kerätty tietoyhteiskunnan palvelujen tarjoamisen yhteydessä.

liite 5 selosteen sisältö

a) rekisterinpitäjän ja mahdollisen yhteisrekisterinpitäjän, rekisterinpitäjän edustajan ja tietosuojavastaavan nimi ja yhteystiedot;

b) käsittelyn tarkoitukset;

c) kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä; ks. yleinen tietosuoja-asetus: L 119/50 FI Euroopan unionin virallinen lehti 4.5.2016

d) henkilötietojen vastaanottajien ryhmät, joille henkilötietoja on luovutettu tai luovutetaan, mukaan lukien kolmansissa maissa tai kansainvälisissä järjestöissä olevat vastaanottajat;

e) tarvittaessa tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle, mukaan lukien tieto siitä, mikä kolmas maa tai kansainvälinen järjestö on kyseessä, sekä asianmukaisia suojatoimia koskevat asiakirjat, jos kyseessä on 49 artiklan 1 kohdan toisessa alakohdassa tarkoitettu siirto;

f) mahdollisuuksien mukaan eri tietoryhmien poistamisen suunnitellut määräajat;

g) mahdollisuuksien mukaan yleinen kuvaus 32 artiklan 1 kohdassa tarkoitetuista teknisistä ja organisatorisista turvatoimista.

liite 6a ilmoitus valvontaviranomaiselle tietoturvaloukkauksesta

a) kuvattava henkilötietojen tietoturvaloukkaus, mukaan lukien mahdollisuuksien mukaan asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät;

b) ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa;

c) kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset;

d) kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

liite 6b Ilmoitus rekisteröidylle tietoturvaloukkauksesta

a) ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa;

b) kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset;

c) kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

liite 7 tietojen käsittelijän kanssa tehtävän sopimuksen vähimmäissisältö

Henkilötietojen käsittelijän suorittamaa käsittelyä on määritettävä sopimuksella käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät, rekisterinpitäjän velvollisuudet ja oikeudet. Tässä sopimuksessa tai muussa oikeudellisessa asiakirjassa on sovittava erityisesti, että henkilötietojen käsittelijä

a) käsittelee henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti;
b) varmistaa, että henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus;
c) toteuttaa kaikki 32[1] artiklassa vaaditut toimenpiteet;
d) noudattaa 2 ja 4 kohdassa[2] tarkoitettuja toisen henkilötietojen käsittelijän käytön edellytyksiä;
e) ottaen huomioon käsittelytoimen luonteen auttaa rekisterinpitäjää asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä mahdollisuuksien mukaan täyttämään rekisterinpitäjän velvollisuuden vastata pyyntöihin, jotka koskevat rekisteröidyn oikeuksien käyttämistä;

---

[1] *32 artikla*

Käsittelyn turvallisuus

1. Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten

a) henkilötietojen pseudonymisointi ja salaus;

b) kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;

c) kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;

d) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

2. Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi.

3. Jäljempänä 40 artiklassa tarkoitettujen hyväksyttyjen käytännesääntöjen tai 42 artiklassa tarkoitetun hyväksytyn sertifiointimekanismin noudattamista voidaan käyttää yhtenä tekijänä sen osoittamiseksi, että tämän artiklan 1 kohdassa asetettuja vaatimuksia noudatetaan.

4. Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava toimenpiteet sen varmistamiseksi, että jokainen rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti, ellei unionin oikeudessa tai jäsenvaltion lainsäädännössä toisin vaadita.

[2] 2. Henkilötietojen käsittelijä ei saa käyttää toisen henkilötietojen käsittelijän palveluksia ilman rekisterinpitäjän erityistä tai yleistä kirjallista ennakkolupaa. Kun kyse on kirjallisesta ennakkoluvasta, henkilötietojen käsittelijän on tiedotettava rekisterinpitäjälle kaikista suunnitelluista muutoksista, jotka koskevat muiden henkilötietojen käsittelijöiden lisäämistä tai vaihtamista, ja annettava siten rekisterinpitäjälle mahdollisuus vastustaa tällaisia muutoksia.

4. Kun henkilötietojen käsittelijä käyttää toisen henkilötietojen käsittelijän palveluksia erityisten käsittelytoimintojen suorittamiseksi rekisterinpitäjän puolesta, kyseiseen toiseen henkilötietojen käsittelijään sovelletaan sopimuksen tai unionin oikeuden tai jäsenvaltion lainsäädännön mukaisen muun oikeudellisen asiakirjan mukaisesti samoja tietosuojavelvoitteita kuin ne, jotka on vahvistettu 3 kohdassa tarkoitetussa rekisterinpitäjän ja henkilötietojen käsittelijän välisessä sopimuksessa tai muussa oikeudellisessa asiakirjassa erityisesti antaen riittävät takeet siitä, että käsittelyyn liittyvät asianmukaiset tekniset ja organisatoriset toimet toteutetaan niin, että käsittely täyttää tämän asetuksen vaatimukset. Kun toinen henkilötietojen käsittelijä ei täytä tietosuojavelvoitteitaan, alkuperäinen henkilötietojen käsittelijä on edelleen täysimääräisesti vastuussa toisen henkilötietojen käsittelijän velvoitteiden suorittamisesta suhteessa rekisterinpitäjään.

f) auttaa rekisterinpitäjää varmistamaan, että 32–36 artiklassa säädettyjä velvollisuuksia noudatetaan ottaen huomioon käsittelyn luonteen ja henkilötietojen käsittelijän saatavilla olevat tiedot;
g) rekisterinpitäjän valinnan mukaan poistaa tai palauttaa käsittelyyn liittyvien palveluiden tarjoamisen päätyttyä kaikki henkilötiedot rekisterinpitäjälle ja poistaa olemassa olevat jäljennökset, paitsi jos unionin oikeudessa tai jäsenvaltion lainsäädännössä vaaditaan säilyttämään henkilötiedot;
h) saattaa rekisterinpitäjän saataville kaikki tiedot, jotka ovat tarpeen tässä artiklassa säädettyjen velvollisuuksien noudattamisen osoittamista varten, ja sallii rekisterinpitäjän tai muun rekisterinpitäjän valtuuttaman auditoijan suorittamat auditoinnit, kuten tarkastukset, sekä osallistuu niihin.

liite 8 tietosuojaselvityksen runko

1. Mitä tietoja vastaanotolla käsitellään?
2. Mistä tiedot saadaan?
3. Mihin tietoa luovutetaan? Luovutetaanko tietoa EU:n ulkopuolelle?
4. Mitkä ovat eri tietojen käyttötarkoitukset
5. Mikä on käsittelyn peruste eri tietojen osalta?
6. Missä tietoa säilytetään? Mikä on vanhentuneen tiedon hävittämismekanismi?
7. Kuinka kauan tietoa säilytetään?
8. Onko tietosuojavastaava nimitetty? Jos ei, miksi?
9. Onko laadittu vaikutustenarviointi? Jos ei, miksi?
10. Miten tieto on suojattu? Miten tiedonsiirto on suojattu?
11. Miten henkilöstö on perehdytetty ja koulutettu tietosuoja-asetuksen noudattamiseen?
12. Millaisia prosesseja vastaanotolla on rekisteröidyn oikeuksien toteuttamiseksi?