Yleinen tietoturvallisuustason kuvaus ja rekisterinpitäjän ohje toimittajille henkilötietojen käsittelystä

Tarkoitus

Tämä ohje kuvaa sitä, miten Lakeuden Etappi Oy käsittelee asiakkaidensa ja sidosryhmiensä henkilötietoja. Vaikka ohje on kirjoitettu tietoturvaohjeeksi toimittajille, on kaikilla henkilöillä oikeus odottaa vähintään tämän kuvauksen mukaista tietoturvallisuustasoa Lakeuden Etapin henkilötietojen käsittelyssä.

Tätä ohjetta noudatetaan tietosuoja-asetuksen tarkoittamana rekisterinpitäjän ohjeena silloin, kun palvelu- tai ohjelmistotoimittaja tai alihankkija (myöhemmin Toimittaja) käsittelee Lakeuden Etappi Oy:n (myöhemmin Tilaaja) puolesta henkilötietoja. Myös yhteisrekisterinpitäjien käsittelyyn liittyvät yleisvelvoitteet ovat samat kuin tässä ohjeessa.

Ohje täydentää osapuolten välisiä sopimuksia. Jos tässä ohjeessa olevista asioista on sovittu sopimuksilla, ovat ne ensisijaisesti sovellettavia.

Hallinnollinen turvaohjeistus

Toimittajalla on oltava riskiarviot henkilötietojen käsittelyn riskeistä ja suunnitelmat riskien hallinnasta. Riskiarviot on päivitettävä säännöllisesti. Toimittajan on tiedotettava Tilaajaa havaituista riskeistä, joista Tilaajan on syytä olla tietoinen.

Toimittajalla tulee olla nimetyt henkilöt, jotka vastaavat tietoturvasta ja tietosuojasta organisaatioissa. Henkilöt ilmoitetaan Tilaajalle sopimuksen teon yhteydessä ja muutoksista tiedotetaan tarvittaessa.

Toimittajan tulee ylläpitää dokumentaatiota siitä, mitä henkilötietoryhmiä se käsittelee ja missä käsittelyä suoritetaan (’henkilötietoryhmät’). Toimittajalla tulee olla ajantasainen tietosuoja-asetuksen (679/2016) tarkoittama seloste käsittelytoimista niiden henkilötietoryhmien osalta, joita se käsittelee säännöllisesti tai toistuvasti. Dokumentaatiosta on ilmettävä myös käsiteltävät erityistietoryhmät ja heikommassa asemassa olevien rekisteröityjen ryhmät (esim. lapset ja vanhukset).

Toimittajan tulee tietää jatkuvasti, kenellä on pääsy Tilaajan tietoihin tai Tilaajan tietoja sisältäviin tietojärjestelmiin. Tieto tulee toimittaa Tilaajalle kohtuullisen ajan sisällä sitä pyydettäessä niin, että tietoturvaloukkauksiin voidaan reagoida niille säädetyssä ajassa. Toimittajalla tulee olla määriteltynä tekniset ja organisatoriset suojatoimet ja keinot, joilla varmistetaan sisäänrakennettu ja oletusarvoinen tietosuoja (esimerkiksi käsittelyn perustuminen todelliseen tarpeeseen, tietojen minimointi ja ylimääräisten henkilötietojen käsittelyltä välttyminen, säilytyksen rajoittamiseen liittyvät menettelyt niin, ettei tietoja kerry liian pitkältä ajalta, ym.).

Ohjeet tilaturvallisuudesta

Kaikki Tilaajan tietoja sisältävät tietojärjestelmien päätteet, tabletit, tietokoneet, verkkojen aktiivilaitteet ja vastaavat komponentit on sijaittava lukituissa tiloissa, joihin pääsy on vain ylläpitohenkilöstöllä, silloin kun ne eivät ole käytössä tai Toimittajan suorassa valvonnassa. Toimittajan tulee tietää jatkuvasti, kenellä on pääsy tiloihin, joissa käsitellään Tilaajan tietoja. Myös muu kuin Toimittajan henkilöstö on oltava dokumentoituna (kiinteistönhuolto, siivouspalvelut, ym.).

Kaikkien tietojärjestelmistä otettujen tulosteiden tai muutoin järjestelmäympäristöstä irrotettujen tallenteiden hallinnasta on oltava käsittelyohjeet niiden säilyttämisestä, valvonnasta ja tuhoamisesta. Fyysistä tietoaineistoa koskevat samat ohjeet kuin sähköistä. Myös fyysisen turvallisuuden riskit on oltava huomioitu riskiarvioissa, esimerkiksi varkaudet, tulipalot ja vesivahingot sekä niiden vaikutukset sekä niiltä varautuminen.

Toimittajalla tulee olla ajantasainen luettelo henkilöstöstä, jolla on pääsy tiloihin, joissa käsitellään Tilaajan henkilötietoa. Pääsyoikeuksia tulee voida hallita esimerkiksi lukituksilla siten, että tietojen käsittelyyn liittyvät oikeudet voidaan rajata tietoja tarvitsevien henkilöstöryhmien tasolla.

Ohjeet henkilöstölle

Toimittajalla tulee olla ohjeet, joista selviää, kenellä on oikeus käsitellä henkilötietoja ja millä perusteilla.

Toimittajan henkilöstöllä tulee olla ajantasainen koulutus tietoturvasta ja tietosuojasta sekä Tilaajan ohjeista siihen liittyen. Henkilöstöllä tulee olla koko ajan saatavilla ajantasainen ohjeistus henkilötietojen käsittelystä, tietojen luokituksesta sekä henkilötietojen käsittelyyn liittyvistä prosesseista ja Tilaajan ohjeista.
Henkilöstön omien laitteiden käyttö työtehtäviin siten, että Tilaajan tietoja tallentuu niille, on kiellettyä.
Tableteissa ja puhelimissa on käytettävä automaattilukitusta ja pääsykoodia, jos niiden kautta on pääsy henkilötietoihin, joissa Tilaaja on rekisterinpitäjänä.

Tilaajan järjestelmiä ja verkkoja käytettäessä tulee muistaa, että niiden toimintaa ja niissä kulkevaa liikennettä seurataan tietoturvan varmistamiseksi teknisten laitteiden ja ohjelmistojen avulla. Seurantaa tehdään vikojen ja ongelmien havaitsemiseksi ja ratkaisemiseksi sekä järjestelmien tietoturvallisuuden varmistamiseksi, luvattoman käytön paljastamiseksi ja oikeudettoman liikesalaisuuksien paljastumisen estämiseksi ja selvittämiseksi.

Tahallinen ohjeiden noudattamatta jättäminen ja väärinkäytös voi johtaa tarkempaan selvitykseen, käyttörajoituksiin ja tarvittaessa muihin toimenpiteisiin. Mikäli väärinkäytös on vakava tai muodostaa rikoksen, annetaan asia poliisin tutkittavaksi.

Lisäksi Toimittajan vastuulla on varmistaa, että ohjeiden lisäksi sen henkilöstöllä on käytettävissä taho, johon henkilöstö voi kaikissa tietoturvaan ja tietosuojaan liittyvissä kysymyksissä olla yhteydessä.

Ohjeet tietoturvallisuudesta
Toimittajan tietoverkkoympäristö, tietojärjestelmät ja päätelaitteet tulee olla suojattu siten, että luvaton tai tunnistamaton pääsy niihin on estetty. Toimittajan tietojärjestelmäympäristö tulee olla testattu tietoturvallisen toiminnan varmistamiseksi vähintään niiltä osin, joita kautta on mahdollista päästä käsiksi Tilaajan henkilötietoon. Pääsyoikeuksia tulee voida hallita siten, että vain ne, joilla on tarve käsitellä henkilötietoja, pääsevät niihin.

Toimittajalla tulee olla ajantasainen toipumissuunnitelma palveluiden häiriöttömän toimittamisen varmistamiseksi. Toimittajalla tulee olla myös ajantasainen varmistussuunnitelma niiltä osin, kuin tietojen saatavuuden häiriöt voivat vaikuttaa Tilaajalle toimitettaviin palveluihin. Varmistukset on oltava suojattuja ja erotettuja yleisistä verkoista siten, että mahdollisten haittaohjelmien leviäminen ei tuhoa myös varmuuskopioita. Varmuuskopiot on sijaittava fyysisesti eri sijainnissa siten, että esimerkiksi tulipalo tai vesivahinko ei tuhoa varmuuskappaleita tuotantolaitteisiin kohdistuvan häiriön sattuessa.

Tietojärjestelmissä, joihin on pääsy laajemmin kuin Toimittajan tai Tilaajan verkoista, on käytettävä henkilötietojen ja kirjautumistietojen salausta. Yhteydet julkisiin verkkoihin tai niiden yli on oltava salattuja silloin kun niissä siirretään Tilaajan tietoja. Kaikki henkilötietojen käsittely on tapahduttava myös sisäverkossa salattujen yhteyksien yli, jos tietoverkkoa käyttävät sellaiset käyttäjäryhmät, joilla ei ole oikeuksia Tilaajan tietoihin.

Toimittajalla tulee olla käytössä tietojärjestelmien automaattinen päivitystoiminto etenkin tietoturvapäivitysten osalta. Jos toimittaja siirtää Tilaajan omistamaa tietoa omiin järjestelmiinsä, on Toimittajan tietojärjestelmissä oltava lokitus, josta on selvittävä henkilötietojen käsittelyn osalta

- Pääsyoikeudet – kenellä on pääsy ja millaiseen tietoon milloinkin
- Tallennus, muutokset ja poistot sekä niiden suorittaja
- Lokeista on selvittävä myös tietojen katselu sekä sen suorittaja

Tietojärjestelmälokit on suojattava siten, että järjestelmän käyttäjät, pääkäyttäjät tai admin-käyttäjät eivät pääse muokkaamaan niitä. Tietojärjestelmässä on oltava ominaisuudet, joilla voidaan toteuttaa käyttäjien

oikeuksia, esimerkiksi turvakieltoasiakkaiden tunnistaminen, käsittelyn rajoituspyynnöt, suostumuksenhallinta ja vastustamisoikeus ja tietojen poistaminen.

Toimittaja ei saa käyttää Tilaajan sille luovuttamaa henkilötietoa omiin tarkoituksiin, kuten järjestelmäkehitykseen ja testaukseen. Jos jokin testaus tai kehitystoimi edellyttäisi henkilötiedon käyttöä, tulee Tilaaja osallistaa testaukseen siten, että riittävät suojatoimenpiteet voidaan suunnitella yhdessä (kuten pseudonymisointi, testausympäristöjen eriyttäminen ja muut tilanteeseen soveltuvat toimet). Mikäli Toimittaja tekee yksipuolisia päätöksiä henkilötietojen käsittelyn keinoista ja tarkoituksista, tekee se itsestään rekisterinpitäjän ja vastaa rekisterinpitäjänä tietosuojalainsäädännön velvoitteiden noudattamisesta suoraan niille henkilöille, joiden tietoja se käsittelee.

Kaikista tietoturvallisuutta heikentävistä muutoksista on informoitava Tilaajaa ennen muutosten tekemistä. Myös Toimittajan alihankkija- ja toimittajamuutoksista on informoitava Tilaajaa. Tilaajalla on oikeus hyväksyä tai kieltää muutokset.

Lisätietoja ja ohjeita saa Lakeuden Etapin tietosuojavastaavalta. Yhteystiedot ja yhteydenottoon liittyvät tiedot löytyvät osoittesta:

https://www.etappi.com/yhtio/saannokset-ja-maaraykset/tietosuoja/