TO

TIETOSUOJA-ASETUKSEN SOVELTAMINEN ALKAA TOUKOKUUSSA

EU:n tietosuoja-asetuksen soveltaminen alkaa 25.5.2018. Tästä alkaen henkilötietojen käsittelyn tulee olla tietosuoja-asetuksen mukaista ja se tulee pystyä lisäksi osoittamaan dokumentoidusti. EU:sta annetaan vähitellen tarkempia tulkintoja asetuksen soveltamisesta ja Suomen lainsäädäntöön valmistellaan muutoksia asetuksen johdosta, mutta lainsäädäntötyö on vielä kesken. Tiedotamme mahdollisista tarkennuksista ja ohjeistuksista sitä mukaa, kun niitä tulee.

Tässä vaiheessa on tehtävä seuraavat toimenpiteet:

1. SELVITÄ, MITÄ HENKILÖTIETOJA KÄSITTELET

Henkilötiedoilla tarkoitetaan kaikkia luonnolliseen henkilöön (=ihminen) liittyviä tietoja. Henkilötietoja ovat esimerkiksi nimi, henkilötunnus, terveystieto, osoite tai sähköpostiosoite.

Henkilötietoja eivät ole yrityksen tiedot tai yritykseen liittyvät tiedot, eivätkä tiedot, jotka eivät yksilöi ketään henkilöä.

Työntekijöiden henkilötietoja sisältävät esimerkiksi
- Tiedot henkilöstöstä
- Palkkakortit
- Palkkalistat
- Työvuorolistat
- Lomalistat
- Ay-jäsenmaksuvaltakirjat
- Jäsenmaksujen tilitysluettelot
- Veroilmoitukset
- Eläketietoilmoitukset
- Ulosottomääräykset
- Tiedot työtodistuksia varten

Yrityksessä voidaan käsitellä myös esimerkiksi kuluttaja-asiakkaiden tai yritysasiakkaiden yhteyshenkilöiden henkilötietoja.

2. SELVITÄ, MITÄ HENKILÖREKISTEREITÄ YRITYKSESSÄSI ON OLEMASSA

Henkilörekisteri muodostuu, jos on olemassa henkilötietoja, joita tallennetaan, säilytetään tai käsitellään jotakin käyttötarkoitusta varten.

Henkilörekisteriksi katsotaan kuuluvaksi kaikki tiedot, joita käytetään samassa käyttöyhteydessä riippumatta siitä, miten ja mihin eri paikkoihin tiedot on tallennettu

INFRA ry
Y-tunnus: 0116966-8

Unioninkatu 14
00130 Helsinki

infra@infra.fi
+358 9 129 91

www.infra.fi

TO

3. VARMISTU, ETTÄ KÄSITTELET HENKILÖTIETOJA TIETOSUOJA-ASETUKSEN MUKAISESTI

- Kartoita henkilötietojen käsittelyn tämänhetkinen tilanne:
  - Mitä henkilötietoja kerätään ja käsitellään?
  - Käyttötarkoitus ja käsittelyn peruste?
  - Onko henkilötietojen käsittelyä ulkoistettu ja onko tietosuoja huomioitu ulkoistussopimuksessa?
  - Luovutetaanko henkilötietoja yrityksestä ja millä perusteella?
  - Henkilötietojen käsittelijät, heidän perehdytys/koulutus ja yrityksen ohjeistus henkilötietojen käsittelyn tietosuojasta?
  - Miten huolehdittu tietoturvasta ja käsittelyn rajoittamisesta määräaikoineen (tekniset ja organisatoriset toimenpiteet)?
  - Miten toteutetaan rekisteröityjen oikeudet?
  - Tuleeko nimetä tietosuojavastaava?
  - Tietoturvaan liittyvien riskien arviointi (ja tarvittaessa vaikutustenarviointi) ja minimointi sekä toimenpiteet tietoturvaloukkausten yhteydessä?
- Korjaa mahdolliset puutteet henkilötietojen käsittelyssä.
- Arvioi henkilötietojen käsittelyyn liittyvät riskit.
- Osoita, että noudatat tietosuoja-asetusta:
  - käsittele henkilötietoja lainmukaisesti
  - käsittele vain kunkin käyttötarkoituksen kannalta tarpeellisia henkilötietoja
  - minimoi käsiteltävät henkilötiedot, älä käsittele tietoja, joita ei tarvita
  - päivitä ja korjaa virheelliset henkilötiedot
  - säilytä henkilötietoja vain sen aikaa, kun niitä tarvitaan
  - huolehdi henkilötietojen oikeellisuudesta
  - suojaa henkilötiedot
- Varaudu tietosuojaloukkauksiin.

4. VARMISTU, ETTÄ SINULLA ON PERUSTE KÄSITELLÄ HENKILÖTIETOJA

Henkilötietoja saa käsitellä neljällä perusteella:

1. Rekisteröidyn vapaaehtoinen, yksilöity ja selkeä suostumus

Henkilötietojen käsittely voi perustua rekisteröidyn antamaan suostumukseen yhtä tai useampaa erityistä henkilötietojen käsittelytarkoitusta varten. Jos käsittely perustuu suostumukseen, rekisterinpitäjän on pystyttävä osoittamaan myös jälkikäteen, että rekisteröity on antanut suostumuksen.

2. Henkilötietojen käsittely perustuu osapuolten väliseen sopimukseen

Suostumusta ei tarvita, jos henkilötietojen käsittely on tarpeen sopimuksen täytäntöön panemiseksi tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi.

INFRA ry
Y-tunnus: 0116966-8

Unioninkatu 14
00130 Helsinki

infra@infra.fi
+358 9 129 91

www.infra.fi

Esimerkiksi palvelun tai tavaran myyntiä tai vuokrausta koskevaan sopimukseen liittyen voidaan sopimusosapuolena olevan asiakkaan henkilötietoja käsitellä sopimuksen perusteella.

3. Rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu

Henkilötietojen käsittely voi tietosuoja-asetuksen mukaan perustua rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseen. Jos käsittely perustuu oikeutettuun etuun, ei käsittelyyn tarvitse pyytää suostumusta.

Asetuksen mukaan oikeutettu etu voi olla olemassa esimerkiksi silloin, kun rekisteröidyn ja rekisterinpitäjän välillä on merkityksellinen ja asianmukainen suhde. Näin on muun muassa, kun rekisteröity on rekisterinpitäjän asiakas tai tämän palveluksessa.

Asetuksessa todetaan lisäksi, että rekisterinpitäjillä, jotka kuuluvat konserniin tai keskuselimeen kuuluvaan laitokseen, voi olla sisäisistä hallinnollisista syistä johtuen oikeutettu etu siirtää konsernin sisällä henkilötietoja, mukaan lukien asiakkaiden tai työntekijöiden henkilötietojen käsittely.

4. Henkilötietojen käsittely perustuu rekisterinpitäjän lakisääteiseen velvollisuuteen

Tietosuoja-asetuksen mukaan laillinen peruste käsitellä henkilötietoja on myös silloin, kun henkilötietojen käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Myöskään tällöin käsittelyyn ei tarvitse pyytää erikseen suostumusta

5. INFORMOI REKISTERÖITYJÄ

Rekisteröidyille on informoitava:

- rekisterinpitäjän ja hänen edustajan yhteystiedot
- henkilötietojen käsittelyn tarkoitukset ja käsittelyn oikeusperuste
- mitä henkilötietoryhmiä yritys kerää ja käsittelee sekä mistä lähteistä tietoja saadaan
- tieto siitä, luovutetaanko henkilötietoja, ja jos luovutetaan, tietojen vastaanottajat / vastaottajien ryhmät
- jos henkilötietoja siirretään EU:n ulkopuolelle, tieto siitä sekä asetuksen edellyttämä muu selvitys siirroista
- henkilötietojen säilytysaika tai jos se ei ole mahdollista, kriteerit ajan määrittämiseksi
- rekisteröidyn asetuksen mukaisista oikeuksista (mm. oikeus pyytää itseään koskevien henkilötietojen oikaisemista) sekä oikeudesta peruuttaa annettu suostumus ja tehdä valitus valvontaviranomaiselle

Jos rekisterinpitäjä aikoo käsitellä henkilötietoja edelleen muihin tarkoituksiin kuin niihin, joihin henkilötiedot kerättiin, rekisterinpitäjän on informoitava rekisteröityä muista tarkoituksista ennen jatkokäsittelyä.

INFRA ry
Y-tunnus: 0116966-8

Unioninkatu 14
00130 Helsinki

infra@infra.fi
+358 9 129 91

www.infra.fi

6. KARTOITA HENKILÖTIETOJEN KÄSITTELYYN LIITTYVÄT RISKIT JA SUOJAA HENKILÖTIEDOT

Rekisterinpitäjän on suunniteltava ja toteutettava asianmukainen tietojen suojaaminen. Sähköisiin järjestelmiin voi liittyä tietovuotoriskejä, mutta myös manuaalisiin aineistoihin voi liittyä riskejä, esimerkiksi varastamisen tai tuhoutumisen (esim. tulipalo) riski. Vielä suurempi riski voi liittyä luvattomaan käyttöön.

Jos yrityksen toimistossa on esimerkiksi työntekijöiden työsopimuksia mapissa lukottomassa kaapissa, nämä ovat melko helposti muiden työntekijöiden tai vierailijoiden saatavilla. Tällaiset riskit pitää välttää ja siksi yrityksen tulee miettiä, miten tiedot suojataan.

Rekisterinpitäjän ja henkilötietojen käsittelijän on arvioitava riskit ja toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet.

Kun arvioidaan riskejä ja asianmukaista turvallisuustasoa, on huomioitava erityisesti, millaisia riskejä on, että henkilötiedot tuhoutuvat, häviävät tai muuttuvat tai että henkilötietoihin pääsee luvatta käsiksi.

Rekisterinpitäjän ja henkilötietojen käsittelijän on varmistettava, että jokainen rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti.

Henkilöstöä tulee myös opastaa ja kouluttaa ja yrityksessä tulee laatia ohjeet henkilötietojen käsittelystä. Ohjeiden noudattamista pitää valvoa.

Toimenpiteitä voivat olla esimerkiksi:

- Henkilöstön koulutus tietoturva-asioihin
- Salasanat
- Järjestelmien käyttöoikeudet ajan tasalla ja vain kulloisenkin työtehtävän mukaisesti
- Tietoturva etätyössä
- Salassapitositoumukset
- Kulunvalvonta toimitiloissa
- Clean desk -policy

7. VARAUDU ILMOITTAMAAN TIETOTURVALOUKKAUKSISTA

Rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta toimivaltaiselle valvontaviranomaiselle. Ilmoituksen voi jättää tekemättä vain, jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä.

INFRA ry
Y-tunnus: 0116966-8

Unioninkatu 14
00130 Helsinki

infra@infra.fi
+358 9 129 91

www.infra.fi

Ilmoituksessa on vähintään kuvattava henkilötietojen tietoturvaloukkaus, ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa sekä kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset ja toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta. Mikäli henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, rekisterinpitäjän on lähtökohtaisesti ilmoitettava tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä.

8. TEE SELOSTE HENKILÖTIETOJEN KÄSITTELYSTÄ

- Rekisterinpitäjän nimi ja yhteystiedot
- Henkilötietojen käsittelyn tarkoitus ja peruste
- Rekisterin tietosisältö
- Tietolähteet
- Henkilötietojen säilyttäminen ja käsittelyn rajoittaminen
- Henkilötietojen luovuttaminen
- Henkilötietojen käsittelyyn liittyvät riskit
- Rekisterin suojaus
- Rekisteröidyn oikeudet
    - Oikeus saada yritykseltä pääsy kysyjää itseään koskeviin henkilötietoihin (= tarkastusoikeus)
    - Oikeus pyytää häntä itseään koskevien tietojen oikaisemista tai poistamista
    - Oikeus käsittelyn rajoittamiseen
    - Oikeus vastustaa häntä itseään koskevien tietojen käsittelyä
    - Oikeus peruuttaa suostumus
    - Oikeus tehdä valitus valvontaviranomaiselle
    - Oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn
- Tietoturvaloukkauksista ilmoittaminen

Ks. lomake liitteenä.

9. VARMISTA TIETOTURVA ULKOISTETUSSA HENKILÖTIETOJEN KÄSITTELYSSÄ

Sopimuksessa on

a) yksiöitävä, mitä henkilötietojen käsittelyä ulkoistetaan ja keitä ja mitä tietoja ulkoistaminen koskee
    - esim. ulkoistetaan palkanmaksu
    - esim. koskee yrityksen työntekijöitä
    - esim. ulkoistettavat tiedot ovat työntekijöiden henkilötunnukset ja yhteystiedot
b) määriteltävä käsittelyn kesto
    - milloin henkilötietojen käsittelijän oikeus tietojenkäsittelyyn alkaa ja päättyy

INFRA ry
Y-tunnus: 0116966-8

Unioninkatu 14
00130 Helsinki

infra@infra.fi
+358 9 129 91

www.infra.fi

c) velvoitettava henkilötietojen käsittelijä sitoutumaan käsittelemään henkilötietoja ainoastaan rekisterinpitäjän ohjeiden ja sopimusehtojen mukaisesti
d) velvoitettava henkilötietojen käsittelijä salassapitoon ja samalla varmistettava, että henkilötietoja käsittelevät henkilöt (henkilötietojen käsittelijän työntekijät) sitoutuvat noudattamaan salassapitovelvollisuutta
e) velvoitettava henkilötietojen käsittelijä toteuttamaan riittävät turvatoimet henkilötietojen suojaamiseksi
   - esim. tietokoneiden virustorjunta, palomuurit ym.
   - esim. toimitilojen kulunvalvonta
   - esim. riittävät ja asiantuntevat resurssit
f) sovittava, tarvitseeko tietojen käsittelijä rekisterinpitäjältä suostumuksen alihankkijan käyttämiseksi vai riittääkö jälkikäteinen ilmoitus.
   - Jos jälkikäteinen ilmoitus riittää, rekisterinpitäjän on tarvittaessa voitava vastustaa alihankkijan käyttämistä
   - Henkilötietojen käsittelijällä on vastuu käyttämästään alihankkijasta
g) velvoitettava käsittelijä on avustamaan rekisterinpitäjää tämän vastatessa rekisteröityjen pyyntöihin
   - esim. tilanteissa, joissa rekisteröidyt haluavat pääsyn omiin tietoihinsa
h) velvoitettava käsittelijä auttamaan rekisterinpitäjää varmistamaan tiettyjen rekisterinpitäjän velvoitteiden, kuten tietojen poistopyynnön, noudattaminen
i) sovittava henkilötietojen poistosta tai palautuksesta käsittelyyn liittyvien palveluiden päättyessä
   - jollei muu lainsäädäntö edellytä tietojen säilyttämistä
   - on sovittava joko, että henkilötietojen käsittelijä poistaa tai palauttaa kaikki henkilötiedot rekisterinpitäjälle ja poistaa olemassa olevat jäljennökset
j) velvoitettava henkilötietojen käsittelijä ilmoittamaan tietoturvaloukkauksista rekisterinpitäjälle

Sopimuksessa voidaan lisäksi sopia osapuolten vahingonkorvausvelvollisuudesta ja mahdollisista vastuunrajoituksista.

Tietosuoja-asetuksen edellyttämän sopimisen voi käytännössä toteuttaa sopimalla asiasta osapuolten välisessä palvelusopimuksessa. Mikäli osapuolten välillä on jo voimassa oleva sopimus, sopimukseen voidaan laatia henkilötietojen käsittelyä koskeva liite, jolloin muita sopimusehtoja ei tarvitse sopia uudestaan.

10. TIETOSUOJA-ASETUKSESSA SÄÄDETTY TIETOSUOJAVASTAAVA

Tieto-asetuksen mukaan tietosuojavastaavan nimittäminen on pakollista, jos rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa. Edellytyksenä on siis, että rekisterinpitäjän ydintehtävien pitää olla henkilötietojen käsittelyä. Tie-

INFRA ry
Y-tunnus: 0116966-8

Unioninkatu 14
00130 Helsinki

infra@infra.fi
+358 9 129 91

www.infra.fi

tosuojavaltuutettu on ohjeistanut, että yrityksen pitää arvioida, kuuluuko sen ydintehtäviin henkilötietojen käsittely ja jos kuuluu, tietosuojavastaava pitää nimetä. Tietosuojavaltuutettu on niin ikään ohjeistanut, että mikäli yritys virheellisesti jättäisi tietosuojavastaavan nimeämättä tilanteessa, jossa se pitäisi nimetä, yritykseltä edellytetään ensisijaisesti asian korjaamista sen sijaan, että yritykselle määrättäisiin sakkoja.

Tietosuojavastaava kannattaa nimittää vain, jos siihen on tietosuoja-asetuksen asettama velvoite. Tietosuojavastaavaa ei ole tarkoituksenmukaista nimittää muissa tilanteissa, sillä tietosuoja-asetuksen tietosuojavastaavaa koskevia määräyksiä sovelletaan myös vapaaehtoisesti nimitettyihin tietosuojavastaaviin. Sen sijaan yrityksen kannattaa nimetä tietosuoja-asioiden yhteyshenkilö, joka on perehtynyt tietosuoja-asetuksen velvoitteisiin ja niiden käytännön toteuttamiseen yrityksessä. Kyseistä henkilö ei kannata nimittää tietosuojavastaavaksi, sillä muutoin henkilö voidaan sekoittaa tietosuoja-asetuksen mukaiseen tietosuojavastaavaan.

Tämänhetkisen tiedon mukaan tietosuojavastaavan nimeämiseen ei juurikaan ole tarvetta infra-alan yrityksissä, sillä henkilötietojen käsittelyä ei voida pitää yritysten ydintehtävänä. Tästä syystä kannattaa rauhassa odottaa mahdollisia tarkempia tulkintoja.

LISÄTIETOJA

Tiina Olin
Lakimies
puh 050 452 6633
tiina.olin@infra.fi

Liitteet Tietosuojakartoitus
Tietosuojaseloste

TIETOSUOJAKARTOITUS

Alla on lueteltu kysymyksiä, jolla kartoitetaan yrityksen nykytila henkilötietojen käsittelyn tietosuojan suhteen ja täytetään samalla osaltaan tietosuoja-asetuksen mukaista osoitusvelvollisuutta tietosuoja-asetuksen velvoitteiden noudattamisesta.

Kartoita henkilötietojen käsittelyn nykytila vastaamalla alla oleviin kysymyksiin. Korjaa puutteet.

Laadi lisäksi seloste henkilötietojen käsittelystä.

1. Mitä henkilötietoja kerätään ja käsitellään? Mitä henkilörekistereitä yrityksessä on?

2. Henkilötietojen käyttötarkoitus ja käsittelyn peruste?

3. Onko henkilötietojen käsittelyä ulkoistettu ja onko tietosuoja huomioitu ulkoistussopimuksessa? (huomioi sopimusehdot, jotka on otettava sopimukseen)

4. Luovutetaanko henkilötietoja yrityksestä ja millä perusteella?

5. Henkilötietojen käsittelijät, heidän perehdytys/koulutus ja yrityksen ohjeistus henkilötietojen käsittelyn tietosuojasta?

6. Miten huolehdittu tietoturvasta ja käsittelyn rajoittamisesta määräaikoineen (tekniset ja organisatoriset toimenpiteet)?

7. Miten toteutetaan rekisteröityjen oikeudet?

8. Tuleeko nimetä tietosuojavastaava?

9. Tietoturvaan liittyvien riskien arviointi (ja tarvittaessa vaikutustenarviointi) ja minimointi sekä toimenpiteet tietoturvaloukkausten yhteydessä?

TIETOSUOJASELOSTE

<table>
<tr><td rowspan="4">REKISTERINPITÄJÄN NIMI JA YHTEYSTIEDOT</td><td colspan="2">Rekisterinpitäjän nimi</td><td>Y-tunnus</td></tr>
<tr><td colspan="3">Postiosoite</td></tr>
<tr><td colspan="3">Yhteyshenkilö</td></tr>
<tr><td>Sähköpostiosoite</td><td colspan="2">Puhelin</td></tr>
<tr><td>REKISTERIN NIMI</td><td colspan="3"></td></tr>
<tr><td>HENKILÖTIETOJEN KÄSITTELYN TARKOITUS JA PERUSTE</td><td colspan="3"></td></tr>
<tr><td>REKISTERIN TIETOSISÄLTÖ</td><td colspan="3"></td></tr>
<tr><td>SÄÄNNÖNMUKAISET TIETOLÄHTEET</td><td colspan="3"></td></tr>
<tr><td>HENKILÖTIETOJEN SÄILYTTÄMINEN JA KÄSITTELYN RAJOITTAMINEN</td><td colspan="3"></td></tr>
</table>

HENKILÖTIETOJEN LUOVUTUS	☐ Henkilötietoja luovutetaan säännönmukaisesti, lisätiedot ☐ Tietoja siirretään EU:n tai ETA:n ulkopuolelle, lisätiedot
HENKILÖTIETOJEN KÄSITTELYYN LIITTYVÄT RISKIT	
REKISTERIN SUOJAUS	☐ Manuaalinen aineisto, miten suojattu ☐ Sähköinen aineisto, miten suojattu
TARKASTUSOIKEUS JA OIKEUS VAATIA TIEDON KORJAAMISTA	
MUUT HENKILÖTIETOJEN KÄSITTELYYN LIITTYVÄT OIKEUDET	
TIETOTURVA-LOUKKAUKSISTA ILMOITTAMINEN	