

Henkilötietosuoja DigiKyky-projekti

Suvi Geier, 10/ 2022

Jyväskylän Ammattikorkeakoulu, Liiketalous, Jatkuva oppiminen

DigiKyky

Vipuvoimaa
EU:lta
2014–2020



jamk

Henkilötieto- ja henkilörekisteri-käsitteet

- Kaikki sellainen tieto, jolla voidaan yksilöidä ja tunnistaa henkilöitä on henkilötietoa. Tällaisia tietoja ovat esimerkiksi nimi, osoite, sähköpostiosoite sekä verkko-tunnistetiedot, joskus jopa koulutustieto voi olla henkilötieto.
- **Henkilörekisteri** on puolestaan näistä henkilötiedoista koostuva tietojoukko, joka on jollakin tapaa jäsennelty niin, että henkilöä koskevat tiedot voidaan löytää helposti ja ilman kohtuuttomia kustannuksia.
- → Henkilörekisteri voi muodostua, vaikkei sellaista tarkoituksella ylläpidettäisiinkään esimerkiksi, kun työpaikkahakemuksia otetaan vastaan sähköpostitse. Esimerkiksi rekrytointimoduulien hakijapankit ovat henkilörekistereitä.

Henkilötietosuoja perustuu lakeihin ja asetuksiin

- Henkilötietosuoja perustuu pääasiassa Tietosuojalakiin (<https://www.finlex.fi/fi/laki/ajantasa/2018/20181050>)

ja

- Lakiin yksityisyyden suojasta työelämässä (<https://www.finlex.fi/fi/laki/ajantasa/2004/20040759>)

Tietosuojalaki 1050/2018

30 § Henkilötietojen käsittely työsuhteen yhteydessä

- Työntekijää koskevien henkilötietojen käsittelystä, työntekijälle tehtävistä testeistä ja tarkastuksista sekä niitä koskevista vaatimuksista, teknisestä valvonnasta työpaikalla sekä työntekijän sähköpostiviestin hakemisesta ja avaamisesta säädetään yksityisyyden suojasta työelämässä annetussa laissa (759/2004).

35 § Vaitiolovelvollisuus

- Joka henkilötietojen käsittelyyn liittyviä toimenpiteitä suorittaessaan on saanut tietää jotakin toisen henkilön ominaisuuksista, henkilökohtaisista oloista, taloudellisesta asemasta taikka toisen liikesalaisuudesta, ei saa oikeudettomasti ilmaista sivulliselle näin saamiaan tietoja eikä käyttää niitä omaksi tai toisen hyödyksi tai toisen vahingoksi.

Työntekijän henkilötietosuoja

Työntekijän henkilötietojen keräämisen yleiset edellytykset ja työnantajan tiedonantovelvollisuus (Laki yksityisyyden suojasta työelämässä, Luku 2, 4 §):

- Työnantajan on kerättävä työntekijää koskevat henkilötiedot ensisijassa työntekijältä itseltään. Jos työnantaja kerää henkilötietoja muualta kuin työntekijältä itseltään, työntekijältä on hankittava suostumus tietojen keräämiseen. Suostumus ei kuitenkaan ole tarpeen silloin, kun viranomainen luovuttaa tietoja työnantajalle tämän laissa säädetyn tehtävän suorittamiseksi tai jos tietojen keräämisestä tai saamisesta laissa erikseen nimenomaisesti säädetään.
- Turvallisuusselvityksen hakemisesta säädetään turvallisuusselvityslaisissa (726/2014). Menettelystä, jolla alaikäisten kanssa työskentelemään valittavien henkilöiden rikostaustaa selvitetään, säädetään lasten kanssa työskentelevien rikostaustan selvittämisestä annetussa laissa (504/2002). Oikeudesta saada tietoja rikosrekisteristä säädetään rikosrekisterilaissa (770/1993).

GDPR-tietosuoja-asetus

- Keväällä 2018 voimaanastunut EU:n yleinen tietosuoja-asetus (General Data Protection Regulation, GDPR) on tärkein tietosuojalainsäädännön muutos yli 20 vuoteen.
- **GDPR:n vaatimat dokumentit ja perustelut henkilötietojen käsittelystä** henkilörekistereissä oli asetuksen tuoma suurin muutos henkilötietojen käsittelyyn. Jokaiselle henkilötiedolle on oltava GDPR:ssä mainittu tarveperusta.
- Samalla henkilörekisterissä olevalle **henkilölle määriteltiin suurempi vapaus sekä saada tietoa omien henkilötietojensa käsittelystä että rajoittaa niiden käyttöä.**
- GDPR-asetus ottaa kantaa ja antaa mahdollisuuden rajoittaa myös henkilö-tietojen siirtämistä esimerkiksi EU:n ulkopuolelle.

Rekisteröidyn oikeudet tietoihinsa

GDPR-tietosuoja-asetuksen mukaan rekisteröidyllä on oikeus:

- saada tietoa henkilötietojensa käsittelystä
 - saada tutustua tietoihin
 - oikaista tietoja
 - poistaa tiedot ja tulla unohdetuksi
 - rajoittaa tietojen käsittelyä
 - siirtää tiedot järjestelmästä toiseen
 - vastustaa tietojen käsittelyä
 - olla joutumatta automaattisen päätöksenteon kohteeksi.
- Rekisteröity ei voi käyttää kaikkia oikeuksia kaikissa tilanteissa. Tilanteeseen vaikuttaa esimerkiksi se, millä perusteella henkilötietoja käsitellään.

Henkilötietosuojaan valvonta ja rekisterinpitäjän velvollisuudet

- Tietosuojalainsäädännön noudattamista valvoo viranomainen:
Tietosuoja-valtuutetun toimistossa tietosuoja-valtuutettu Anu Talus (1.11.2020 alkaen), apulaistietosuoja-valtuutettu Heljä-Tuulia Pihamaa (22.3.2021 alkaen) ja apulaistietosuoja-valtuutettu Annina Hautala (1.9.2022 alkaen).
<https://tietosuoja.fi/tietosuoja-valtuutetun-toimisto>
- **Organisaatioiden velvollisuus on valvoa omia toimiaan** henkilötietojen käsittelyssä ja siten myös dokumentoida henkilötietojen tietoturvaloukkaukset sekä niiden vaikutukset ja toteutetut korjaavat toimet riippumatta siitä, mitä toimenpiteitä tietoturvaloukkauksesta lopulta seuraa.
Dokumentointivelvollisuuden tai ilmoituksen tekemisen laiminlyöminen on tietosuoja-asetuksen vastaista.

Henkilötietosuojan valvonta ja rekisterinpitäjän velvollisuudet

- Dokumentointivelvollisuuden piiriin kuuluvat myös tietojärjestelmään kohdistuneen tietoturvaloukkauksen osalta tapahtuma-ajan lokitiedot. Tietosuojavaltuutettu voi pyytää lokitietoja tietoturvaloukkausta koskevan ilmoituksen käsittelyä varten.
- Henkilötietojen tietoturvaloukkauksesta on ilmoitettava tietosuojavaltuutetun toimistolle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta.
<https://tietosuoja.fi/tietoturvaloukkaukset>

Henkilötietojen tietoturvaloukkaukset.

"Ihminen on tietoturvan heikoin lenkki"

Tietoturvaloukkaukset ovat usein vahinkoja tai seurauksia inhimillisistä virheistä tai osaamattomuudesta. Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi:

- hävinnyt tiedonsiirtoväline, kuten USB-tikku
- varastettu tietokone
- hakkerointi
- haittaohjelmatartunta
- kyberhyökkäys
- tulipalo datakeskuksessa
- tiliotteen tai sähköpostin postitus väärälle henkilölle.

Tietoturvaloukkaukset

- Tietoturvaloukkauksista määrätään tuntuviakin sakkoja. Suurin sakko on Ranskan tietosuojaviranomaisen Googlelle määräämä 50 miljoonan euron sakko. Saksassa on määrätty kymmenien tuhansien eurojen sakkoja ja loput sakot ovat olleetmittaluokaltaan tuhansia euroja. Suomessa ei helmikuussa 2019 ole määrätty sakkoja. Sakkojen lukumäärä on pieni suhteutettuna 59 000 ilmoitettuun tietosuojaloukkaukseen. (Lähde: <http://blogi.tietosi.fi/fi/gdpr-paivitys-sanktioita-odotellessa>)

Henkilötietosuoja rekrytoinnissa

Työntekijöitä on työyhteisössä kohdeltava oikeudenmukaisesti ja yhdenvertaisesti niin, että ketään ei syrjitä. Syrjintä on kielletty myös laissa:

Yhdenvertaisuuslaki (1325/2014)

- Ketään ei saa syrjiä iän, alkuperän, kansalaisuuden, kielen, uskonnon, vakaumuksen, mielipiteen, poliittisen toiminnan, ammattiyhdistystoiminnan, perhesuhteiden, terveydentilan, vammaisuuden, seksuaalisen suuntautumisen tai muun henkilöön liittyvän syyn perusteella.
- <https://valtioneuvosto.fi/-/1410853/yhdenvertaisuuslaki-uudistuu>
- <https://syrjinta.fi/etusivu> - Yhdenvertaisuusvaltuutetun toiminta
- Mitä syrjintä on – ja ei ole?
<https://www.tyosuojelu.fi/tyosuhde/yhdenvertaisuus/syrjinta>

Laki yksityisyyden suojasta työelämässä

Terveydentilaa koskevien tietojen käsittely 5 §

Työnantajalla on oikeus käsitellä työntekijän terveydentilaa koskevia tietoja, **jos tiedot on kerätty työntekijältä itseltään tai hänen kirjallisella suostumuksellaan muualta ja** tietojen käsittely on tarpeen sairausajan palkan tai siihen rinnastettavien terveydentilaan liittyvien etuuksien suorittamiseksi taikka sen selvittämiseksi, onko työstä poissaoloon perusteltu syy, taikka jos työntekijä nimenomaisesti haluaa selvitetävän työkykyisyyttään terveydentilaa koskevien tietojen perusteella. Lisäksi työnantajalla on oikeus käsitellä näitä tietoja niissä tilanteissa ja siinä laajuudessa, kuin muualla laissa erikseen säädetään.

jamk