

Liite 2 Tilaajan ohjeet Palveluntuottajalle

Palveluntuottaja saa käsitellä henkilötietoja ainoastaan Tilaajan antamien dokumentoitujen ohjeiden mukaisesti. Tilaajan tässä dokumentissa antamat ohjeet perustuvat Henkilötietojen Käsittelyn Ehtoihin ja numerointi viittaa Ehtojen vastaaviin kohtiin.

3. Palveluntuottajan yleiset velvollisuudet

3.2 Tekniset ja organisatoriset turvatoimet

A. Ohjeistus Palveluntuottajalle, kun Palveluntuottaja käsittelee henkilötietoja **Tilaajan tietojärjestelmässä**:

Palveluntuottaja käsittelee henkilötietoja vain Tilaajan kirjallisesta yksilöidystä toimeksiannosta Tilaajan määrittelemässä laajuudessa Tilaajan antaman käyttöoikeuden perusteella.

Palveluntuottajan on ilmoitettava viipymättä Tilaajalle kaikista Tilaajan tietojärjestelmän käyttöön liittyvistä muutoksista.

Palveluntuottajan vastuut ja velvoitteet kuvataan tarkemmin Tilaajan ja Palveluntuottajan välisessä tietojärjestelmäsopimuksessa.

B. Ohjeistus Palveluntuottajalle, kun henkilötiedot ovat **Palveluntuottajan tietojärjestelmässä**:

Palveluntuottajan tulee nimetä tietojärjestelmälle omistaja ja vastuhenkilö tai pääkäyttäjä. Palveluntuottajan tulee dokumentoida tietojärjestelmän valvonta- ja ylläpitovastuut. Palveluntuottajan tulee dokumentoida menettelytavat, joihin perustuen järjestelmän teknistä ja organisatorista turvallisuutta testataan ja arvioidaan säännöllisesti.

Palveluntuottajan tulee arvioida ja dokumentoida tietojärjestelmään kohdistuvat tietoturvaohaukset, analysoida riskit (esim. sivullisen pääsy tietoihin, tietosuojarikkomukset, tietojen katoaminen) sekä laatia niistä hallinta-, suojaus- ja toipumissuunnitelma. Palveluntuottajalla tulee olla tietojärjestelmänsä ajantasaiset, riskiarvion mukaiset dokumentaatiot (esim. prosessi-, käyttötapaus-, tietovirta-, liittymä- ja verkkodokumentaatiot).

Palveluntuottajan tulee dokumentoida ja luokitella tietojärjestelmässä käsiteltävät tietosisällöt (henkilötietoryhmät).

Palveluntuottajan tulee suojata erityiset henkilötietoryhmät tietosuojalain 6 §:n mukaisesti käsittelyn riskitasoon suhteuttaen.

Tietojärjestelmän tulee kirjata lokiin Tilaajan henkilötietojen käsittelytoimet (esim. muutokset, poistot) ja käsittelyn ajankohta käyttäjätasolla. Erityisten henkilötietoryhmien osalta tulee lokiin kirjata myös tietojen katselu. Tietojärjestelmän lokien on oltava suojattu muutoksilta ja Palveluntuottajan on rajoitettava niihin pääsy käyttöoikeuksin vain ylläpitohenkilöstölle. Lokien on tuotettava käyttökelpoista informaatiota henkilötietojen käsittelystä, jotta tapahtumia pystytään tarvittaessa tosiasiallisesti selvittämään. Palveluntuottajan on pyydyttävä ja ilman aiheetonta viivytystä toimitettava em. käyttöoikeudet ja lokitiedot Tilaajalle veloitusetta.

Henkilötietojen käsittely tulee minimoida niin, että Palveluntuottajan toimesta käsitellään vain käyttötarkoitukseen nähden tarpeellisia henkilötietoja. Palveluntuottajan tulee toteuttaa sisäänrakennetun ja oletusarvoisen tietosuojan vaatimukset.

Palveluntuottajan tulee suojata tietoliikenneyhteydet käyttämiensä tietojärjestelmien välillä asianmukaisia tiedonsiirtoprotokollia käyttäen.

Palveluntuottajan on huomioitava tietosuoja- ja tietoturva-vaatimukset myös sovelluskehityksessä.

Palveluntuottajan ei tule käyttää tietojärjestelmän testauksessa Tilaajan henkilötietoa.

Palveluntuottajan tulee laatia pääsynvalvontaperiaatteet pääsyoikeuksia varten:

- Järjestelmän käyttäjän luonti-, muutos ja poistoprosessi oltava kuvattuna.
- Järjestelmän käyttöoikeuksien säännöllinen tarkastaminen oltava kuvattuna.
- Kaikilla järjestelmän käyttäjillä tulee olla henkilökohtaiset käyttäjätunnukset.
- Kaikki järjestelmän käyttäjät tulee olla dokumentoituna (myös pääkäyttäjät ja ylläpitäjät)
- Mikäli järjestelmään kirjaututaan käyttäjätunnuksella ja salasanalla, Palveluntuottajan tulee kuvata salasanapolitiikka tai mikäli järjestelmään kirjaututaan toimikortilla, tulee sen toiminta kuvata.

Yksittäisen käyttäjän kirjautumiset/epäonnistuneet kirjautumiset on pystyttävä tarvittaessa jälkikäteen selvittämään, mikäli tämä on riskiarvion perusteella tarpeen.

Palveluntuottajan tulee laatia tietojärjestelmän varmuuskopiointisuunnitelma:

- Erilaiset tietojen palautustarpeet huomioidaan.
- Varmuuskopiot suojataan asianmukaisesti.
- Varmuuskopioiden palauttamista testataan säännöllisesti.

Palveluntuottajan tulee toteuttaa tietojärjestelmän tietoturvapäivitykset riskiarvion mukaisesti riittävällä tasolla.

C. Ohjeistus Palveluntuottajalle, kun henkilötietoja käsitellään **analogisesti (paperiaineisto)**:

Henkilötietoja sisältävä analoginen aineisto on säilytettävä lukitussa tilassa, johon pääsyä valvotaan. Ko. aineiston säilyttämiseen käytettävän lukitun tilan pääsyvalvonnan suorittamistapa tulee dokumentoida kirjallisesti.

Henkilötietoja sisältävään analogiseen aineistoon kohdistuvista häiriö- tai ongelmatilanteista, kuten esimerkiksi vesivahingoista, tulipaloista, murroista tms., tulee ilmoittaa Tilaajalle viivytyksettä.

Palveluntuottaja saa suorittaa Tilaajan lukuun tarkoituksenmukaisia tiedonsiirtoja vain Tilaajan kirjallisten ohjeiden mukaisesti.

3.5. Tilaaja voi esimerkiksi pyytää Palveluntuottajaa täydentämään tai päivittämään laadittuja dokumentteja, joihin tarvitaan henkilötietojen käsittelijän kuvauksia henkilötietojen käsittelyn toteuttamisesta. Mahdolliset ennakkokuulemiset ja niiden ajankohdat ilmoitetaan Palveluntuottajalle etukäteen

3.6 Ohjeistus palveluntuottajalle rekisteröityjen **tieto- ja tarkastuspyyntöjä** koskien:

1. Palveluntuottajan tulee ohjeistaa rekisteröityjä toimittamaan tarkastuspyynnöt Tilaajan ohjeiden mukaisesti suoraan Pohjois-Pohjanmaan hyvinvointialueen kirjaamoon (Pohjois-Pohjanmaan hyvinvointialue, Kirjaamo, PL 10, 90029 Pohde).
2. Mikäli rekisteröity esittää em. pyynnön suullisesti, Palveluntuottajan tulee ensisijaisesti ohjeistaa rekisteröityä kirjallisen pyynnön tekemiseen. Jos kirjallinen pyyntö ei ole mahdollinen, Palveluntuottaja tulee ottaa suullinen pyyntö vastaan ja varmistaa pyytäjän henkilöllisyys ja toimittaa pyyntö Pohjois-Pohjanmaan hyvinvointialueen kirjaamoon.

3. Palveluntuottajan tulee Tilaajan pyynnöstä toimittaa pyydettyt tiedot pyydettyssä muodossa viipymättä Tilaajalle. Tilaaja toimittaa pyydettyt tiedot rekisteröidylle saatuaan ne Palveluntuottajalta.

5. Palveluhenkilöstö

5.1. Tilaajan niin edellyttäessä, kaikkien Palveluntuottajan alaisuudessa toimivien henkilöiden, joilla on pääsy henkilötietoihin ja/tai oikeus käsitellä henkilötietoja, tulee lukea ja allekirjoittaa Tilaajan Tietoturva- ja käyttäjäsitoumus ja suorittaa Tilaajan tarjoama tietoturvan ja tietosuojan verkkokoulutus.

6. Alihankkijat, jotka käsittelevät henkilötietoja

6.2. Palveluntuottajan mahdollisella alihankkijalla, jonka Tilaaja on hyväksynyt, tulee olla vastaava kelpoisuus ja palvelun tuottamisen edellytykset kuin Palveluntuottajalla.

6.4. Palveluntuottajan tulee perehdyttää alihankkijat Ehtoihin ja Tilaajan ohjeisiin. Alihankkijoiden tulee Tilaajan niin edellyttäessä lukea ja allekirjoittaa Tilaajan Tietoturva- ja käyttäjäsitoumus ja suorittaa Tilaajan tarjoama tietoturvan ja tietosuojan verkkokoulutus.

9. Henkilötietojen käsittelyn päättymisen

9.2. Henkilötietojen käsittely sopimuksen päättyessä tai purkautuessa

- A. Ohjeistus Palveluntuottajalle **analogista (paperimuotoista)** aineistoa koskien, mikäli asiakirjoja ei ole siirretty Tilaajalle aikaisemmin:

Sopimuksen päättyessä tai purkautuessa Palveluntuottaja tulee toimittaa Tilaajalle hallussaan olevat Tilaajan aineistot järjestettynä ja luetteloituna analogisena tai digitoituna Tilaajan ohjeistuksen mukaisesti.

- B. Ohjeistus Palveluntuottajalle **sähköistä aineistoa** koskien, mikäli asiakirjoja ei ole siirretty Tilaajalle aikaisemmin:

Sopimuksen päättyessä tai purkautuessa Palveluntuottaja siirtää sähköisessä muodossa olevat henkilötiedot Tilaajan järjestelmään Tilaajan kulloinkin erikseen ohjeistamalla tavalla.

Palveluntuottajan tulee Tilaajan pyynnöstä esittää poistamisesta riittävä selvitys.

- C. Jos Palveluntuottaja käsittelee omassa järjestelmässään Tilaajan pitkään (yli 20 vuotta) tai pysyvästi säilytettävää aineistoa, Palveluntuottaja on velvollinen siirtämään em. henkilötiedot Tilaajalle säännöllisesti ja ilman erillisiä kustannuksia Tilaajan tarkemman ohjeistuksen mukaisesti.

Jos sähköinen siirto ei ole mahdollinen, niin Palveluntuottajan tulee siirtää em. henkilötiedot analogisessa muodossa säännöllisesti noudattaen edellä kuvattua analogisen aineiston siirto-ohjeistusta.