Henkilötietojen käsittelyn ehdot

Liite 3

Kempeleen kunta ei lähtökohtaisesti hyväksy palvelutuottajan tai tietojärjestelmätoimittajan omia henkilötietojen käsittelyä koskevia ehtoja.

EU:n yleisen tietosuoja-asetuksen (679/2016) soveltaminen alkoi 25.5.2018. Tämän johdosta Kempeleen kunta on laatinut henkilötietojen käsittelyn ehdot ja siihen liittyvät tilaajan ohjeet henkilötietojen käsittelystä. Kyseiset ehdot perustuvat Kuntaliiton malliehtoihin (versio 4, maaliskuu 2018) henkilötietojen käsittelystä.

Edellä mainitut henkilötietojen käsittelyn ehdot ja tilaajan ohjeet ovat osa sääntökirjaa ja niihin tulee palveluntuottajan sitoutua hakeutuessaan palveluntuottajaksi. Ilmoitus tietoturvaloukkauksesta ja Seloste käsittelytoimista lähetetään palveluntuottajalle täytettävässä muodossa palveluntuottajaksi hyväksymisen jälkeen.

TILAAJAN OHJEET HENKILÖTIETOJEN KÄSITTELIJÄLLE

1. Yleistä

1.1. Tämä henkilötietojen käsittelyn ehdot (jäljempänä ”Ehdot”) on osa Palvelusetelin sääntökirjaa (jäljempänä ”Sääntökirja”). Näissä ehdoissa määritellään Tilaajaa ja Palveluntuottajaa sitovasti ne henkilötietojen käsittelyä ja tietosuojaa koskevat ehdot, joiden mukaisesti Palveluntuottaja Tilaajan toimeksiannosta käsittelee henkilötietoja Tilaajan puolesta. Näissä ehdoissa kuvatuista Palveluntuottajan toimenpiteistä ja velvollisuuksista ei suoriteta erillistä korvausta, ellei näissä ehdoissa ole toisin sovittu.

1.2. Palveluntuottaja noudattaa voimassa olevan tietosuojalainsäädännön edellyttämiä menettelytapoja ja henkilötietojen käsittelyä sekä suojaamista koskevia säännöksiä. Palveluntuottaja vastaa siitä, että palvelu on kulloinkin voimassa olevan tietosuojalainsäädännön ja Sääntökirjan mukainen, ottaen erityisesti huomioon, mitä sisäänrakennetusta ja oletusarvoisesta tietosuojasta on säädetty.

1.3. Palveluntuottaja sitoutuu noudattamaan henkilötietojen käsittelijänä näiden Ehtojen sekä näiden Ehtojen liitteiden mukaisia ohjeita sekä ehtoja henkilötietojen käsittelystä.

2. Osapuolten roolit henkilötietojen käsittelyssä

2.1. Käsiteltäessä henkilötietoja Tilaaja on rekisterinpitäjä ja Palveluntuottaja on henkilötietojen käsittelijä (jäljempänä myös ”Käsittelijä”), ellei henkilötietojen käsittelyn tarkoituksesta muuta johdu. ”Tilaajan henkilötiedoilla” tarkoitetaan näissä ehdoissa henkilötietoja, joista Tilaaja vastaa rekisterinpitäjänä.

2.2. Henkilötietojen käsittelyn kohde, luonne ja tarkoitus sekä henkilötietojen tyypit ja rekisteröityjen ryhmät sekä rekisterinpitäjän ja käsittelijän velvollisuudet ja oikeudet kuvataan näiden Ehtojen liitteessä 1 ”Käsittelytoimien kuvaus” ja liitteessä 2 ”Ohjeet käsittelijöille”. Palveluntuottaja sitoutuu noudattamaan käsittelytoimien kuvauksessa ja käsittelijöiden ohjeistuksessa olevia ehtoja ja kuvauksia. Tilaaja vastaa ohjeistuksen ylläpidosta ja saatavuudesta. Palveluntuottaja on velvollinen ylläpitämään selostetta Tilaajan lukuun suoritettavista henkilötietojen käsittelytoimista (Liite 4 ”Seloste käsittelytoimista”).

2.3. Jos kohdan 2.2 mukaista käsittelytoimien kuvausta ei ole tehty tai se on puutteellinen, Tilaaja laatii tai täydentää käsittelytoimien kuvausta tarvittaessa yhteistyössä Palveluntuottajan kanssa.

3. Palveluntuottajan yleiset velvollisuudet

3.1. Palveluntuottaja käsittelee henkilötietoja Sääntökirjan, näiden Ehtojen ja muiden Tilaajan antamien ohjeiden mukaisesti. Ryhmittymän ollessa Käsittelijänä velvoitteet koskevat kaikkia Ryhmittymän jäseniä ja Ryhmittymän käyttämiä alihankkijoita, jotka osallistuvat henkilötietojen käsittelyyn.

3.2. Palveluntuottaja huolehtii tietosuoja-asetuksen 32 artiklan 1 kohdan mukaisista teknisistä ja organisatorisista turvatoimista Tilaajan ohjeiden (Liite 2 ”Tilaajan ohjeet henkilötietojen käsittelijälle”) mukaisesti, joilla varmistetaan, että Tilaajan henkilötietojen käsittely tapahtuu Sääntökirjan vaatimusten ja sovittujen käytäntöjen mukaisesti. Toimenpiteiden tarkoituksena on varmistaa henkilötietojen lainmukainen käsittely sekä käsittelyjärjestelmien ja palveluiden luottamuksellisuus, eheys, saatavuus ja vikasietoisuus. Toimenpiteet kirjataan henkilötietojen käsittelyn ehtojen liitteeseen (Liite 4 ”Seloste käsittelytoimista”), jonka Palveluntuottaja toimittaa Tilaajalle viipymättä.

3.3. Palveluntuottaja ei käsittele eikä muulla tavoin hyödynnä Palveluntuottajaksi hyväksymisen perusteella käsittelemiään henkilötietoja muutoin kuin Sääntökirjan mukaisessa tarkoituksessa ja laajuudessa.

3.4. Palveluntuottaja nimeää tietosuojavastaavan tai tietosuojasta vastaavan yhteyshenkilön Tilaajan henkilötietoihin liittyviä yhteydenottoja varten. Palveluntuottaja ilmoittaa kirjallisesti tietosuojavastaavan tai yhteyshenkilön yhteystiedot Tilaajalle (Liite 4 ”Seloste käsittelytoimista”).

3.5. Palveluntuottaja saattaa Tilaajan saataville tämän pyynnöstä viipymättä kaikki tiedot, jotka Tilaaja tarvitsee rekisterinpitäjälle ja Palveluntuottajalle säädettyjen velvollisuuksien noudattamisen osoittamista varten, ja osallistuu pyydettäessä sovitulla tavalla Tilaajan vastuulla olevien kuvausten ja muiden dokumenttien, kuten vaikutustenarvioinnin laatimiseen ja ylläpitämiseen sekä tietosuoja-asetuksen mukaisen ennakkokuulemisen suorittamiseen. Palveluntuottaja tekee nämä tehtävät ilman eri korvausta.

3.6. Palveluntuottaja ilmoittaa Tilaajalle viipymättä kaikista rekisteröityjen pyynnöistä, jotka koskevat rekisteröidyn oikeuksien käyttämistä. Palveluntuottaja ei itse vastaa näihin pyyntöihin. Palveluntuottaja avustaa Tilaajaa, jotta Tilaaja pystyy täyttämään velvollisuutensa vastata näihin pyyntöihin. Pyynnöt voivat edellyttää Palveluntuottajalta esimerkiksi avustamista rekisteröidylle tiedottamisessa ja viestinnässä, rekisteröidyn pääsyoikeuden toteuttamisessa, henkilötietojen oikaisemisessa tai poistamisessa, käsittelyn rajoittamisen toteuttamisessa tai rekisteröidyn omien henkilötietojen siirtämisessä järjestelmästä toiseen. Palveluntuottajalla ei ole oikeutta laskuttaa em. toimenpiteistä Palveluntuottajalle mahdollisesti aiheutuneista lisäkuluista Tilaajaa.

3.7. Palveluntuottaja sallii Tilaajan tai sen valtuuttaman auditoijan suorittamat tarkastukset sekä osallistuu niihin. Tarkastusmenettelyä koskevat tarkemmat ehdot ovat Tilaajan ohjeissa (Liite 2 ”Tilaajan ohjeet henkilötietojen käsittelijälle”).

4. Tilaajan ohjeet

4.1. Palveluntuottaja noudattaa Tilaajan henkilötietojen käsittelyssä Sääntökirjassa sekä näissä Ehdoissa ja näiden Ehtojen liitteissä esitettyjä ehtoja sekä muita mahdollisia Tilaajan kirjallisia ohjeita. Tilaaja vastaa ohjeiden ylläpidosta ja saatavuudesta. Palveluntuottaja on velvollinen ilmoittamaan kirjallisesti, ilman aiheetonta viivytystä Tilaajalle, jos Tilaajan antamat ohjeet ovat puutteellisia tai jos Palveluntuottaja epäilee niitä lainvastaisiksi.

4.2. Tilaajalla on oikeus muuttaa, täydentää ja päivittää Palveluntuottajalle antamiaan henkilötietojen käsittelyä ja tietosuojaa koskevia ohjeita. Jos ohjeiden muutoksista aiheutuu Sääntökirjan mukaisiin palveluihin liittyviä muita kuin vähäisiä muutoksia, niiden vaikutuksesta sovitaan Sääntökirjan mukaisessa muutoshallintamenettelyssä.

5. Palveluhenkilöstö

5.1. Palveluntuottaja sitoutuu siihen, että kaikki sen alaisuudessa toimivat henkilöt, joilla on oikeus käsitellä Tilaajan henkilötietoja, noudattavat sovittuja ja lainsäädännössä määriteltyjä salassapitoehtoja.

5.2. Palveluntuottaja on velvollinen varmistamaan, että jokainen sen alaisuudessa toimiva henkilö, jolla on pääsy Tilaajan henkilötietoihin, on tietoinen henkilötietojen käsittelyyn liittyvistä velvoitteistaan ja käsittelee Tilaajan henkilötietoja ainoastaan Sääntökirjan, näiden Ehtojen ja muiden Tilaajan kirjallisten ohjeiden mukaisesti.

6. Alihankkijat, jotka käsittelevät henkilötietoja

6.1. Siltä osin kuin Palveluntuottaja käyttää toiminnassaan alihankkijoita, jotka käsittelevät henkilötietoja, alihankintaan sovelletaan Sääntökirjan lisäksi näiden Ehtojen ehtoja.

6.2. Jos Palveluntuottajan alihankkija käsittelee Tilaajan henkilötietoja, alihankkijan käyttäminen edellyttää Tilaajan ennakkoon kirjallisesti antamaa lupaa.

6.3. Palveluntuottaja tekee alihankkijan kanssa kirjallisen sopimuksen, jossa se sitouttaa käyttämänsä alihankkijat noudattamaan omalta osaltaan Sääntökirjassa Palveluntuottajalle asetettuja velvoitteita sekä Tilaajan antamia kulloinkin voimassa olevia henkilötietojen käsittelyyn liittyviä ohjeita. Palveluntuottaja vastaa, että Sääntökirjan mukainen Tilaajan tarkastusoikeus voidaan ulottaa alihankkijaan.

6.4. Palveluntuottaja vastaa käyttämänsä alihankkijan osuudesta kuin omastaan. Palveluntuottaja vastaa siitä, että alihankkija noudattaa omalta osaltaan henkilötietojen käsittelijälle asetettuja velvoitteita. Jos Tilaaja katsoo, että Palveluntuottajan alihankkija ei täytä tietosuojavelvoitteitaan, Palveluntuottajalla on velvollisuus vaihtaa alihankkijaa Tilaajan vaatimuksesta.

6.5. Henkilötietojen käsittelyyn osallistuvan alihankkijan vaihtaminen edellyttää Tilaajan ennakkoon kirjallisesti antamaa lupaa.

7. Palvelun paikka

7.1. Ellei palvelun tuottamispaikasta ole toisin sovittu, Palveluntuottajalla ja Palveluntuottajan mahdollisella alihankkijalla on oikeus käsitellä Tilaajan henkilötietoja ainoastaan Euroopan talousalueella. Käsiteltäessä henkilötietoja etäyhteyden välityksellä, käsittelijän tulee olla ja käsittelyn tulee tapahtua Euroopan talousalueella.

7.2. Jos Tilaaja ja Palveluntuottaja sopivat, että Palveluntuottaja saa siirtää Tilaajan henkilötietoja Euroopan talousalueen ulkopuolelle, molemmat osapuolet huolehtivat siitä, että henkilötietojen siirto toteutetaan lainsäädännön mukaisesti.

8. Tietoturvaloukkaukset

8.1. Palveluntuottajan on ilmoitettava kirjallisesti Tilaajalle tietoonsa tulleesta henkilötietojen tietoturvaloukkauksesta ja annettava Tilaajalle liitteen (Liite 3 ”Ilmoitus tietoturvaloukkauksesta”) mukaiset tiedot tietoturvaloukkauksesta välittömästi ja kuitenkin viimeistään 36 tunnin kuluessa tietoturvaloukkauksen havaittuaan.

8.2. Palveluntuottaja sitoutuu ilmoittamaan Tilaajalle ilman aiheetonta viivytystä muista palvelun häiriö tai ongelmatilanteista (kuten esim. tietojen saatavuuteen ja käytettävyyteen liittyvät ongelmat), joilla voi olla vaikutuksia rekisteröityjen asemaan ja oikeuksiin.

8.3. Henkilötietojen tietoturvaloukkauksen havaittuaan Palveluntuottaja ryhtyy viipymättä toimenpiteisiin tietoturvaloukkauksen poistamiseksi ja sen vaikutusten rajoittamiseksi ja korjaamiseksi liitteessä (Liite 3 ” Ilmoitus tietoturvaloukkauksesta”) tarkemmin kuvatulla tavalla.

9. Henkilötietojen käsittelyn päättyminen

9.1. Palveluntuottajaksi hyväksymisen voimassaoloaikana Palveluntuottaja ei saa poistaa Tilaajan lukuun käsittelemiään henkilötietoja ilman Tilaajan nimenomaista pyyntöä.

9.2. Palveluntuottajaksi hyväksymisen päättyessä tai purkautuessa Palveluntuottaja palauttaa Tilaajalle kaikki Tilaajan puolesta käsitellyt henkilötiedot sekä hävittää hallussaan olevat kopiot henkilötiedoista, ellei muuta ole sovittu. Tietoja ei saa poistaa, jos lainsäädännössä tai viranomaisen määräyksellä on edellytetty, että Palveluntuottaja säilyttää henkilötiedot.

Liitteet
Liite 3 Tilaajan ohjeet henkilötietojen käsittelijälle
Liite 3.1 Käsittelytoimien kuvaus
Liite 3.2 Ilmoitus tietoturvaloukkauksesta
Liite 3.3 Palveluntuottajan seloste käsittelytoimista

KÄSITTELYTOIMIEN KUVAUS

1. Osapuolet

Tilaaja: Kempeleen kunta/ Ikääntyneiden hoiva ja huolenpito
Palveluntuottaja:_____

2. Dokumentin tarkoitus

Tilaaja on hyväksynyt Palveluntuottajan Palvelusetelituottajaksi, joka koskee sellaista palvelua, jossa Palveluntuottaja toimii Tilaajan ylläpitämään henkilörekisteriin kuuluvien henkilötietojen käsittelijänä.

Tässä dokumentissa kuvataan käsittelytoimet, joita Palveluntuottaja henkilötietojen käsittelijänä tekee Tilaajan puolesta, henkilötietojen tyypit sekä käsiteltävät henkilötiedot.

Henkilötietojen käsittelyssä Palveluntuottajan on noudatettava Palvelusetelin Sääntökirjaa sekä Tilaajan ohjeita.

3. Henkilötietojen tyypit ja rekisteröityjen ryhmät

Palveluntuottaja käsittelee Tilaajan puolesta palvelun tuottamiseen liittyen seuraavia Tilaajan henkilörekisteriin kuuluvia henkilötietoja:

Tehostetun palveluasumisen asiakkaat. Palvelun toteuttamiseen liittyvät tarpeelliset henkilötiedot.

4. Käsittelyn luonne ja tarkoitus

Tilaaja on hyväksynyt Palveluntuottajan tuottamaan palvelusetelipalvelua. Palveluntuottaja voi käsitellä palvelun tuottamiseen nähden tarpeellisia henkilötietoja joko omassa asiakastietojärjestelmässä tai eri sopimukseen perustuen käyttäen Tilaajan asiakastietojärjestelmää.

5. Henkilötietojen käsittelyn kesto

Palveluntuottaja käsittelee tässä liitteessä yksilöityjä henkilötietoja seuraavan ajan: Palvelusetelituottajaksi hyväksymisen voimassaoloajan ja asiakaskohtaisesti vain sen ajan, kun asiakkaalla on voimassa oleva palvelu-/asiakassuhde palveluntuottajaan.

Tilaajan ohjeet henkilötietojen käsittelijälle (Perustuu henkilötietojen käsittelyn Ehtoihin. Numerointi viittaa Ehtojen vastaaviin kohtiin.)

3. Palveluntuottajan yleiset velvollisuudet

3.3 Palveluntuottaja ei saa käsitellä eikä muulla tavoin hyödyntää Palvelusetelituottajaksi hyväksymisen perusteella käsittelemiään henkilötietoja muutoin kuin Palvelusetelin Sääntökirjan mukaisessa tarkoituksessa ja laajuudessa.

3.3.1 Palveluntuottaja ei esim. saa hyödyntää Tilaajan henkilötietoja muiden kuin Tilaajan asiakkaiden palveluiden tuottamisessa.

3.3.2 Ohjeistus Palveluntuottajalle, kun henkilötiedot ovat **Palveluntuottajan omassa tietojärjestelmässä:**

3.3.2.1 Palveluntuottajan tulee nimetä tietojärjestelmälle omistaja ja vastuuhenkilö tai pääkäyttäjä.
3.3.2.2 Palveluntuottajan tulee dokumentoida tietojärjestelmän valvonta- ja ylläpitovastuut.
3.3.2.3 Palveluntuottajan tulee arvioida ja dokumentoida tietojärjestelmään kohdistuvat tietoturvauhat, analysoida riskit (esim. sivullisen pääsy tietoihin, tietosuojarikkomukset, tietojen katoaminen) sekä laatia niistä hallinta-, suojaus- ja toipumissuunnitelma.
3.3.2.4 Palveluntuottajalla tulee olla tietojärjestelmänsä ajantasaiset, riskiarvion mukaiset dokumentaatiot (esim. prosessi-, käyttötapaus-, tietovirta-, liittymä- ja verkkodokumentaatiot).
3.3.2.5 Palveluntuottajan tulee dokumentoida, mitä Tilaajan henkilötietoja Palveluntuottajalla on oikeus käsitellä ja kuka niitä käsittelee.
3.3.2.6 Palveluntuottajan tulee dokumentoida menettelytavat, joihin perustuen järjestelmän teknistä ja organisatorista turvallisuutta testataan ja arvioidaan säännöllisesti.
3.3.2.7 Palveluntuottajan tulee dokumentoida ja luokitella tietojärjestelmässä käsiteltävät tietosisällöt (henkilötietoryhmät).
3.3.2.8 Palveluntuottajan tulee selvittää ja dokumentoida tietojärjestelmässä mahdollisesti käsiteltävät erityiset henkilötietoryhmät tai alle 16-vuotiaita koskevat tiedot.
3.3.2.9 Mikäli tietojärjestelmässä käsitellään arkaluonteisia henkilötietoja tai riskitaso sitä muuten edellyttää, Palveluntuottajan tulee suojata tiedot joko salakirjoittamalla (tietokannan suojaus) tai pseudonymisoimalla.

3.3.2.10 Tietojärjestelmän tulee kirjata lokiin Tilaajan henkilötietojen käsittelytoimet (esim. muutokset, poistot) ja käsittelyn ajankohta käyttäjätasolla. Erityisten henkilötietoryhmien osalta tulee lokiin kirjata myös tietojen katselu.
3.3.2.11 Tietojärjestelmän lokien on oltava suojattu muutoksilta ja Palveluntuottajan on rajoitettava niihin pääsy käyttöoikeuksin vain ylläpitohenkilöstölle.
3.3.2.12 Lokien on tuotettava käyttökelpoista informaatiota henkilötietojen käsittelystä, jotta tapahtumia pystytään tarvittaessa tosiasiallisesti selvittämään.
3.3.2.13 Palveluntuottajan on pyydettäessä ja ilman aiheetonta viivytystä toimitettava em. käyttöoikeudet ja lokitiedot Tilaajalle veloituksetta.
3.3.2.14 Tietojärjestelmän tulee tukea suostumusten ja kieltojen hallintaa, mikäli henkilötietojen käsittely perustuu suostumukseen ja/tai käsittelyn voi kieltää.
3.3.2.15 Henkilötietojen käsittely tulee minimoida niin, että Palveluntuottajan toimesta käsitellään vain käyttötarkoitukseen nähden tarpeellisia henkilötietoja.
3.3.2.16 Järjestelmässä tulee voida käyttää suojatoimena henkilötiedon anonymisointia tai pseudonymisointia silloin, kun se riskiarvion perusteella on tarpeellista.
3.3.2.17 Palveluntuottajan tulee suojata tietoliikenneyhteydet käyttämiensä tietojärjestelmien välillä asianmukaisia tiedonsiirtoprotokollia käyttäen.
3.3.2.18 Palveluntuottajan tulee toteuttaa sisäänrakennetun ja oletusarvoisen tietosuojan vaatimukset.
3.3.2.19 Palveluntuottajan on huomioitava tietosuoja- ja tietoturvavaatimukset myös sovelluskehityksessä.
3.3.2.20 Palveluntuottajan ei tule käyttää tietojärjestelmän testauksessa oikeaa henkilötietoa, vaan anonymisoitua, pseudonymisoitua tai testikäyttöön generoitua tietoa.
3.3.2.21 Palveluntuottajan tulee laatia pääsynvalvontaperiaatteet pääsyoikeuksia varten:
3.3.2.21.1 Järjestelmän käyttäjän luonti-, muutos ja poistoprosessi oltava kuvattuna.
3.3.2.21.2 Järjestelmän käyttöoikeuksien säännöllinen tarkastaminen oltava kuvattuna.
3.3.2.21.3 Kaikilla järjestelmän käyttäjillä tulee olla henkilökohtaiset käyttäjätunnukset.
3.3.2.21.4 Kaikki järjestelmän käyttäjät tulee olla dokumentoituna (myös pääkäyttäjät ja ylläpitäjät)
3.3.2.21.5 Mikäli järjestelmään kirjaudutaan käyttäjätunnuksella ja salasanalla, Palveluntuottajan tulee kuvata salasanapolitiikka.
3.3.2.21.6 Mikäli järjestelmään kirjaudutaan toimikortilla, tulee sen toiminta kuvata.

3.3.2.22 Yksittäisen käyttäjän kirjautumiset/epäonnistuneet kirjautumiset on pystyttävä tarvittaessa jälkikäteen selvittämään, mikäli tämä on riskiarvion perusteella tarpeen.
3.3.2.23 Palveluntuottajan tulee laatia tietojärjestelmän varmuuskopiointisuunnitelma:
3.3.2.23.1 Huomioitava erilaiset tietojen palautustarpeet.
3.3.2.23.2 Varmuuskopiot on suojattava asianmukaisesti.
3.3.2.23.3 Varmuuskopioiden palauttamista testataan säännöllisesti.
3.3.2.24 Palveluntuottajan tulee toteuttaa tietojärjestelmän tietoturvapäivitykset riskiarvion mukaisesti riittävällä tasolla.

3.3.3 Ohjeistus Palveluntuottajalle, kun Palveluntuottaja käsittelee henkilötietoja **Tilaajan tietojärjestelmässä:**

3.3.3.1 Palveluntuottaja käsittelee henkilötietoja vain Tilaajan kirjallisesta yksilöidystä toimeksiannosta Tilaajan määrittelemässä laajuudessa Tilaajan antaman käyttöoikeuden perusteella.
3.3.3.2 Palveluntuottajan on ilmoitettava viipymättä Tilaajalle kaikista Tilaajan tietojärjestelmän käyttöön liittyvistä muutoksista.

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

3.3.4.1 Henkilötietoja sisältävä analoginen aineisto on säilytettävä lukitussa tilassa, johon pääsyä valvotaan. Ko. aineiston säilyttämiseen käytettävän lukitun tilan pääsyvalvonnan suorittamistapa tulee dokumentoida kirjallisesti.
3.3.4.2 Henkilötietoja sisältävään analogiseen aineistoon kohdistuvista häiriö- tai ongelmatilanteista, kuten esimerkiksi vesivahingoista, tulipaloista, murroista tms., tulee ilmoittaa Tilaajalle viivytyksettä.
3.3.4.3 Palveluntuottaja saa suorittaa Tilaajan lukuun tarkoituksenmukaisia tiedonsiirtoja vain Tilaajan kirjallisten ohjeiden mukaisesti.

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

3.5. Rekisteröityjen tieto- ja tarkastuspyyntöjä koskeva ohjeistus Palveluntuottajalle:

1. Palveluntuottajan tulee ohjeistaa rekisteröityjä toimittamaan allekirjoitetut kirjalliset tarkastuspyynnöt suoraan Kempeleen kunnan kirjaamoon (Vihikari 10, 90440 Kempele)

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 Kempeleen kunnan kirjaamoon.
3. Tilaaja toimittaa rekisteröityjen tarkastuspyynnöt Tilaajan organisaatiossa oikealle rekisterinpitäjälle.
4. Palveluntuottajan tulee Tilaajan pyynnöstä toimittaa pyydetyt tiedot pyydetyssä muodossa viipymättä Tilaajalle.
5. Tilaaja toimittaa pyydetyt tiedot saatuaan ne Palveluntuottajalta.

3.6 Palveluntuottajan tulee esim. mahdollistaa Tilaajan tai sen valtuuttaman auditoijan pääsy tiloihin ja järjestelmiin, joissa Tilaajan henkilötiedot ovat.

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 kolmen (3) vuoden välein.

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 henkilötietojen käsittelyn ehtoihin ja Tilaajan ohjeisiin. Alihankkijoiden tulee Tilaajan niin edellyttäessä lukea ja allekirjoittaa Tilaajan Tietoturva- ja käyttäjäsitoumus ja suorittaa Tilaajan tarjoama tietoturvan ja tietosuojan verkkokoulutus kolmen (3) vuoden välein.

9. Henkilötietojen käsittelyn päättyminen

9.2. Palvelusetelituottajaksi hyväksymisen päättyessä tai purkautuessa Palveluntuottajan tulee toimittaa Tilaajalle kaikki Tilaajan puolesta käsitellyt henkilötiedot sekä hävittää omilta taltioiltaan mahdolliset kopiot henkilötiedoista, ellei muuta ole sovittu. Tietoja ei saa poistaa, jos lainsäädännössä tai viranomaisen määräyksellä on edellytetty, että Palveluntuottaja säilyttää henkilötiedot.

9.2.1 Ohjeistus Palveluntuottajalle analogista (paperimuotoista) aineistoa koskien:
Palvelusetelituottajaksi hyväksymisen päättyessä tai purkautuessa Palveluntuottaja tulee toimittaa Tilaajalle hallussaan olevat Tilaajan analogiset aineistot järjestettynä ja luetteloituna Tilaajan

ohjeistuksen mukaisesti.

9.2.2 Ohjeistus Palveluntuottajalle sähköistä aineistoa koskien

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

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.

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

ILMOITUS TIETOTURVALOUKKAUKSESTA

Tietojenkäsittelijä on velvollinen ilmoittamaan välittömästi, kuitenkin viimeistään 36 tunnin kuluessa tietoturvaloukkauksen havaittuaan asiasta rekisterinpitäjälle. Siltä osin, kun kaikkia tietoja ei ole mahdollista toimittaa samanaikaisesti, tiedot voidaan toimittaa vaiheittain ilman aiheetonta viivytystä. Ilmoittaminen tulee tehdä tällä lomakkeella.

1. Tietojenkäsittelijän tietosuojavastaavan tai ”vastuutahon” nimi ja yhteystiedot
2. Kuvaus henkilötietojen tietoturvaloukkauksesta
2.1 asianomaisten rekisteröityjen ryhmät
2.2 ryhmien arvioidut lukumäärät
2.3 henkilötietotyyppien ryhmät ja arvioidut lukumäärät
3. Kuvaus henkilötietojen tietoturvaloukkauksen todennäköisistä seurauksista
4. Kuvaus toimenpiteistä, joita tietojenkäsittelijä ehdottaa tai jotka tietojenkäsittelijä on toteuttanut
henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

Perustiedot tietoturvaloukkauksesta

Mahdollisimman tarkka kuvaus tietoturvaloukkauksesta kaiken saatavissa olevan tiedon perusteella:
1. Milloin tietoturvaloukkaus tapahtui?
2. Miten tietoturvaloukkaus tapahtui?
3. Mikäli tämä ilmoitus tehdään säädetyn määräajan ulkopuolella, ilmoita perustelut tälle.
4. Minkälaisia suojakeinoja (organisatorisia/teknisiä) organisaatiolla oli käytössä tapahtuneen kaltaisten tietoturvaloukkausten estämiseksi?

Henkilötiedot, joihin tietoturvaloukkaus kohdistui

1. Mihin henkilötietoryhmiin ja rekisteröityjen ryhmiin tietoturvaloukkaus kohdistui? Kohdistuiko tietoturvaloukkaus erityisiin henkilötietoryhmiin (esim. arkaluonteisiin henkilötietoihin)?
2. Kuinka montaa rekisteröitynyttä tietoturvaloukkaus koskee?
3. Ovatko ko. rekisteröidyt tietoisia tietoturvaloukkauksen tapahtumisesta?
4. Kuvaile potentiaalisia, rekisteröityjä ja heidän yksityisyyden suojaansa koskevia riskejä ja haittoja
jotka tietoturvaloukkauksesta johtuvat.
5. Onko organisaatiolle tullut yhteydenottoja rekisteröidyiltä tietoturvaloukkauksen johdosta?
6. Onko organisaatio ohjeistanut rekisteröityjä mahdollista toimista, joilla he voivat pyrkiä rajaamaan tietoturvaloukkauksen seurauksia?

Tietoturvaloukkauksen tutkiminen, rajoittaminen ja siitä toipuminen

1. Onko palveluntuottaja ryhtynyt toimenpiteisiin tietoturvaloukkauksen seurausten minimoinniksi tai rajoittamiseksi? Kuvaile näitä toimenpiteitä.
2. Onko altistunut tieto saatu takaisin palveluntuottaja haltuun? Jos kyllä, kuvaile miten ja milloin tämä tapahtui.
3. Minkälaisiin toimiin palveluntuottaja on ryhtynyt vastaavanlaisten tietoturvaloukkausten estämiseksi jatkossa?

Muuta

1. Onko palveluntuottaja tehnyt ilmoituksen tietoturvaloukkauksesta Poliisille?
2. Onko palveluntuottaja tehnyt ilmoituksen tietoturvaloukkauksesta jollekin muulle viranomaiselle, mukaan lukien tietosuojan valvontaviranomaiset Euroopan unionin jäsenvaltioissa?