Pohde
Pohjois-Pohjanmaan hyvinvointialue

Liite 2 Rekisterinpitäjän ohjeet Käsittelijälle

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

3. Käsittelijän yleiset velvollisuudet

3.2 Tekniset ja organisatoriset turvatoimet

A. Ohjeistus Käsittelijälle, kun Käsittelijä käsittelee henkilötietoja **Rekisterinpitäjän tietojärjestelmässä**:

Käsittelijä käsittelee henkilötietoja vain Rekisterinpitäjän kirjallisesta yksilöidystä toimeksiannosta Rekisterinpitäjän määrittelemässä laajuudessa Rekisterinpitäjän antaman käyttöoikeuden perusteella. Käsittelijän tulee ylläpitää selostetta kaikista Rekisterinpitäjän lukuun suoritettavista käsittelytoimista tietosuoja-asetuksen 30 artiklan mukaisesti.

Käsittelijän on ilmoitettava viipymättä Rekisterinpitäjälle kaikista Rekisterinpitäjän tietojärjestelmän käyttöön liittyvistä muutoksista.

Käsittelijän on Rekisterinpitäjän tietojärjestelmää käyttäessään noudatettava kaikkia Sopimuksessa tai sen liitteissä sovittuja Käsittelijän teknisiin ja organisatorisiin turvatoimiin liittyviä vastuita ja velvoitteita.

B. Ohjeistus Käsittelijälle, kun henkilötiedot ovat **Käsittelijän tietojärjestelmässä**:

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

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

liittymä- ja verkkodokumentaatiot). Käsittelijän tulee ylläpitää selostetta kaikista Rekisterinpitäjän lukuun suoritettavista käsittelytoimista tietosuoja-asetuksen 30 artiklan mukaisesti.

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

Tietojärjestelmän tulee kirjata lokiin Rekisterinpitäjän 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 Käsittelijän on rajoitettava niihin pääsy käyttöoikeuksin vain ylläpitohenkilöstölle. Lokien on tuotettava käyttökelpoista informaatiota henkilötietojen käsittelystä, jotta tapahtumia pystytään tarvittaessa tosiasiallisesti selvittämään. Käsittelijän on pyydettäessä ja ilman aiheetonta viivytystä toimitettava em. käyttöoikeudet ja lokitiedot Rekisterinpitäjälle veloituksetta.

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

Käsittelijän tulee suojata tietoliikenneyhteydet käyttämiensä tietojärjestelmien välillä asianmukaisia tiedonsiirtoprotokollia käyttäen.

Käsittelijän on huomioitava tietosuoja- ja tietoturvavaatimukset myös sovelluskehityksessä.

Käsittelijän ei tule käyttää tietojärjestelmän testauksessa Rekisterinpitäjän henkilötietoa.

Käsittelijän 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 kirjaudutaan käyttäjätunnuksella ja salasanalla, Käsittelijän tulee kuvata salasanapolitiikka tai mikäli järjestelmään kirjaudutaan toimikortilla, tulee sen toiminta kuvata.

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

Käsittelijän tulee laatia tietojärjestelmän varmuuskopiointisuunnitelma:
- Erilaiset tietojen palautustarpeet huomioidaan.
- Varmuuskopiot suojataan asianmukaisesti.
- Varmuuskopioiden palauttamista testataan säännöllisesti.

Käsittelijän tulee toteuttaa tietojärjestelmän tietoturvapäivitykset riskiarvion mukaisesti riittävällä tasolla.

C. Ohjeistus Käsittelijälle, 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 Rekisterinpitäjälle viivytyksettä.

Käsittelijä saa suorittaa Rekisterinpitäjän lukuun tarkoituksenmukaisia tiedonsiirtoja vain Rekisterinpitäjän kirjallisten ohjeiden mukaisesti.

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

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

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

3. Käsittelijän tulee Rekisterinpitäjän pyynnöstä toimittaa pyydetyt tiedot pyydetyssä muodossa viipymättä Rekisterinpitäjälle. Rekisterinpitäjä toimittaa pyydetyt tiedot rekisteröidylle saatuaan ne Käsittelijältä.

5. Palveluhenkilöstö

5.2. Kaikkien Käsittelijän alaisuudessa toimivien henkilöiden, jotka käsittelevät Rekisterinpitäjän henkilötietoja, tulee lukea ja allekirjoittaa Rekisterinpitäjän Salassapito- ja käyttäjäsitoumuksen sisältöä vastaava sitoumus ja suorittaa Rekisterinpitäjän tarjoamaa tietoturvan ja tietosuojan verkkokoulutusta vastaava koulutus. Rekisterinpitäjän niin edellyttäessä, Käsittelijän alaisuudessa toimivien henkilöiden, jotka käsittelevät Rekisterinpitäjän henkilötietoja, tulee lukea ja allekirjoittaa Rekisterinpitäjän Salassapito- ja käyttäjäsitoumus ja suorittaa Rekisterinpitäjän tarjoama tietoturvan ja tietosuojan verkkokoulutus.

6. Alihankkijat, jotka käsittelevät Rekisterinpitäjän henkilötietoja

6.2. Käsittelijän mahdollisella Alikäsittelijällä, jonka Rekisterinpitäjä on hyväksynyt, tulee olla toteuttamansa käsittelyn osalta riittävä kelpoisuus ja palvelun tuottamisen edellytykset.

6.4. Käsittelijän tulee perehdyttää Alikäsittelijät Ehtoihin ja Rekisterinpitäjän ohjeisiin. Käsittelijä vastaa, että Rekisterinpitäjän niin edellyttäessä Alikäsittelijöiden alaisuudessa toimivien henkilöiden, jotka käsittelevät Rekisterinpitäjän henkilötietoja, tulee lukea ja allekirjoittaa Rekisterinpitäjän Salassapito- ja käyttäjäsitoumus ja suorittaa Rekisterinpitäjän tarjoama tietoturvan ja tietosuojan verkkokoulutus.

9. Henkilötietojen käsittelyn päättyminen

9.2. Henkilötietojen käsittely sopimuksen päättyessä tai purkautuessa

A. Ohjeistus Käsittelijälle **analogista (paperimuotoista)** aineistoa koskien, mikäli asiakirjoja ei ole siirretty Rekisterinpitäjälle aikaisemmin:

   Sopimuksen päättyessä tai purkautuessa Käsittelijän tulee toimittaa Rekisterinpitäjälle hallussaan olevat Rekisterinpitäjän aineistot järjestettynä ja luetteloituna analogisena tai digitoituna Rekisterinpitäjän ohjeistuksen mukaisesti. Käsittelijän tulee Rekisterinpitäjän pyynnöstä esittää riittävä selvitys siitä, että Käsittelijä on toimittanut kaikki Rekisterinpitäjän henkilötiedot Rekisterinpitäjälle.

B. Ohjeistus Käsittelijälle **sähköistä aineistoa** koskien, mikäli asiakirjoja ei ole siirretty Rekisterinpitäjälle aikaisemmin:

   Sopimuksen päättyessä tai purkautuessa Käsittelijä siirtää sähköisessä muodossa olevat henkilötiedot Rekisterinpitäjän järjestelmään Rekisterinpitäjän kulloinkin erikseen ohjeistamalla tavalla.

   Käsittelijän tulee Rekisterinpitäjän pyynnöstä esittää poistamisesta riittävä selvitys.

C. Jos Käsittelijä käsittelee omassa järjestelmässään Rekisterinpitäjän pitkään (yli 20 vuotta) tai pysyvästi säilytettävää aineistoa, Käsittelijä on velvollinen siirtämään em. henkilötiedot Rekisterinpitäjälle säännöllisesti ja ilman erillisiä kustannuksia Rekisterinpitäjän tarkemman ohjeistuksen mukaisesti. Käsittelijän tulee Rekisterinpitäjän pyynnöstä esittää siirtämisestä riittävä selvitys.

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