10 kohdan muistilista henkilötietojen turvalliseen käsittelyyn

KYBERKUU Kymenlaaksossa

Henkilötiedoksi lasketaan kaikki tiedot, joista henkilö on mahdollista tunnistaa joko suoraan tai välillisesti. Henkilön välillisellä tunnistamisella tarkoitetaan tilanteita, joissa tiedon yhdistäminen toiseen tietoon mahdollistaa tunnistamisen. Asiakasnumero on hyvä esimerkki tiedosta, josta henkilö voidaan tunnistaa välillisesti.

Tietosuoja-asetuksessa on määritelty erikseen erityiset henkilötietoryhmät, joiden käsittely on lähtökohtaisesti kiellettyä. Näihin tietoihin kuuluvat esimerkiksi terveystiedot, poliittiset mielipiteet ja biometriset tiedot. Ryhmään kuuluvia arkaluonteisia tietoja tulee suojata erityisen tarkasti.

1) Tiedä roolisi

Rekisterinpitäjä? Yhteisrekisterinpitäjä? Henkilötietojen käsittelijä? Alikäsittelijä? Riippuen yrityksen roolista, myös vastuut ovat erilaiset.

Rekisterinpitäjä määrittelee, mihin tarkoitukseen ja miten henkilötietoja käsitellään. Kun rekisterinpitäjiä on vähintään kaksi, puhutaan yhteisrekisterinpitäjistä. Rekisterinpitäjä tai yhteisrekisterinpitäjä on vastuussa siitä, että tietoja käsitellään yleisen tietosuoja-asetuksen velvoitteiden mukaan. Yhteisrekisterinpitäjien tulee myös määrittää keskinäiset vastuut.

Henkilötietojen käsittelijä käsittelee tietoja rekisterinpitäjän lukuun. Tietojen käsittelyssä tulee noudattaa rekisterinpitäjän ohjeita. Henkilötietojen käsittelijän velvollisuuksista tulee sopia sopimuksella.

Henkilötietojen käsittelijällä voi olla myös alikäsittelijä. Alikäsittelijä voidaan nimittää vain rekisterinpitäjän luvalla. Myös alikäsittelijän velvollisuuksista tulee sopia sopimuksella, jolla varmistetaan että henkilötietojen suojan taso pysyy samana kuin rekisterinpitäjän ja henkilötietojen käsittelijän välisessä sopimuksessa on määritetty.

Lisätietoa rooleista ja esimerkiksi roolien välisistä sopimuksista löydät täältä: https://www.edpb.europa.eu/sme-data-protection-guide/data-controller-data-processor_fi

XAMK Kaakkois-Suomen ammattikorkeakoulu
KYMEN LAAKSON LIITTO
Euroopan unionin osarahoittama
Kyberturvan tulevaisuus Kymenlaaksossa, KymVake ja CyberCare Kymi

» Katso lisää: Kyberasema.fi

2) Nimitä tarvittaessa tietosuojavastaava

Yrityksen tulee nimetä tietosuojavastaava silloin, jos yrityksessä käsitellään arkaluontoisia tietoja laajamittaisesti, tai jos ihmisiä seurataan laajamittaisesti, säännöllisesti ja järjestelmällisesti.

Tietosuojavastaava voidaan myös nimittää vapaaehtoisesti, vaikkei se olisi tietosuoja-asetuksen perusteella velvoitettua.

3) Kartoita riskit

Henkilötietojen käsittelyyn liittyviä riskejä tulee arvioida rekisteröidyn näkökulmasta. Mitä fyysisiä, aineellisia tai aineettomia vahinkoja rekisteröidylle voi aiheutua henkilötietojen käsittelystä? Mitä vapauksia ja oikeuksia käsittely voi vaarantaa?

Riskien arvioinnissa on huomioitava käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset. Arvioinnin perusteella määritellään ne toimenpiteet, joilla tietosuojan toteutuminen varmistetaan.

4) Tee tarvittaessa tietosuojaa koskeva vaikutustenarviointi

Tietosuojaa koskeva vaikutustenarviointi auttaa rekisterinpitäjää tunnistamaan, arvioimaan ja hallitsemaan riskejä.

Vaikutustenarviointia velvoitetaan tilanteissa, joissa tietojen käsittely voi aiheuttaa korkean riskin ihmisten oikeuksille ja vapauksille. Sen voi halutessaan tehdä myös muulloin.

Lisätietoa ja ohjeen vaikutustenarvioinnin tekemiseen löydät täältä: https://tietosuoja.fi/vaikutustenarviointi

5) Varmista suojaustoimenpiteet

Henkilötietojen suojaamiseksi on otettava käyttöön riittävät tekniset ja organisatoriset suojatoimenpiteet.
Organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi toimintatapojen dokumentointia, työntekijöiden tietoisuuden varmistamista ja salassapitosopimuksia.

Tekniset toimenpiteet voivat puolestaan olla laitteiden ja toimitilojen suojaamiseen liittyvät toimenpiteet ja pääsynhallinta.

XAMK Kaakkois-Suomen ammattikorkeakoulu
KYMEN LAAKSON LIITTO
Euroopan unionin osarahoittama
Kyberturvan tulevaisuus Kymenlaaksossa, KymVake ja CyberCare Kymi

» Katso lisää: Kyberasema.fi

6) Minimoi tietojen kerääminen

Yritys saa kerätä vain niitä henkilötietoja, joita tiedoille suunniteltua tarkoitusta varten tarvitaan. Älä kerää ylimääräistä tietoa. Poista tiedot, kun et tarvitse niitä enää. Huomioi kuitenkin, joitain tietoja voi olla pakollista säilyttää tietyn ajan.

7) Huomioi informointivelvollisuus

Rekisteröidylle tulee kertoa kaikki henkilötietojen käsittelyä koskevat tiedot helposti ymmärrettävässä muodossa. Alla oleva lista rekisteröidylle kerrottavista tiedoista on otettu suoraan tietosuojavaltuutetun toimiston verkkosivuilta. Kerro rekisteröidylle:

- kuka rekisterinpitäjä on
- mitä tarkoitusta varten rekisteröidyn henkilötietoja tarvitaan
- kuinka kauan henkilötietoja tarvitaan
- luovutetaanko henkilötietoja eteenpäin tai siirretäänkö niitä ETA-maiden ulkopuolelle
- miten rekisteröity voi käyttää henkilötietoihin liittyviä oikeuksiaan
- rekisteröidyn oikeuksiin ja vapauksiin kohdistuvista riskeistä

Tiettyä muotoa tietojen antamiselle ei ole määritetty. Yksi yleinen tapa on tietosuojaseloste. Muista päivittää tietoja ja kertoa muutoksista rekisteröidyille.

8) Huomioi rekisteröidyn oikeudet

Kuten aiemmassa kohdassa on mainittu, rekisteröidyllä on oikeus saada tietoa siitä, kuinka hänen tietojaan käsitellään. Sen lisäksi rekisteröidyllä on oikeus tutustua hänestä kerättyihin tietoihin ja oikaista virheelliset tiedot.
Rekisteröidyn pyyntöön tulee reagoida mahdollisimman nopeasti, kuitenkin pääasiassa kuukauden kuluessa pyynnön vastaanottamisesta.

Rekisteröity voi myös rajoittaa tai vastustaa tietojen käsittelyä, pyytää tietojen poistamista tai siirtää tiedot toiseen järjestelmään.
Rekisteröidyllä on myös oikeus olla joutumatta automaattisen päätöksenteon kohteeksi.
Oikeuksissa on eroavaisuuksia tilanteesta riippuen. Voit lukea lisää osoitteesta: https://tietosuoja.fi/rekisteroidyn-oikeudet-eri-tilanteissa

KYBERKUU Kymenlaaksossa
XAMK Kaakkois-Suomen ammattikorkeakoulu
KYMEN LAAKSON LIITTO
Euroopan unionin osarahoittama
Kyberturvan tulevaisuus Kymenlaaksossa, KymVake ja CyberCare Kymi

9) Reagoi tietoturvaloukkauksiin

Kaikki henkilötietojen tietoturvaloukkaukset tulee dokumentoida. Tietoturvaloukkaukseksi lasketaan tilanteet, joissa tiedot tuhoutuvat, häviävät, muuttuvat tai jos niitä luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole tietojen käsittelyoikeutta.

Jos tietoturvaloukkaus todennäköisesti aiheuttaa riskin yksilön oikeuksille ja vapauksille, siitä tulee tehdä ilmoitus tietosuojaviranomaiselle 72 tunnin kuluessa siitä, kun tietoturvaloukkaus on tullut tietoon. Vastuu ilmoituksen tekemisestä on rekisterinpitäjällä. Erikseen voi olla myös sovittuna, että henkilötietojen käsittelijä ilmoittaa loukkauksista tietosuojaviranomaiselle. Muussa tapauksessa henkilötietojen käsittelijä ilmoittaa havaitsemastaan tietoturvaloukkauksesta ensin rekisterinpitäjälle.

Koko ilmoitusta ei tarvitse tehdä heti. Jos loukkaukseen liittyvät tiedot ovat vielä vajavaisia, voidaan tietosuojaviranomaiselle tehdä ensin alustava ilmoitus, jota täydennetään kun lisätietoa on saatavilla.

Jos riski on korkea, tulee asiasta ilmoittaa myös henkilölle tai henkilöille, jotka sen kohteeksi ovat joutuneet.

10) Huomioi yrityksen sisäiset ohjeet ja koulutukset

Henkilötietojen käsittelyä tekevien työntekijöiden on tärkeää olla tietoisia yrityksen tietosuojaan liittyvistä käytännöistä ja tietojen käsittelyyn liittyvistä riskeistä. Osaamista on tärkeää ylläpitää säännöllisillä tietosuoja ja -turvakoulutuksilla.

Tietosuojan linkkilista:

- Tietosuojavaltuutetun toimiston sivuilta löydät kattavasti henkilötietojen käsittelyyn liittyvää tietoa. Sivuilla voit myös tehdä tietosuojaan liittyviä ilmoituksia. https://tietosuoja.fi/organisaatiot
- Täältä löydät tietosuojaneuvoston tietosuojaoppaan pk-yrityksille. Opas on suomenkielinen. https://www.edpb.europa.eu/sme-data-protection-guide/home_fi
- Tietosuojavaltuutetun toimiston ja TIEKE ry:n tietosuojatyökalu pk-yrityksille auttaa sinua mm. kartoittamaan yrityksesi roolin ja testaamaan, miten hyvin tietosuoja-asetuksen asettamia velvollisuuksia noudatetaan yrityksessä. https://www.tietosuojaapkyrityksille.fi/

KYBERKUU Kymenlaaksossa
XAMK Kaakkois-Suomen ammattikorkeakoulu
KYMEN LAAKSON LIITTO
Euroopan unionin osarahoittama
Kyberturvan tulevaisuus Kymenlaaksossa, KymVake ja CyberCare Kymi