Euroopan komissio

Yleinen tietosuoja-asetus: uusia mahdollisuuksia, uusia velvoitteita

Tarpeellista tietoa yrityksille EU:n yleisestä tietosuoja-asetuksesta

Oikeus- ja kuluttaja-asiat

Printed by Bietlot in Belgium

Luxemburg: Euroopan unionin julkaisutoimisto, 2018

Print	ISBN 978-92-79-79410-0	doi:10.2838/947451	DS-01-18-082-FI-C
PDF	ISBN 978-92-79-79449-0	doi:10.2838/4220	DS-01-18-082-FI-N

SISÄLLYSLUETTELO

LUKU 1

LIIKETOIMINTAMAHDOLLISUUKSIA

Yleisellä tietosuoja-asetuksella säädellään yritysten tapaa käsitellä ja hallita henkilötietoja. Asetus tulee voimaan 25.5.2018, ja sitä sovelletaan kaikkiin yrityksiin ja organisaatioihin (esim. sairaaloihin ja julkishallintoon). Se on merkittävin muutos EU:n tietosuojalainsäädännössä yli 20 vuoteen.

Yleinen tietosuoja-asetus antaa kansalaisille enemmän valtaa hallita omien henkilötietojensa käyttöä ja keventää sääntely-ympäristöä yrityksille. Tätä varten asetuksella luodaan yhdenmukaiset puitteet tietosuojalainsäädännölle koko EU:ssa. Toisin sanoen koko EU:ssa sovelletaan yksiä sääntöjä sen sijaan, että jokaisella maalla olisi omat tietosuojalakinsa. Eri maissa toimivan yrityksen ei siten tarvitse enää noudattaa monia, usein toisistaan poikkeavia säädöksiä. Voidakseen tarjota palveluja eri puolilla EU:ta niiden on noudatettava vain yleistä tietosuoja-asetusta.

Yleisen tietosuoja-asetuksen edut yrityksille

- **Yksi unioni, yksi lainsäädäntö:** yksien sääntöjen ansiosta yritysten on helpompaa ja edullisempaa harjoittaa liiketoimintaa EU:ssa.
- **Yhden luukun järjestelmä:** useimmissa tapauksissa yritykset ovat tekemisissä vain yhden tietosuojaviranomaisen kanssa.
- **Euroopan maaperällä eurooppalaiset säännöt:** EU:n ulkopuolelle sijoittautuneiden yritysten on noudatettava samoja sääntöjä kuin eurooppalaisten yritysten, kun ne tarjoavat tuotteita ja palveluja EU:n alueella asuville henkilöille.
- **Riskiperusteinen lähestymistapa:** yleisessä tietosuoja-asetuksessa ei aseteta raskaita ja kaikille samantasoisia velvoitteita, vaan velvoitteet mukautetaan riskitasoon.
- **Innovaatioon soveltuvat säännöt:** yleinen tietosuoja-asetus on teknologianeutraali.

Tärkeintä on luottamus

Henkilötietosuoja on merkittävä huolenaihe ihmisille. Luottamus digitaalisia ympäristöjä kohtaan on edelleen heikko. Eurobarometrikyselyn mukaan

- kahdeksan kymmenestä on sitä mieltä, ettei omien henkilötietojen käsittely ole täysin omassa hallinnassa
- kuusi kymmenestä ei luota verkkoyrityksiin
- yli 90 prosenttia eurooppalaisista haluaa, että kaikissa EU-maissa sovelletaan samoja tietosuojaoikeuksia.

Yleinen tietosuoja-asetus antaa yrityksille mahdollisuuden lisätä kuluttajien luottamusta hallinnoimalla henkilötietoja riskiperusteisesti.

”Yritykset, jotka eivät suojaa asianmukaisesti yksilöiden henkilötietoja, menettävät kuluttajan luottamuksen. Luottamus on ensisijaisen tärkeää, jotta ihmiset saadaan käyttämään uusia tuotteita ja palveluja.”

LUKU 2

PERUSTIETOA YLEISESTÄ TIETOSUOJA-ASETUKSESTA

Koskeeko yleinen tietosuoja-asetus minun yritystäni?

Yleinen tietosuoja-asetus koskee ***kaikkia*** yrityksiä, jotka

käsittelevät henkilötietoja automaattisesti tai **manuaalisesti** (jos tiedot järjestetään tiettyjen perusteiden mukaisesti).

Sääntöjä on noudatettava myös siinä tapauksessa, että yrityksesi käsittelee tietoja ainoastaan toisten yritysten puolesta.

Asetusta sovelletaan, jos

- yrityksesi käsittelee henkilötietoja ja on sijoittautunut EU:n alueelle, riippumatta siitä, missä varsinainen tietojenkäsittely tapahtuu, tai
- yrityksen kotipaikka on EU:n ulkopuolella, mutta se tarjoaa tuotteita tai palveluja tai seuraa yksilöiden käyttäytymistä EU:ssa.

Mitkä tiedot ovat henkilötietoja?

Henkilötietoja ovat kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot. Näitä ovat muun muassa:

- nimi
- osoite ja puhelinnumero
- sijainti
- terveystiedot
- tulot ja pankkitilitiedot
- kulttuuriin liittyvät mieltymykset
- ... ja monet muut tiedot.

Asetuksen soveltamisalaan kuuluvat myös henkilötiedot, jotka on anonymisoitu, salattu tai pseudonymisoitu mutta joita voidaan kuitenkin käyttää henkilön tunnistamiseen. Henkilötietoja, jotka on anonymisoitu peruuttamattomasti tai siten, ettei henkilö ole enää tunnistettavissa, ei kuitenkaan katsota henkilötiedoiksi, eivätkä ne siten kuulu asetuksen soveltamisalaan.

Yleinen tietosuoja-asetus on myös teknologianeutraali, mikä tarkoittaa sitä, että se suojaa henkilötietoja riippumatta siitä, mitä teknologiaa tietojenkäsittelyssä käytetään ja miten henkilötietoja säilytetään. Yritys kuuluu asetuksen soveltamisalaan riippumatta siitä, käsitelläänkö ja säilytetäänkö henkilötietoja tietojärjestelmässä vai paperiasiakirjoina.

”Yritys kuuluu asetuksen soveltamisalaan riippumatta siitä, käsitelläänkö ja säilytetäänkö henkilötietoja tietojärjestelmässä vai paperiasiakirjoina.”

Erityisiin tietoryhmiin kuuluvien henkilötietojen (arkaluontoiset tiedot) kanssa on noudatettava erityistä varovaisuutta

Jos yrityksesi keräämät henkilötiedot sisältävät esimerkiksi henkilön terveyttä, rotua, seksuaalista suuntautumista, uskontoa tai vakaumusta, poliittisia mielipiteitä tai ammattiliiton jäsenyyttä koskevia tietoja, nämä tiedot luokitellaan arkaluontoisiksi tiedoiksi. Yritys saa käsitellä näitä tietoja vain erityistilanteissa, ja käsittely saattaa edellyttää lisäsuojatoimia, kuten salaamista.

Mitä on henkilötietojen käsittely?

Yleisen tietosuoja-asetuksen mukaan henkilötietojen käsittelyn määritelmä käsittää muun muassa henkilötietojen keruun, käytön ja poistamisen.

Valvotaanko yrityksen tiloja valvontakameroilla? Käytetäänkö henkilötietoja sisältävää tietokantaa liiketoimintatarkoituksiin? Lähettääkö yritys mainoksia sähköpostitse? Poistaako yritys (digitaalisia) työntekijätiedostoja tai jaettuja asiakirjoja? Lataako yritys jonkun henkilön kuvan verkkosivustolleen tai sosiaaliseen mediaan?

Jos vastasit johonkin edellä esitetyistä kysymyksistä myöntävästi, yrityksesi käsittelee henkilötietoja.

Miten yleinen tietosuoja-asetus auttaa alentamaan kustannuksia?

Yleisessä tietosuoja-asetuksessa huomioidaan yritysten tarpeet. Asetuksen tavoitteena on muun muassa vähentää hallinnollisia vaatimuksia ja näin alentaa kuluja ja minimoida hallinnollista taakkaa:

- **Ei enää ennakkoilmoituksia**: uudistuksen myötä suurin osa valvontaviranomaisille tehtävistä ennakkoilmoituksista ja niihin liittyvistä kustannuksista poistuu.
- **Tietosuojavastaavat**: yritysten on nimitettävä tietosuojavastaava etupäässä siksi, että yrityksen ydinliiketoimintaan liittyy arkaluonteisten henkilötietojen käsittelyä laajassa mittakaavassa tai yksilöiden laajamittaista, säännöllistä ja järjestelmällistä seurantaa. Julkishallinnot ovat velvollisia nimittämään tietosuojavastaavan.
- **Tietosuojaa koskevat vaikutustenarvioinnit**: yritykset ovat velvollisia tekemään tietosuojaa koskevan vaikutustenarvioinnin, jos suunniteltu käsittely aiheuttaa yksilöiden oikeuksiin ja vapauksiin liittyvän korkean riskin.
- **Rekisterin pitäminen**: alle 250 työntekijän yritykset eivät ole velvollisia pitämään rekisteriä, paitsi jos tietojenkäsittely ei ole satunnaista tai se kohdistuu arkaluonteisiin tietoihin.

”Asetuksen tavoitteena on muun muassa vähentää hallinnollisia vaatimuksia ja näin alentaa kuluja ja minimoida hallinnollista taakkaa.”

LUKU 3

ASETUKSEN MUKAISET VELVOITTEET YRITYKSILLE

Yleisessä tietosuoja-asetuksessa asetetaan yrityksille EU:n tasolla tietojenkäsittelyä koskevia suoria velvoitteita. Asetuksen mukaan yritys voi käsitellä henkilötietoja vain tietyin edellytyksin. Käsittelyn on esimerkiksi oltava asianmukaista ja läpinäkyvää, tietoja voidaan käsitellä vain erityiseen ja lainmukaiseen tarkoitukseen ja tietojenkäsittelyn on rajoituttava kyseisen tarkoituksen mukaisiin tietoihin. Tietojenkäsittelyn on myös perustuttava johonkin seuraavista oikeudellisista perusteista.

- Kyseisen yksilön **suostumus**.
- Yrityksen ja yksilön väliseen **sopimukseen perustuva velvoite**.
- **Lakisääteinen velvoite**.
- Yksilön **elintärkeiden etujen** suojaaminen.
- **Yleisen edun vuoksi toteuttavan tehtävän** suorittaminen.
- Yrityksen **oikeutetut edut**, mutta vain kun yritys on tarkistanut, ettei käsittely vaikuta merkittävästi kyseisen henkilön perusoikeuksiin ja -vapauksiin. Jos henkilön oikeudet syrjäyttävät yrityksen edut, yritys ei voi käsitellä tietoja.

Suostumuksen pyytäminen henkilötietojen käytölle

Yleisessä tietosuoja-asetuksessa säädetään suostumukseen perustuvaa tietojenkäsittelyä koskevat tiukat säännöt. Sääntöjen tarkoituksena on varmistaa, että henkilö ymmärtää, mihin hän antaa suostumuksensa. Suostumuksen on oltava siten **vapaaehtoinen, yksilöity, tietoinen** ja **yksiselitteinen**, ja suostumuspyyntö on esitettävä selkeällä ja yksinkertaisella kielellä. Lisäksi suostumus pitää ilmaista **suostumusta ilmaisevalla toimella**, kuten rastittamalla ruutu verkossa tai allekirjoittamalla lomake.

Jos suostumuksen perusteella käsitellään **lasta** koskevia henkilötietoja, käsittelylle on saatava myös vanhemman suostumus. Koska ikäraja vaihtelee maakohtaisesti 13:sta 16 vuoteen, asia kannattaa tarkistaa kansallisesta lainsäädännöstä.

Muista!
Kun suostumus henkilötietojen käsittelyyn on annettu, voit käsitellä tietoja vain ilmoitettuun tarkoitukseen. Sinun on myös annettava henkilölle mahdollisuus peruuttaa suostumus.

Yrityksen roolin ja vastuun määrittäminen

Kun olet todennut, että yleinen tietosuoja-asetus koskee yritystäsi ja että yrityksesi käsittelee henkilötietoja, on aika määritellä yrityksesi rooli.

Tietosuojasäännöt ja velvoitteet vaihtelevat sen mukaan, onko yritys rekisterinpitäjä vai henkilötietojen käsittelijä. Rekisterinpitäjä määrittelee henkilötietojen käsittelyn tarkoituksen ja käsittelytavan, kun taas henkilötietojen käsittelijä vain käsittelee henkilötietoja rekisterinpitäjän puolesta. Tämä ei kuitenkaan tarkoita sitä, että henkilötietojen käsittelijä voi piiloutua rekisterinpitäjän taakse.

Asetuksessa rekisterinpitäjä velvoitetaan käyttämään vain sellaista henkilötietojen käsittelijää, joka voi antaa riittävät takeet. Takeista on määrättävä rekisterinpitäjän ja henkilötietojen käsittelijän välisessä kirjallisessa sopimuksessa. Sopimuksessa on oltava joukko pakollisia lausekkeita, joissa esimerkiksi todetaan, että henkilötietojen käsittelijä käsittelee tietoja ainoastaan rekisterinpitäjän kirjallisten ohjeiden mukaisesti.

Yksilön oikeuksia suojaavat velvoitteet

Yleisessä tietosuoja-asetuksessa on joukko velvoitteita, joiden tarkoituksena on suojella yksilön oikeuksia hallita omia henkilötietojaan.

Yrityksiä koskeva velvoite: avoin tiedottaminen

Yritysten on annettava yksilöille tietoa siitä, kuka tietoja käsittelee, mitä tietoja käsitellään ja miksi. Vähintään seuraavat tiedot on ilmoitettava selkeästi:

- yrityksen tiedot
- tietojenkäsittelyn tarkoitus
- tietojenkäsittelyn oikeusperusta
- kenelle tiedot (mahdollisesti) välitetään

Joissakin tapauksissa on annettava myös seuraavat tiedot:

- tietosuojavastaavan yhteystiedot
- oikeutettu etu (jos oikeutettu etu on käsittelyn oikeudellinen peruste)
- peruste tietojen siirtämisellä EU:n ulkopuoliseen maahan
- tietojen säilytysaika
- yksilön tietosuojaoikeudet (mm. oikeus saada pääsy tietoihin, pyytää tietojen oikaisemista tai poistamista, rajoittaa tai vastustaa käsittelyä taikka siirtää tiedot)
- miten suostumuksen voi peruuttaa (jos suostumus on käsittelyn oikeudellinen peruste)
- onko tietojen antamiselle lakisääteinen tai sopimukseen perustuva velvoite
- automaattisen päätöksenteon yhteydessä tietoa päätöksentekoprosessiin liittyvästä logiikasta sekä päätöksen merkityksestä ja seurauksista.

”Yritysten on annettava yksilöille tietoa siitä, kuka tietoja käsittelee, mitä tietoja käsitellään ja miksi.”

Yrityksiä koskeva velvoite: oikeus saada pääsy tietoihin ja oikeus siirtää tiedot

Yksilöillä on oikeus pyytää saada pääsy omiin henkilötietoihinsa maksutta ja helposti saatavilla olevassa muodossa. Jos yrityksesi saa tällaisen pyynnön, sen pitää

- kertoa yksilölle, käsitteleekö yrityksesi häntä koskevia henkilötietoja
- antaa tietoa käsittelystä (mm. käsittelyn tarkoitus, käsitellyt henkilötietoluokat, tietojen vastaanottajat)
- toimittaa henkilölle jäljennös käsitellyistä henkilötiedoista.

Jos käsittely perustuu suostumukseen tai sopimukseen, yksilöllä on oikeus pyytää henkilötietojen palauttamista tai siirtämistä toiselle yritykselle. Tätä kutsutaan oikeudeksi siirtää tiedot. Tiedot pitää toimittaa yleisesti käytetyssä ja koneluettavassa muodossa.

Vaikka nämä kaksi oikeutta liittyvät läheisesti toisiinsa, ne ovat erillisiä oikeuksia. Niitä ei saa siten sekoittaa toisiinsa, ja yksilölle annettavat tiedot määräytyvät kyseessä olevan oikeuden mukaan.

Yrityksiä koskeva velvoite: oikeus pyytää tietojen poistamista (oikeus tulla unohdetuksi)

Joissakin tapauksissa yksilö voi pyytää rekisterinpitäjää poistamaan henkilötiedot, jos esimerkiksi tietoja ei enää tarvita käsittelytarkoituksen täyttämiseen. Yritys ei ole kuitenkaan velvollinen täyttämään yksilön pyyntöä seuraavissa tapauksissa:

- Käsittely on välttämätöntä sananvapauden ja tiedonsaantioikeuden kunnioittamiseksi.
- Henkilötietojen säilyttämiselle on lakisääteinen velvoite.
- Henkilötietojen säilyttämiseen on muita yleiseen etuun liittyviä syitä, kuten kansanterveyteen tai tieteelliseen ja historialliseen tutkimukseen liittyvät syyt.
- Henkilötietoja säilytetään oikeudellisen vaateen laatimiseksi.

Yrityksiä koskeva velvoite: oikeus pyytää tietojen oikaisemista ja oikeus vastustaa käsittelyä

Jos yksilö uskoo henkilötietojensa olevan virheellisiä, puutteellisia tai epätarkkoja, hän voi pyytää yritystä korjaamaan tiedot tai täydentämään niitä ilman aiheetonta viivytystä.

Yksilöllä on myös oikeus milloin tahansa vastustaa henkilötietojensa käsittelyä tiettyihin tarkoituksiin, jos yritys käsittelee tietoja oikeutetun edun tai yleisen edun vuoksi toteutettavan tehtävän suorittamiseksi. Jos yrityksesi oikeutettu etu ei syrjäytä yksilön etua, henkilötietojen käsittely on lopetettava. Myös silloin, jos yksilö pyytää tietojenkäsittelyn rajoittamista, on otettava huomioon, syrjäyttääkö yrityksen oikeutettu etu yksilön edun. Suoramarkkinoinnin yhteydessä yritys on kuitenkin aina velvollinen lopettamaan henkilötietojen käsittelyn yksilön pyynnöstä.

Automaattinen päätöksenteko ja profilointi

Yksilöllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen tietojenkäsittelyyn. Säännöstä kuitenkin poiketaan esimerkiksi silloin, jos yksilö on antanut nimenomaisen suostumuksensa automaattiselle päätöksenteolle. Jos automaattinen päätöksenteko ei perustu lainsäädäntöön, yrityksen pitää

- ilmoittaa yksilölle, että päätös tehdään automaattisesti
- antaa yksilölle oikeus tarkistuttaa automaattinen päätös ihmisellä
- antaa yksilölle mahdollisuus riitauttaa automaattinen päätös.

Jos pankki esimerkiksi käyttää tietyn yksilön lainahakemuksen käsittelyssä automaattista päätöksentekoa, yksilölle pitää ilmoittaa, että päätös tehdään automaattisesti, ja hänelle on annettava mahdollisuus riitauttaa päätös ja pyytää päätöksen tarkistuttamista ihmisellä.

Riskiin perustuvat velvoitteet

Yleisessä tietosuoja-asetuksessa on yksilöiden oikeuksia suojaavien velvoitteiden lisäksi joukko velvoitteita, jotka perustuvat käsittelyn aiheuttamaan riskiin.

Yrityksiä koskeva velvoite: tietosuojavastaavan nimittäminen

Tietosuojavastaava valvoo, että yritys noudattaa yleistä tietosuoja-asetusta. Yksi tietosuojavastaavan tärkeimmistä tehtävistä on tiedottaa henkilötietojen käsittelystä vastaaville työntekijöille näitä koskevista velvoitteista. Tietosuojavastaava tekee myös yhteistyötä tietosuojaviranomaisen kanssa sekä toimii tietosuojaviranomaisen ja yksilöiden välisenä yhteyshenkilönä.

Yrityksesi pitää nimittää tietosuojavastaava seuraavissa tapauksissa:

- yritys seuraa yksilöitä säännöllisesti ja järjestelmällisesti tai käsittelee tiettyjä tietoluokkia
- kyseinen käsittely on osa yrityksen ydinliiketoimintaa tai
- käsittelyä tehdään laajassa mittakaavassa.

Jos yritys esimerkiksi käsittelee henkilötietoja kohdentaakseen mainontaa hakukoneiden kautta ihmisten verkkokäyttäytymisen perusteella, yleinen tietosuoja-asetus velvoittaa yrityksen nimittämään tietosuojavastaavan. Jos yritys taas lähettää asiakkailleen mainosmateriaalia kerran vuodessa, tietosuojavastaavaa ei tarvitse nimittää. Samoin jos olet lääkäri, joka kerää potilaiden terveystietoja, tietosuojavastaavaa ei todennäköisesti tarvitse nimittää. Jos kuitenkin käsittelet genetiikkaa tai terveyttä koskevia henkilötietoja sairaalan puolesta, tietosuojavastaavaa tarvitaan.

Yrityksiä koskeva velvoite: sisäänrakennettu ja oletusarvoinen tietosuoja

Yleisessä tietosuoja-asetuksessa esitellään kaksi uutta periaatetta: sisäänrakennettu ja oletusarvoinen tietosuoja.

Sisäänrakennetun tietosuojan avulla varmistetaan, että yritys ottaa tietosuojan huomioon jo varhaisessa vaiheessa, kun henkilötietojen uusia käsittelytapoja suunnitellaan. Tämän periaatteen mukaisesti rekisterinpitäjän pitää ryhtyä kaikkiin teknisiin ja organisatorisiin toimiin tietosuojaperiaatteiden noudattamiseksi ja yksilöiden oikeuksien suojelemiseksi. Näihin toimiin kuuluu muun muassa tietojen pseudonymisointi.

Sisäänrakennettu tietosuoja minimoi yksityisyyteen kohdistuvat riskit ja lisää luottamusta. Kun tietosuoja otetaan huomioon jo uusien tuotteiden tai palvelujen kehittämisen aikana, voidaan mahdolliset tietosuojaongelmat välttää jo varhaisessa vaiheessa. Käytäntö auttaa myös lisäämään tietoisuutta tietosuojasta yrityksen kaikilla osastoilla ja tasoilla.

Oletusarvoisen tietosuojan avulla varmistetaan, että yritys käyttää aina yksityisyyttä parhaiten suojaavia oletusasetuksia. Jos on esimerkiksi mahdollista käyttää kahta eri yksityisyysasetusta, joista toinen estää henkilötietojen luvattoman käytön, yrityksen olisi valittava kyseinen asetus.

”Sisäänrakennettu tietosuoja minimoi yksityisyyteen kohdistuvat riskit ja lisää luottamusta.”

”Oletusarvoisen tietosuojan avulla varmistetaan, että yritys käyttää aina yksityisyyttä parhaiten suojaavia oletusasetuksia.”

Yrityksiä koskeva velvoite: asianmukainen tiedotus tietoturvaloukkauksen sattuessa

Tietoturvaloukkauksesta on kyse silloin, jos yrityksen vastuulla olevat henkilötiedot vuotavat vahingossa tai laittomasti luvattomille vastaanottajille, jos ne eivät ole väliaikaisesti saatavilla tai jos ne muuttuvat.

On tärkeää, että yrityksellä on käytössä asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla tietoturvaloukkaukset vältetään. Jos tietoturvaloukkaus kuitenkin tapahtuu ja asettaa yksilön oikeudet ja vapaudet vaaraan, yrityksen on ilmoitettava asiasta tietosuojaviranomaiselle viimeistään 72 tunnin sisällä tietoturvaloukkauksen havaitsemisesta.

Jos tietoturvaloukkaus aiheuttaa korkean riskin yksilöille, joiden tietoja se koskee, yrityksen on mahdollisesti ilmoitettava asiasta myös heille.

Tietojen siirtäminen EU:n ulkopuolelle

Yleistä tietosuoja-asetusta sovelletaan Euroopan talousalueella (ETA), johon kuuluvat EU-maiden lisäksi Islanti, Liechtenstein ja Norja. Kun henkilötietoja siirretään ETA-alueen ulkopuolelle, yleisen tietosuoja-asetuksen suoja siirtyy tietojen mukana. Yritysten on siten tietoja ulkomaille siirtäessään varmistettava, että käytössä on tiettyjä suojatoimia.

Yleinen tietosuoja-asetus tarjoaa erilaisia mekanismeja tietojen siirtämiseen kolmansiin maihin. Asetuksen mukaan siirtäminen on sallittua seuraavissa tapauksissa:

1. maan tietosuoja on EU:n mukaan riittävä
2. yritys ryhtyy tarvittaviin toimiin varmistaakseen asianmukaisen tietosuojan esimerkiksi sisällyttämällä henkilötietojen EU:n ulkopuolisen maahantuojan kanssa tekemäänsä sopimukseen tiettyjä lausekkeita tai
3. yrityksellä on siirtämiselle erityiset perusteet (ns. ”poikkeukset”), kuten yksilön suostumus.

Lisätietoja kansainvälisistä tiedonsiirroista saa Euroopan komission tiedonannosta ”Henkilötietojen vaihtaminen ja suojaaminen globalisoituneessa maailmassa”: http://eur-lex.europa.eu/legal-content/fi/TXT/HTML/?uri=CELEX:52017DC0007&from=fi

Milloin täytyy tehdä tietosuojaa koskeva vaikutustenarviointi?

Tietosuojaa koskeva vaikutustenarviointi on tehtävä silloin, kun suunniteltu käsittely aiheuttaa yksilöiden oikeuksiin ja vapauksiin kohdistuvan korkean riskin. Näin voi olla esimerkiksi silloin, jos käytetään uutta teknologiaa.

Yleisen tietosuoja-asetuksen mukaan kyse on korkeasta riskistä ainakin seuraavissa tapauksissa:

- automaattisen käsittelyn ja profilointimekanismien järjestelmällinen ja kattava käyttö yksilöiden arvioimisessa
- julkisen alueen järjestelmällinen ja laaja-alainen valvonta (esim. videovalvonta)
- arkaluonteisten tietojen (esim. terveystietojen) käsittely laajassa mittakaavassa.

Tietosuojaa koskevan vaikutustenarvioinnin tarkoituksena on tunnistaa yksilöiden oikeuksiin ja vapauksiin mahdollisesti kohdistuvat riskit ennen kuin henkilötietojen käsittely alkaa ja riski toteutuu. Riskien pienentäminen etukäteen auttaa välttämään vahingot ja minimoimaan kustannukset.

Jos tietosuojaa koskevassa vaikutustenarvioinnissa määritellyillä toimilla ei onnistuta poistamaan kaikkia tunnistettuja riskejä, pitää ennen tietojen käsittelyä ottaa yhteyttä tietosuojaviranomaiseen.

”Tietosuojaa koskeva vaikutustenarviointi on tehtävä silloin, kun suunniteltu käsittely aiheuttaa yksilöiden oikeuksiin ja vapauksiin kohdistuvan korkean riskin.”

Mitä yrityksen pitää tehdä?

Pyyntöihin vastaaminen

Jos yrityksesi vastaanottaa yksilöltä oikeuksien käyttämistä koskevan pyynnön, siihen pitää vastata ilman aiheetonta viivytystä ja joka tapauksessa yhden kuukauden kuluessa sen vastaanottamisesta. Määräaikaa voidaan kuitenkin jatkaa kahdella kuukaudella, jos pyynnöt ovat monimutkaisia tai niitä on useita, kunhan yksilölle ilmoitetaan asiasta. Pyynnöt on käsiteltävä **maksutta**. Jos pyyntöä ei voida toteuttaa, asiasta on ilmoitettava kyseiselle henkilölle perusteluineen. Hänelle on myös ilmoitettava oikeudesta tehdä valitus tietosuojaviranomaiselle.

Vaatimustenmukaisuuden osoittaminen ja rekisterinpito

Yksi yleisen tietosuoja-asetuksen perusperiaatteita on varmistaa, että yritykset voivat osoittaa noudattavansa vaatimuksia. Yrityksen on siten pystyttävä todistamaan, että se toimii yleisen tietosuoja-asetuksen mukaisesti ja täyttää kaikki sovellettavat velvoitteet – erityisesti tietosuojaviranomaisen pyynnöstä tai tämän tehdessä tarkastuksen.

Vaatimustenmukaisuus voidaan osoittaa pitämällä rekisteriä muun muassa seuraavista tiedoista:

- tietojenkäsittelystä vastaavan yrityksen nimi ja yhteystiedot
- henkilötietojen käsittelyn syy(t)
- kuvaus ihmisryhmistä, joiden henkilötietoja käsitellään
- henkilötietoja vastaanottavien organisaatioiden ryhmät
- tietojen siirtäminen toiseen maahan tai organisaatioon
- henkilötietojen säilytysaika
- kuvaus henkilötietojen käsittelyn yhteydessä käytettävistä turvatoimista.

Yrityksen pitäisi lisäksi laatia työntekijöilleen tietojenkäsittelyä koskevat kirjalliset käytännöt ja ohjeet sekä päivittää ne säännöllisesti.

LUKU 4

ONKO YRITYKSESI VALMIS TÄYTTÄMÄÄN VAATIMUKSET?

Yleisen tietosuoja-asetuksen mukaan yrityksillä on vastuu henkilötietojen käsittelyyn liittyvissä asioissa. Ensimmäiseksi yritysten on kartoitettava nykyiset tietojenkäsittelytoimet ja arvioitava sisäiset liiketoimintaprosessinsa. Yrityksen pitää erityisesti

- määritellä, millaisia tietoja se säilyttää, mihin tarkoitukseen niitä säilytetään ja mikä on säilytyksen oikeusperusta
- arvioida kaikki voimassa olevat sopimukset ja erityisesti rekisterinpitäjien ja henkilötietojen käsittelijöiden väliset sopimukset
- arvioida kaikki mahdolliset tapaukset, joissa tietoja siirretään kansainvälisesti, ja
- arvioida yrityksen yleinen hallinto (mm. käytössä olevat tietojärjestelmät ja organisatoriset menettelyt) ja se, pitääkö yrityksen nimittää tietosuojavastaava tai haluaako yritys nimittää sellaisen.

Olennainen osa prosessia on varmistaa, että yrityksen ylin johto osallistuu kyseiseen arviointityöhön, antaa panoksensa tietosuojapolitiikan laadintaan sekä saa säännöllisesti tietoa sen muutoksista ja voi ottaa niihin kantaa.

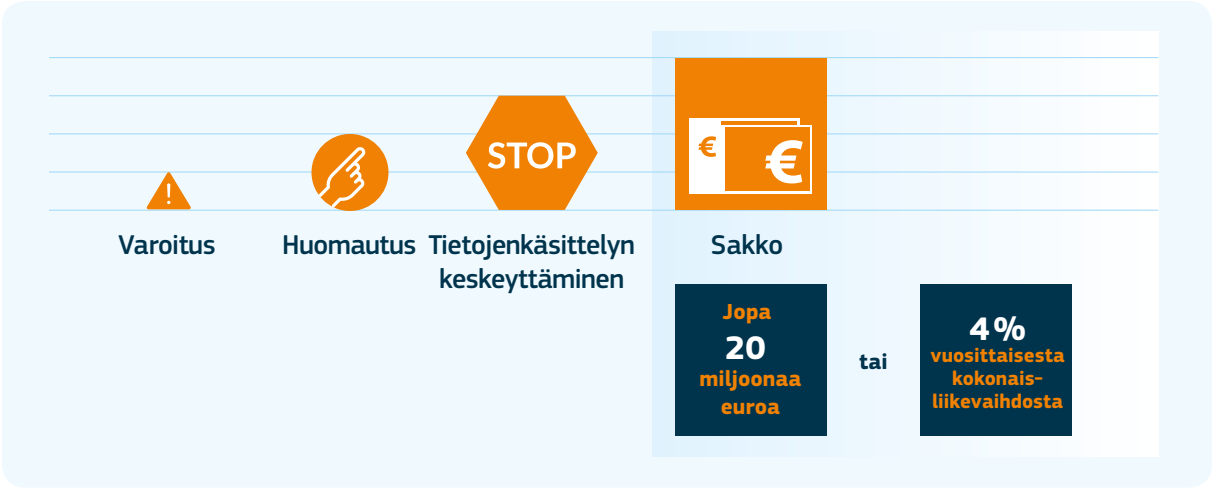
Käsitteleekö yrityksesi tietoja useissa maissa?

Rajat ylittävän tietojenkäsittelyn tapauksessa toimivaltainen viranomainen voi olla oman maasi tietosuojaviranomaisen sijasta käsittelymaan valvontaviranomainen. EU:ssa toimivaltainen viranomainen on yleensä sen maan tietosuojaviranomainen, jossa yrityksen päätoimipaikka sijaitsee (jossa päätökset käsittelytavasta ja käsittelytarkoituksista tehdään).

Noudattamatta jättämisen riskit

Yleisen tietosuoja-asetuksen noudattamatta jättämisestä voidaan määrätä huomattavia sakkoja – tietyistä rikkomuksista jopa 20 miljoonaa euroa tai neljä prosenttia yrityksen kokonaisliikevaihdosta. Tietosuojaviranomainen voi myös määrätä muita korjaavia toimenpiteitä, kuten kieltää henkilötietojen käsittelyn. Yritysten on myös huomioitava noudattamatta jättämisen mahdolliset vaikutukset yritysten maineeseen.

Yleisen tietosuoja-asetuksen noudattamatta jättämisen kustannukset ovat selkeästi suuremmat kuin sen noudattamisen edellyttämät investoinnit.



Jos sinulla on kysyttävää tai huolenaiheita, ota yhteyttä kansalliseen tietosuojaviranomaiseen.

Löydä oman maasi tietosuojaviranomainen verkosta:

http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

TÄRKEÄ TIEDOTE

Tässä esitteessä annettujen tietojen ja ohjeiden tarkoituksena on edistää EU:n tietosuojasääntöjen tuntemusta.

Tarkoituksena on ainoastaan antaa ohjeita, ja vain yleisen tietosuoja-asetuksen tekstillä on oikeudellista merkitystä. Näin ollen vain asetuksella voidaan luoda oikeuksia ja määrätä velvollisuuksia luonnollisille henkilöille. Ohjeilla ei luoda täytäntöönpanokelpoisia oikeuksia tai odotuksia.

EU-lainsäädännön sitova tulkinta kuuluu yksinomaan Euroopan unionin tuomioistuimen toimivaltaan. Ohjeissa esitetyt näkemykset eivät ennakoi komission mahdollista kantaa unionin tuomioistuimessa.

Euroopan komissio tai kukaan sen puolesta toimiva henkilö ei ole vastuussa esitteen tietojen mahdollisesta käytöstä.

Esite heijastelee sen laadintahetkellä vallitsevaa tilannetta, ja sen sisältöön voidaan tehdä parannuksia tai muutoksia ilman ennakkoilmoitusta.

Yhteydenotot EU:hun

Käynti tiedotuspisteessä

Euroopan unionin alueella toimii yhteensä satoja Europe Direct -tiedotuspisteitä.
Lähimmän tiedotuspisteen osoite löytyy verkosta: https://europa.eu/european-union/contact_fi

Yhteydenotot puhelimitse tai sähköpostitse

Europe Direct -palvelu vastaa Euroopan unionia koskeviin kysymyksiin. Palveluun voi ottaa yhteyttä
– soittamalla maksuttomaan palvelunumeroon 00 800 678 910 11 (jotkin operaattorit voivat periä puhelumaksun),
– soittamalla puhelinnumeroon +32 22999696 tai
– sähköpostitse: https://europa.eu/european-union/contact_fi.

Tietoa EU:sta

Verkkosivut

Tietoa Euroopan unionista on saatavilla kaikilla EU:n virallisilla kielillä Europa-sivustolla, https://europa.eu/european-union/index_fi.

EU:n julkaisut

EU:n ilmaisia ja maksullisia julkaisuja voi ladata tai tilata EU Bookshopista, osoitteesta https://publications.europa.eu/bookshop. Ilmaisia julkaisuja on mahdollista saada usean kappaleen erinä ottamalla yhteyttä Europe Direct -palveluun tai paikalliseen tiedotuspisteeseen (ks. https://europa.eu/european-union/contact_fi).

EU:n lainsäädäntö ja siihen liittyvät asiakirjat

EU:n koko lainsäädäntö vuodesta 1952 ja muuta tietoa EU:n oikeudesta on saatavilla kaikilla virallisilla kielillä EUR-Lex-tietokannassa osoitteessa http://eur-lex.europa.eu.

EU:n avoin data

EU:n avoimen datan portaalin (http://data.europa.eu/euodp/fi) kautta on saatavilla EU:n data-aineistoja. Data on ilmaiseksi ladattavissa ja uudelleenkäytettävissä sekä kaupallista että ei-kaupallista käyttöä varten.

DS-01-18-082-FI-C

Yleisellä tietosuoja-asetuksella säädellään yritysten tapaa käsitellä ja hallita henkilötietoja. Yhden yhteisen eurooppalaisen tietosuojalain ansiosta yritykset voivat tarjota tuotteita ja palveluja koko EU:ssa noudattaen ensisijaisesti vain yhtä tietosuojalakia.

Yleinen tietosuoja-asetus yksinkertaistaa yritysten sääntely-ympäristöä ja tarjoaa niille mahdollisuuden parantaa henkilötietojen hallintaa ja siten lisätä kuluttajan luottamusta yrityksiä kohtaan.

Esitteessä kuvaillaan yrityksille yleisen tietosuoja-asetuksen mukaisesti kuuluvat velvoitteet.

europa.eu/dataprotection/fi

Julkaisutoimisto

ISBN 978-92-79-79410-0