

YRITTÄJÄN TIETOSUOJAOPAS

SISÄLLYSLUETTELO

1. JOHDANTO	3	5. ERITYISET HENKILÖTIETORYHMÄT ELI ARKALUONTEISET TIEDOT	12	13. TIETOJEN SIIRTÄMINEN EU:N ULKOPUOLELLE	29
2. SANASTO	4	6. REKISTERÖITYJEN OIKEUDET	14	14. TIETOSUOJAVASTAAVA	31
Henkilötieto	4	Oikeus saada tietoa henkilötietojen		Tietosuojavastaavan nimittäminen	31
Henkilötietojen käsittely	4	käsittelystä	15	Tietosuojavastaavan asema ja tehtävät	32
Rekisteri	5	Oikeus tietojen oikaisemiseen	16	15. KÄSITTELYN TURVALLISUUS	34
Rekisterinpitäjä	5	Oikeus tulla unohdetuksi	16	Vaikutustenarviointi	34
Rekisteröity	5	Oikeus siirtää tiedot järjestelmästä toiseen	17	16. TIETOTURVALOUKKAUKSET	35
Henkilötietojen käsittelijä	5	Oikeus rajoittaa tietojen käsittelyä	17	Tietosuojaloukkauksesta ilmoittaminen	
Profilointi	5	Oikeus vastustaa käsittelyä	18	valvontaviranomaiselle	35
Anonymisointi	6	Oikeus olla joutumatta		Tietosuojaloukkauksesta ilmoittaminen	
Pseudonymisointi	6	profiloinnin kohteeksi	18	rekisteröidylle	36
Suostumus	6	7. KUN TIETOJA KERÄTÄÄN REKISTERÖIDYLTÄ	20	17. SANKTIOT JA SAKOT	37
Tietoturvaloukkaus	6	8. KUN TIETOJA EI OLE SAATU REKISTERÖIDYLTÄ ITSELTÄÄN	22	Rikkomuksista hallinnollisia sakkoja	37
Geneettiset tiedot	7	9. HENKILÖTIETOJEN KÄYTTÖ MUUHUN TARKOITUKSEEN	23	18. KÄYTÄNNÖN TOIMENPITEITÄ YRITTÄJILLE	38
Biometriset tiedot	7	10. SELOSTE KÄSITTELYTOIMISTA	24		
Henkilötietoryhmä	7	11. SUORAMARKKINOINTI	25		
Erityiset henkilötietoryhmät	7	Perinteinen suoramarkkinointi	25		
Valvontaviranomainen	7	Ulkoistettu suoramarkkinointi	25		
3. HENKILÖTIETOJEN KÄSITTELYN PERIAATTEET	8	Sähköinen suoramarkkinointi	26		
4. KUUSI SYYTÄ HENKILÖTIETOJEN KÄSITTELYYN	9	12. TIETOJENKÄSITTELYN ULKOISTAMINEN	27		
Suostumus	10	Tietojenkäsittelysopimuksessa tulisi			
Oikeutettu etu	10	sopia vähintään seuraavista asioista	27		
Suoramarkkinointi	10				
Sopimus	11				
Lakisääteinen velvoite	11				
Elintärkeä etu	11				
Julkinen tehtävä	11				

1. JOHDANTO

Tietosuoja-asetus tulee voimaan toukokuussa 2018. Siitä alkaen henkilötietojen käsittelyn on oltava tietosuoja-asetuksen mukaista. Tämä ohje auttaa yrittäjiä toimimaan uuden tietosuojalain mukaisesti.

Tietosuoja-asetuksesta (jäljempänä "tietosuoja-asetus" tai "asetus") käytetään myös nimitystä GDPR eli General Data Protection Regulation. Sen tarkoituksena on ajantasaistaa tietosuojan sääntelyä. Teknologia on kehittynyt niin paljon, että tietosuojasta huolehtimiseen tarvitaan uudenlaista sääntelyä.

Tietosuoja-asetuksen tavoitteena on, että kansalaiset voivat hallita tietojaan paremmin. Asetus sääntelee mm. henkilötietojen keräämistä, käsittelyä ja luovuttamista sekä näihin liittyviä oikeuksia ja velvollisuuksia. Lähes kaikki yritykset käsittelevät toiminnassaan henkilötietoja. Säännöt ovat samat kaikille EU:ssa toimiville yrityksille kotipaikasta riippumatta.

Asetusta täydentää työelämän tietosuojalaki, jonka yhteensopivuutta tietosuoja-asetukseen arvioi työ- ja elinkeinoministeriön asettama työryhmä. Arvio annetaan keväällä 2018.

Omat muistiinpanot:



**Tietosuojaoppaan on
laatinut asiantuntija,
varatuomari
Petri Holopainen,
Suomen Yrittäjät.**

**VOIT LIITTYÄ
SUOMEN YRITTÄJIEN
JÄSENEKSI TÄÄLLÄ:
www.yrittajat.fi/liity**

2. SANASTO

Henkilötieto

Henkilötiedolla tarkoitetaan luonnollista henkilöä (jäljempänä "rekisteröity") tai hänen ominaisuuksiaan kuvaavia tietoja. Lisäksi sillä tarkoitetaan rekisteröidyn elinolosuhteita kuvaavia merkintöjä, jotka voidaan yhdistää häneen, hänen perheeseensä tai hänen kanssaan yhteisessä taloudessa eläviin henkilöihin.

Kyse voi olla esimerkiksi asiakkaiden, työntekijöiden tai yrityskontaktien henkilötiedoista, kuten nimestä, osoitteesta, puhelinnumerosta tai mistä tahansa muusta tiedosta, jonka voi liittää tiettyyn henkilöön.

Henkilötietojen käsittely

Henkilötietojen käsittelyllä tarkoitetaan henkilötietojen

- keräämistä
- tallentamista
- järjestämistä
- jäsentämistä
- säilyttämistä
- muokkaamista tai muuttamista
- hakemista (esim. tietokannasta)
- kyselyä (esim. etsi sivulta -tyyppinen haku)
- käyttämistä

Henkilötietojen käsittelyä on myös tietojen luovuttaminen

- ▶ levittämällä
- ▶ asettamalla ne muutoin saataville.

Käsittely tarkoittaa myös tietojen

- käytön rajoittamista.

Omat muistiinpanot:

[illegible]

JATKUU SEURAAVALLA SIVULLA 

Rekisteri

Rekisterillä tarkoitetaan mitä tahansa henkilötietoja sisältävää jäsenneltyä tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein. Tietojoukko voi olla keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu. Tämä tarkoittaa sitä, että rekisterissä olevan tiedon ei fyysisesti tarvitse olla samassa paikassa, vaan henkilötiedot voivat olla myös hajallaan esimerkiksi eri tietokoneilla ja eri maissa. Teknisesti rekisteri voi olla esimerkiksi paperinen rekisteri, Excel-tiedosto tai asiakastietojen hallintaan käytetty ohjelmisto.

Rekisterinpitäjä

Rekisterinpitäjä on yritys, joka säilyttää henkilötietoja ja jolla on oikeus määrätä henkilörekisterin käytöstä.

Rekisteröity

Rekisteröity tarkoittaa henkilöä, jonka tietoja on tallennettu rekisteriin.

Henkilötietojen käsittelijä

- ▶ itsenäinen elinkeinon- tai toiminnanharjoittaja, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Henkilötietojen käsittelijä on itsenäinen elinkeinon- tai toiminnanharjoittaja, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Tällaisesta on kysymys esimerkiksi silloin, kun yritys siirtää työntekijätietoja palkanmaksusta vastaavalle tilitoimistolle. Tällöin henkilötietojen katsotaan siirtyvän henkilötietojen käsittelijälle eli sille palveluntarjoajalle, joka käsittelee henkilötietoja rekisterinpitäjän puolesta.

Profilointi

Profiloinnilla tarkoitetaan mitä tahansa henkilötietojen automaattista käsittelyä, jossa henkilötietoja käyttämällä arvioidaan luonnollisen henkilön tiettyjä henkilökohtaisia ominaisuuksia. Profiloinnista puhutaan erityisesti, kun analysoidaan tai ennakoitetaan piirteitä, jotka liittyvät henkilön työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksenkohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkumiseen.

Omat muistiinpanot:

JATKUU SEURAAVALLA SIVULLA ➔

Anonymisointi

Anonymisointi tarkoittaa henkilötiedon tunnistettavuuden muuttamista siten, että sitä ei voida enää yhdistää rekisteröityyn. Anonymisoidut tiedot eivät ole henkilötietoja.

Pseudonymisointi

Pseudonymisoinnilla tarkoitetaan henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää suoraan tiettyyn rekisteröityyn eli rekisterissä olevaan henkilöön.

Yhdistäminen voi olla mahdollista lisätietojen avulla, mutta lisätiedot on säilytettävä erillään varsinaisesta rekisteristä. Teknisillä ja organisatorisilla keinoilla pitää varmistaa, ettei rekisterin tietoja voi yhdistää tunnistettuun tai tunnistettavissa olevaan henkilöön. Tekninen keino voi olla esimerkiksi ohjelmiston käyttö, kun ohjelmiston avulla varmistetaan, ettei tietoja voi yhdistää. Organisaatorisilla keinoilla tarkoitetaan työolojen tai työtehtävien järjestelyä siten, ettei henkilötietoja päästä yhdistämään.

Suostumus

Rekisteröidyn suostumuksella tarkoitetaan mitä tahansa vapaaehtoista, yksilöityä, tietoista ja yksiselitteistä tahdonilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn. Tahdonilmaisuu voi esimerkiksi olla se, että rekisteröity rastittaa ruudun vieraillessaan internetsivustolla tai täyttäessään paperilomaketta.

Tietoturvaloukkaus

Henkilötietojen tietoturvaloukkauksella tarkoitetaan sellaista tapahtumaa, jonka seurauksena siirrettyjä, tallennettuja tai muuten käsiteltyjä henkilötietoja vahingossa tai lainvastaisesti tuhoutuu, häviää tai muuttuu. Tietoturvaloukkaukseksi katsotaan myös tietojen luvaton luovuttaminen sekä luvaton pääsy tietoihin.

Omat muistiinpanot:

JATKUU SEURAAVALLA SIVULLA ➔

Geneettiset tiedot

Geneettisillä tiedoilla tarkoitetaan henkilötietoja, jotka koskevat henkilön perittyjä tai hankittuja geneettisiä ominaisuuksia. Geneettisistä tiedoista selviää yksilöllistä tietoa henkilön fysiologiasta tai terveydentilasta. Geneettiset tiedot saadaan biologisesta näytteestä analysoimalla.

Biometriset tiedot

Biometrisillä tiedoilla tarkoitetaan kaikkia luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyviä teknisellä käsittelyllä saatuja henkilötietoja, joiden perusteella kyseinen luonnollinen henkilö voidaan tunnistaa tai tunnistaminen voidaan varmistaa. Biometrisiä tietoja ovat esimerkiksi kasvokuvat ja sormenjäljet.

Henkilötietoryhmä

Henkilötietoryhmällä tarkoitetaan tiettyä samankaltaista tietojoukkoa. Tällaisia ovat esimerkiksi työntekijöitä koskevat tiedot tai asiakkaita koskevat tiedot.

Erityiset henkilötietoryhmät

Tietosuojalaissa termillä erityiset henkilötietoryhmät tarkoitetaan arkaluonteisia tietoja, joista ilmenee

- | | |
|--|--|
| ➤ rotu tai etninen alkuperä | ➤ terveydentila |
| ➤ poliittinen mielipide | ➤ seksuaalinen käyttäytyminen ja suuntautuminen |
| ➤ uskonnollinen tai filosofinen vakaumus | ➤ geneettinen tai biometrinen informaatio, josta henkilön voi tunnistaa. |
| ➤ ammattiliiton jäsenyys | |

Valvontaviranomainen

Valvontaviranomainen valvoo lain noudattamista. Tämän ohjeen kirjoittamishetkellä tietosuojalain valvontaviranomainen on tietosuojavaltuutetun toimisto. Viranomainen saattaa vaihtua tulevaisuudessa tai sen nimi saattaa muuttua.

Omat muistiinpanot:

4. KUUSI SYYTÄ HENKILÖTIETOJEN KÄSITTELYYN

Tietosuoja-asetuksessa määritellään kuusi syytä, joiden perusteella henkilötietoja saa laillisesti käsitellä. Vähintään yhden näistä kuudesta edellytyksestä tulee täytyä:

1.	suostumus
2.	oikeutettu etu
3.	sopimus
4.	lakisääteinen velvoite
5.	elintärkeä tai yleinen etu
6.	julkinen tehtävä

 Katso tietosuoja-asetuksen artikla 6.

Omat muistiinpanot:

JATKUU SEURAAVALLA SIVULLA 

Suostumus

Suostumus tarkoittaa, että rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten. Rekisterinpitäjän tulee dokumentoida saatu suostumus, koska se pitää pystyä todentamaan. Suostumus tulee antaa tarkoituksellisesti, eli sitä ei voi antaa vaikenemalla, valmiiksi rastitetuilla ruuduilla tai jättämällä jotakin tekemättä.

Lasten tietojen käsittely

Tietosuoja-asetus antaa erityistä suojaa lasten henkilötiedoille. Se poikkeaa siten henkilötietolain määräyksistä. Tietoyhteiskunnan palvelujen tarjoaminen suoraan lapselle on sallittu ainoastaan, jos lapsi on vähintään 16-vuotias. Alle 16-vuotiaan lapsen henkilötietoja saa käsitellä vain huoltajan suostumuksella.

Tietoyhteiskunnan palvelut tarkoittavat etänä, sähköisesti, pyynnöstä ja vastiketta vastaan tarjottavia palveluja. Katso tietosuoja-asetuksen artikkelit 7 ja 8.

Oikeutettu etu

Henkilötietojen käsittelyn perusteena voi olla oikeutettu etu. Tämä tarkoittaa sitä, että rekisterinpitäjän ja rekisteröidyn välillä on asianmukainen ja merkityksellinen suhde, kuten jäsenyys, asiakkuus tai työsuhde.

Oikeutettuja etuja arvioitaessa tulee ottaa huomioon rekisteröidyn perusoikeudet ja vapaudet, jotka saattavat syrjäyttää tällaiset edut, erityisesti silloin, jos rekisteröity on lapsi. Tällöin lapsesta kerättyjä tietoja ei saa käyttää laajempaan tarkoitukseen kuin voidaan katsoa käyttötarkoituksen perusteella tarpeelliseksi.

Suoramarkkinointia voi tehdä oikeutetun edun perusteella. EU:ssa valmistellaan sähköisen viestinnän tietosuoja-asetusta, jossa säädellään evästeiden käytöstä ja sähköisestä suoramarkkinoinnista. Ennen tämän uuden asetuksen tuloa tietoyhteiskuntakaareissa säännellään sähköisestä suoramarkkinoinnista, ja tähän vaaditaan suostumus etukäteen. Suoramarkkinointia harjoittavien yritysten kannattaa siis seurata lainsäädännön kehitystä. Suoramarkkinoinnista kerrotaan lisää luvussa 11.

Omat muistiinpanot:

JATKUU SEURAAVALLA SIVULLA ➔

Sopimus

Henkilötietojen käsittely on lainmukaista, kun se on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena.

Henkilötiedon käsittely sopimuksen täytäntöön panemiseksi tarkoittaa käytännössä esimerkiksi lehtiyhtiölle annetun osoitteen käyttämistä, jotta lehti voidaan toimittaa rekisteröidylle.

Lakisääteinen velvoite

Henkilötietojen käsittely on sallittua, kun se on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Tällöin ei tarvita erikseen rekisteröidyn suostumusta. Lakisääteinen velvoite on kyseessä myös silloin, kun työnantaja ilmoittaa työntekijöiden palkkatiedot veroviranomaisille.

Esimerkiksi osakeyhtiön on osakeyhtiölain perusteella pidettävä osakasluettelo, jolloin tätä koskevien henkilötietojen käsittely on tarpeen.

Elintärkeä tai yleinen etu

Henkilötietoja voidaan käsitellä silloin, kun käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi. Tällainen tarkoitus voi olla esimerkiksi ihmishenkien suojeleminen luonnonkatastrofin yhteydessä. Yritys voi käsitellä henkilötietoja varoitukseen ihmisiä esimerkiksi hyökyaallosta.

Julkinen tehtävä

Henkilötietoja voidaan käsitellä julkisen tehtävän suorittamiseksi.

⁵ Katso tietosuoja-asetuksen artikla 6.

Omat muistiinpanot:

Omat muistiinpanot:

Tietosuojalaissa termillä erityiset henkilötietoryhmät tarkoitetaan arkaluonteisia tietoja, joista ilmenee

- rotu tai etninen alkuperä
- poliittinen mielipide
- uskonnollinen tai filosofinen vakaumus
- ammattiliiton jäsenyys
- terveydentila
- seksuaalinen käyttäytyminen ja suuntautuminen
- geneettinen tai biometrinen informaatio, josta henkilön voi tunnistaa.

Pääsääntöisesti arkaluonteisten tietojen käsittely on kiellettyä. Rekisteröidyn suostumus ei kumoakaan lakiin perustuvaa käsittelykieltoa.

Arkaluonteisia tietoja saa käsitellä seuraavissa tapauksissa:

- Rekisteröity on antanut nimenomaisen suostumuksensa kyseisten henkilötietojen käsitte-
lyyn yhtä tai useampaa tiettyä tarkoitusta varten. Tietoja ei kuitenkaan voi käsitellä, jos
käsittely on kielletty lainsäädännössä. Rekisteröidyn suostumus ei kumoa lakiin perus-
tuvaa käsittelykieltoa.
- Käsittely on tarpeen rekisterinpitäjän tai rekisteröidyn velvoitteiden ja erityisten
oikeuksien noudattamiseksi työoikeuden, sosiaaliturvan ja sosiaalisen suojelun alalla.
- Käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen
suojaamiseksi, jos rekisteröity on fyysisesti tai juridisesti estynyt antamasta suostumus-
taan.

JATKUU SEURAAVALLA SIVULLA

- Omat muistiinpanot:

6. REKISTERÖITYJEN OIKEUDET

Tietosuoja-asetuksessa on säädetty rekisteröityjen oikeuksista. Rekisteröidyn oikeudet tarkoittavat rekisterinpitäjälle velvollisuuksia.

Rekisteröidyllä on oikeus

1.	saada läpinäkyvästi tietoa henkilötietojen käsittelystä
2.	saada pääsy omiin tietoihin
3.	tietojen oikaisemiseen
4.	tulla unohdetuksi, eli tietojen poistamiseen
5.	siirtää tiedot järjestelmästä toiseen
6.	rajoittaa tietojen käsittelyä

Yrittäjän on ilmoitettava henkilötiedon oikaisusta, poistoista tai käsittelyn rajoituksista jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu, paitsi jos tämä aiheuttaa kohtuutonta vaivaa. Yrittäjän on ilmoitettava rekisteröidyille näistä vastaanottajista, jos rekisteröity sitä pyytää.

§ Katso tietosuoja-asetuksen artiklat 12, 15–20.

Omat muistiinpanot:

[illegible]

JATKUU SEURAAVALLA SIVULLA 

Oikeus saada tietoa henkilötietojen käsittelystä

Rekisteröidyllä on aina oikeus saada tietää, käsittelee否 yritys hänen tietojaan. Jos tietoja käsitellään, on rekisteröidyllä oikeus saada tietoonsa hänestä tallennetut henkilötiedot sekä saada seuraavat tiedot:

- käsiteltävät henkilötietoryhmät
- vastaanottajat tai vastaanottajaryhmät, joille yritys on luovuttanut henkilötietoja tai joille tietoja on tarkoitus luovuttaa
- mahdollisuuksien mukaan henkilötietojen suunniteltu säilytysaika tai jos säilytysaikaa ei voi ilmoittaa, tämän ajan määrittämiskriteerit
- kaikki tietojen alkuperästä käytettävissä olevat tiedot, jos henkilötietoja ei kerätä rekisteröidyltä
- ilmoitus henkilötiedon siirtoa EU:n ulkopuolelle koskevista asianmukaisista toimista
- automaattisen päätöksenteon (mukaan lukien profiloinnin) olemassaolo, keskeiset tiedot tietojen käsittelyyn liittyvästä logiikasta sekä käsittelyn merkittävydestä ja mahdollisista seurauksista rekisteröidylle.

Lisäksi rekisteröidylle tulee kertoa, että hänellä on oikeus

- pyytää rekisterinpitäjältä häntä koskevien henkilötietojen oikaisemista, poistamista tai henkilötietojen käsittelyn rajoittamista
- tehdä valitus valvontaviranomaiselle.

Pääsy tietoihin toteutetaan siten, että rekisteröidylle toimitetaan jäljennös käsiteltävistä henkilötiedoista sekä tietosuojaseloste eli tätä tarkoitusta varten laadittu seloste. Rekisteröidylle ei tarvitse antaa esimerkiksi tietoja, joissa on mukana liikesalaisuuksia tai muiden henkilöiden henkilötietoja. Yritys voi laatia edellä olevista tiedoista erillisen selosteen tai muotoilla tietosuojaselosteensa kattamaan nämä tiedot.

Omat muistiinpanot:

JATKUU SEURAAVALLA SIVULLA ➔

Oikeus tietojen oikaisemiseen

Rekisteröidyllä on oikeus vaatia, että yritys oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot. Rekisteröidyllä on oikeus saada puutteelliset henkilötiedot täydennettyä, muun muassa toimittamalla lisäselvitys.

Yrityksen tulisi pystyä muokkaamaan rekisterinsä tietoja jälkikäteen, jotta epätarkat tai virheelliset tiedot voidaan korjata.

 Katso tietosuoja-asetuksen artikla 16.

Oikeus tulla unohdetuksi

Rekisteröidyllä on oikeus saada yritys poistamaan häntä koskevat tiedot eli oikeus tulla unohdetuksi seuraavissa tilanteissa:

-  Henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä muutoin käsiteltiin. Jos esimerkiksi kokoustila on varattu ja asiakkaan tiedot on kerätty vain tätä varten, tulee tiedot poistaa asiakkaan pyynnöstä kokouksen jälkeen (olettaen, että tietoja ei enää tarvita muun lainsäädännön tai edun nojalla).
-  Henkilötietojen käsittely perustuu suostumukseen ja rekisteröity peruuttaa antamansa suostumuksen. Jos rekisteröity vastustaa muuta käsittelyä kuin käsittelyä suoramarkkinointia varten, on lisäedellytyksenä se, että käsittelyyn ei ole olemassa perusteltua syytä.
-  Rekisteröity vastustaa käsittelyä. Jos rekisteröity vastustaa muuta käsittelyä kuin käsittelyä suoramarkkinointia varten, on lisäedellytyksenä se, että käsittelyyn ei ole olemassa perusteltua syytä.
-  Henkilötietoja on käsitelty lainvastaisesti.
-  Henkilötiedot on poistettava lakisääteisen veloitteen noudattamiseksi.
-  Henkilötiedot on kerätty tarjottaessa sähköisiä palveluja suoraan lapselle.

Yrityksillä voi olla oikeutettu etu henkilötietojen käsittelyyn, jolloin tietoja ei tarvitse poistaa. Yrityksillä on siten oikeus käsitellä työntekijöidensä tietoja, vaikka työntekijä sitä vastustaisikin.

 Katso tietosuoja-asetuksen artikla 17.

Omat muistiinpanot:

JATKUU SEURAAVALLA SIVULLA 

S Katso tietosuoja-asetuksen artiklat 18 ja 19.

Rekisteröidyllä on oikeus olla joutumatta profiloinnin kohteeksi. Profilointi tarkoittaa, että henkilölle tehdään hänen henkilökohtaisia ominaisuuksiaan arvioiva, mahdollisesti toimenpiteen sisältävä päätös yksinomaan automaattisen tietojenkäsittelyn perusteella. Automatoitu päätöksenteko aiheuttaa henkilölle oikeudellisia tai muita vaikutuksia. Tällaisia voivat olla esimerkiksi online-luottihakemuksen automaattinen epääminen tai sähköinen ja automaattinen rekrytointi ilman, että kukaan ihminen osallistuu päätöksentekoon.

[illegible]

REKISTERÖITYJEN OIKEUDET 18

- perustuu rekisteröidyn nimenomaiseen suostumukseen
- on välttämätön rekisteröidyn ja yrittäjän välisen sopimuksen tekemistä tai päätöksen-
tekoa varten
- on hyväksytty EU- tai kansallisessa lainsäädännössä.

§ Katso tietosuoja-asetuksen artikla 22.

[illegible]

7. KUN TIETOJA KERÄTÄÄN REKISTERÖIDYLTÄ

Henkilötietojen käsittelyn tulee olla läpinäkyvää, ja rekisteröidyille tulee kertoa, kuinka heitä koskevia tietoja kerätään ja kuinka niitä käytetään. Tiedot tulisi antaa tiiviisti, yksinkertaisella ja selkeällä kielellä. Rekisteröityjen tulee saada tiedot maksutta.

Kuitenkin, jos pyyntöjä esitetään toistuvasti ja ne ovat kohtuuttomia tai ilmeisen perusteettomia, voi yritys periä kohtuullisen maksun tai kieltäytyä antamasta tietoja. Tällöin yrityksen tulisi pystyä osoittamaan pyynnön perusteettomuus tai kohtuuttomuus.

Yrityksen tulisi pitää kuvaus henkilötietojen käsittelystä rekisteröidyn saatavilla. Asetuksen mukaan tiedot tulisi toimittaa kirjallisesti, suullisesti tai sähköisesti. Esimerkiksi messuilla järjestettävästä arvontaan osallistumisesta ja henkilötietojen käsittelystä voidaan kertoa antamalla rekisteröitävälle paperi, jossa kuvaillaan henkilötietojen käyttöä.

Kun kerätään rekisteröidyltä häntä koskevia henkilötietoja, rekisterinpitäjän on toimitettava rekisteröidylle kaikki seuraavat tiedot:

- tietosuojavastaavan yhteystiedot, jos sellainen on
- peruste eli syy, jonka perusteella henkilötietoja saa käsitellä
- henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste eli syy, jonka perusteella henkilötietoja saa käsitellä
- henkilötietojen vastaanottajat tai vastaanottajaryhmät
- aikooko rekisterinpitäjä siirtää henkilötietoja EU:n ulkopuolelle
- rekisteröidyn oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää tietojen oikaisemista tai poistamista tai käsittelyn rajoittamista tai vastustaa käsittelyä sekä oikeutta siirtää tiedot järjestelmästä toiseen

Omat muistiinpanot:

JATKUU SEURAAVALLA SIVULLA ➔

- oikeus peruuttaa suostumus milloin tahansa ilman, että se vaikuttaa suostumuksen perusteella ja ennen sen peruuttamista suoritettun käsittelyn lainmukaisuuteen
- onko henkilötietojen antaminen lakisääteinen, sopimukseen perustuva tai sopimuksen tekemisen edellyttämä vaatimus
- onko rekisteröidyn pakko toimittaa henkilötiedot ja mitä tällaisten tietojen antamatta jättämisestä mahdollisesti seuraa.
- automaattisen päätöksenteon eli profiloinnin olemassaolo, merkitykselliset tiedot käsitte-lyyn liittyvästä logiikasta sekä käsittelyn merkittävyys ja mahdolliset seuraukset rekiste-röidylle.

Jos rekisterinpitäjä aikoo käsitellä henkilötietoja edelleen muuhun tarkoitukseen kuin siihen, johon henkilötiedot kerättiin, rekisterinpitäjän on ilmoitettava asiasta rekisteröidylle ennen kyseistä jatkokäsittelyä ja annettava asiaan kuuluvat lisätiedot.

Yrittäjän voi olla helpointa kuvata henkilötietojen käsittelyn nykytilaa laatimalla perinteinen rekisteriseloste. Tietosuojaviranomaiset aikovat julkistaa mallin tietosuoja-asetuksen mukaisesta tietosuojaselosteesta. Käytännössä yritykset voivat hyödyntää nykyisen henkilötietolain veloitteen perusteella laadittuja rekisteriselosteitaan ja laajentaa niitä vastaamaan tietosuoja-asetuksen edellytyksiä. Yrittäjän tulisi pitää selosteet ajan tasalla päivittämällä niitä tasaisin väliajoin.

Informointivelvoite tarkoittaa käytännössä sitä, että yrityksen tulee antaa edellä mainitut tiedot henkilötietoja vastaanottaessaan. Tiedot voidaan antaa esimerkiksi tietosuojaselosteena tai muulla tavalla verkkosivuilla, tai tietoja voidaan pitää saatavilla työpaikan intranetissä tai fyysisenä kappaleena esimerkiksi ilmoitustaululla.

§ Katso tietosuoja-asetuksen artikla 13.

Omat muistiinpanot:

[illegible]

8. KUN TIETOJA EI OLE SAATU REKISTERÖIDYLTÄ ITSELTÄÄN

Jos rekisterissä olevia henkilötietoja ei ole saatu rekisteröidyltä itseltään, rekisterinpitäjän on toimitettava rekisteröidylle seuraavat tiedot:

- yrityksen mahdollisen tietosuojavastaavan yhteystiedot
- henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste, eli tietosuoja-asetuksen peruste käsitellä henkilötietoja (ks. luku 4)
- rekisterissä olevat henkilötietoryhmät
- tarvittaessa tieto siitä, että rekisterinpitäjä aikoo siirtää henkilötietoja kolmannessa maassa olevalle vastaanottajalle tai kansainväliselle järjestölle
- henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit
- rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut
- oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin
- oikeus pyytää tietojen oikaisemista tai poistamista tai käsittelyn rajoittamista
- oikeus vastustaa käsittelyä
- oikeus siirtää tiedot järjestelmästä toiseen
- oikeus tehdä valitus valvontaviranomaiselle
- mistä henkilötiedot on saatu sekä tarvittaessa se, onko tiedot saatu yleisesti saatavilla olevista lähteistä
- automaattisen päätöksenteon eli profiloinnin olemassaolo.

Rekisterinpitäjän on toimitettava nämä tiedot viimeistään kuukauden kuluessa henkilötietojen saamisesta tai, jos henkilötietoja käytetään viestintään asianomaisen rekisteröidyn kanssa, viimeistään silloin kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran. Edellä luetellut tiedot tulee luovuttaa myös silloin, jos henkilötietoja on tarkoitus luovuttaa toiselle vastaanottajalle, viimeistään silloin kun näitä tietoja luovutetaan ensimmäisen kerran.

5 Katso tietosuoja-asetuksen artikla 14.

Omat muistiinpanot:

10. SELOSTE KÄSITTELYTOIMISTA

Tietosuoja-asetus velvoittaa yrityksen tekemään selosteen käsittelytoimista. Tätä tulee pitää yleisesti saatavilla esimerkiksi yrityksen nettisivuilla tai yrityksen toimipaikassa.

Yrittäjän tulee tehdä jokaisesta rekisteristä oma seloste käsittelytoimista. Tällaisia rekistereitä ovat esimerkiksi asiakasrekisteri ja työntekijärekisteri.

Selosteessa tulisi olla seuraavat tiedot:

- rekisterinpitäjän ja mahdollisen yhteisrekisterinpitäjän, rekisterinpitäjän edustajan ja tietosuojavastaavan nimi ja yhteystiedot
- käsittelyn tarkoitukset
- kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä
- henkilötietojen vastaanottajien ryhmät, joille henkilötietoja on luovutettu tai luovutetaan
- tarvittaessa tiedot henkilötietojen luovuttamisesta EU-alueen ulkopuolelle
- mahdollisuuksien mukaan eri tietoryhmien poistamisen suunnitellut määräajat
- mahdollisuuksien mukaan yleinen kuvaus käsittelyn turvallisuuden varmistamiseksi toteutetuista teknisistä ja organisatorisista turvatoimista.

S Katso tietosuoja-asetuksen artiklat 13 ja 30.

Omat muistiinpanot:

[illegible]

11. SUORAMARKKINOINTI

Suoramarkkinointia saa harjoittaa jatkossakin, jos vastaanottajille kerrotaan mahdollisuudesta kieltää suoramarkkinointi. Tämä mahdollisuus kieltäytyä suoramarkkinoinnista tulee saattaa rekisteröidyn tietoon. Rekisteröidyllä on oikeus ilman maksua vastustaa käsittelyä.

Perinteinen suoramarkkinointi

Perinteisellä suoramarkkinoinnilla tarkoitetaan postitse tai puhelimitse tehtävää suoramarkkinointia. Suomessa saa tehdä kuluttajalle suoramarkkinointia näillä perinteisillä menetelmillä, kunnes vastaanottaja sen kieltää. Kuluttajalta ei siten tarvitse pyytää ennakoon suostumusta perinteiseen suoramarkkinointiin.

Kuluttajalle pitää kertoa oikeudesta kieltää suoramarkkinointi. Tietoa voidaan antaa asiakassuhteen tai muun yhteydenpidon aloitushetkellä sekä selosteessa käsittelytoimista. Henkilöille tulisi lähtökohtaisesti kertoa paikan päällä, että heidän yhteystietonsa tallennetaan suoramarkkinointirekisteriin. Tällainen teksti voisi olla esimerkiksi paperissa, johon yhteystiedot kirjoitetaan. Teksti voi olla seuraavanlainen:

"Osallistujan tietoja voidaan käsitellä Yritys Oy:n suoramarkkinointitarkoituksiin. Suoramarkkinoinnin voi kieltää ilmoittamalla siitä asiakaspalveluumme..."

Ulkoistettu suoramarkkinointi

Suoramarkkinointikirjeiden postitus saatetaan ulkoistaa tulostus- ja postipalveluja tarjoavalle yhteistyökumppanille. Tällöin markkinoijan asiakkaiden tai potentiaalisten asiakkaiden henkilötietoja käsittelevät muutkin kuin markkinoija. Käsittelijän tulisi antaa rekisterinpitäjälle asianmukaiset selvitykset ja sitoumukset sekä riittävät takeet henkilötietojen suojaamisesta asianmukaisesti.

Käytännössä tämä tarkoittaa sitä, että markkinoijan ja palveluntarjoajan välisessä yhteistyö- ja toimeksiantosopimuksessa tulisi olla sopimuslausekkeet tietosuojasetuksen mukaisista velvoitteista. Markkinoija on viimekädessä vastuussa, että henkilötietoja käsitellään lainmukaisesti. Rekisterinpitäjä vastaa siis myös yhteistyökumppaninsa toimista. Tämän takia keskinäisistä vahingonkorvausvelvollisuuksista olisi tärkeä sopia. Käsittelyn ulkoistamisesta kerrotaan luvussa 12.

Omat muistiinpanot:

JATKUU SEURAAVALLA SIVULLA ➔

12. TIETOJENKÄSITTELYN ULKOISTAMINEN

Rekisterinpitäjä voi ulkoistaa henkilötietojen käsittelyn. Ulkoistettuja palveluita ovat esimerkiksi

- ▶ tilitoimisto, joka maksaa työntekijöiden palkat
- ▶ IT-tuki, jolla on pääsy henkilötietoihin.

Näissä tilanteissa henkilötietojen katsotaan siirtyvän niin sanotulle henkilötietojen käsittelijälle eli sille palveluntarjoajalle, joka käsittelee henkilötietoja rekisterinpitäjän puolesta.

Rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka huolehtivat asianmukaisista suojatoimista ja varmistavat, että käsittely täyttää tietosuojasetuksen vaatimukset. Näin varmistetaan rekisteröidyn oikeuksien suojeleminen.

Tietojen käsittelijän on kerrottava rekisterinpitäjälle, jos se suunnittelee esimerkiksi henkilötietojen käsittelijöiden lisäämistä tai vaihtamista, ja annettava siten rekisterinpitäjälle mahdollisuus vastustaa tällaisia muutoksia.

Yrittäjän tulisi ohjeistaa henkilötietojen käsittelijänä toimivaa palveluntarjoajaa. Ohjeet tulisi antaa kirjallisina. Ne ovat useimmiten osa niin sanottua tietojenkäsittelysopimusta, jossa määritetään sekä rekisterinpitäjän että henkilötietojen käsittelijän oikeudet ja velvollisuudet suhteessa käsiteltäviin henkilötietoihin.

Tietojenkäsittelysopimuksessa tulisi sopia vähintään seuraavista asioista

- ▶ **Tietojenkäsittelyn yksilöinti** – Sopimukseen tulisi yksilöidä,
 - ▶ keitä yksilöitä (työntekijät)
 - ▶ millaisia tietoja (palkanmaksutiedot) ulkoistus koskee.
- ▶ **Sitoutuminen rekisterinpitäjän ohjeisiin** – Henkilötietojen käsittelijän tulee sitoutua käsittelemään henkilötietoja ainoastaan rekisterinpitäjän ohjeiden ja sopimusehtojen mukaisesti.

Omat muistiinpanot:

JATKUU SEURAAVALLA SIVULLA ➔

- **Salassapito** – Sopimuksessa tulee varmistaa, että henkilötietojen käsittelyyn oikeutetut henkilöt, kuten henkilötietojen käsittelijän työntekijät, ovat sitoutuneet noudattamaan salassapitovelvollisuutta.
- **Tietoturva** – Henkilötietojen käsittelijän on sitouduttava sopimuksessa toteuttamaan riittävät turvatoimet henkilötietojen suojaamiseksi. Kyse voi olla teknisistä toiminnoista, kuten tietokoneiden virustorjunnasta ja palomuuereista, toimitilojen kulunvalvonnasta tai organisaatorisista toiminnoista, kuten riittävistä ja asiantuntevista resursseista.
- **Käsittelijän omat alihankkijat** – Sopimuksessa tulee sopia, tarvitseeko henkilötietojen käsittelijä rekisterinpitäjältä suostumuksen toisen käsittelijän, eli palveluntarjoajan oman alihankkijan, ottamiseksi osaksi tietojenkäsittelyä vai riittääkö jälkikäteen ilmoitus ja rekisterinpitäjän vastustamismahdollisuus.
- **Avustamisvelvollisuus** – Sopimuksessa tulee sopia, että käsittelijän on autettava rekisterinpitäjää täyttämään tämän yksilöiden oikeuksiin liittyvät velvollisuudet. Yksilöillä on lukuisia oikeuksia, kuten oikeus saada pääsy itseään koskeviin henkilötietoihin ja saada virheelliset tiedot oikaistuksi.
- **Tiedonantovelvollisuus** – Käsittelijän on saatettava rekisterinpitäjän saataville kaikki sellaiset tiedot, jotka ovat tarpeen, jotta voidaan osoittaa rekisterinpitäjän toimineen oikein.
- **Auditointioikeus** – Käsittelijän on sallittava rekisterinpitäjän tai muun sen valtuuttaman auditoinnin suorittamat auditoinnit ja osallistuttava niihin.
- **Tietojen poistaminen** – Kun käsittelyyn liittyvien palveluiden tarjoaminen on päättynyt, tulee henkilötietojen käsittelijän poistaa tai palauttaa kaikki henkilötiedot rekisterinpitäjälle, jollei käsittelijällä ole lakisääteistä velvollisuutta säilyttää henkilötietoja.
- **Vahingonkorvausvastuu** – Rekisterinpitäjä on viimekädessä vastuussa, että henkilötietoja käsitellään lainmukaisesti, joten rekisterinpitäjä vastaa myös yhteistyökumppaninsa toiminnoista. Tämän takia keskinäisistä vahingonkorvausvelvollisuuksista olisi tärkeä sopia.

[illegible]

S Katso tietosuojaa-asetuksen artiklat 28 ja 29.

13. TIETOJEN SIIRTÄMINEN EU:N ULKOPUOLELLE

Nykyään on tavallista, että tietoja saatetaan siirtää EU:n ulkopuolelle eli niin sanottuihin kolmansiin maihin. Tällainen saattaa tulla vastaan, kun esimerkiksi suomalainen matkailuyritys myy retkiä Islantiin ja osallistujien tiedot siirretään yhteistyökumppanille Islantiin. Myös pilvipalvelut hyödyntävät usein toiminnassaan EU:n ulkopuolella toimivia palvelimia.

Olisi hyvä tarkistaa ennen tiedon siirtämistä, onko komissio katsonut kohdemaan täyttävän kriteerit.

Kriteerit täyttyviä maita ovat tällä hetkellä

- Andorra
 - Argentiina
 - Färsaaret
 - Islanti
 - Israel
 - Jersey
 - Kanada
 - Mansaari
 - Norja
 - Sveitsi
 - Uruguay
 - Uusi-Seelanti
 - Yhdysvallat (rajoitetusti).

Yhdysvalloissa kriteerit katsotaan täyttyvän vain niillä yrityksillä, jotka ovat liittyneet Privacy Shield -järjestelmään. Siten vain näihin yrityksiin saa siirtää henkilötietoja. Yhdysvaltojen kauppaministeriö pitää yllä julkista listaa järjestelmään liittyneistä yrityksistä osoitteessa www.privacyshield.gov.

Jos komissio ei ole tehnyt päätöstä tietystä maasta henkilötietojen siirtäminen sinne sallittua, jos yrittäjä tai henkilötietojen käsittelijä ovat toteuttaneet asianmukaiset suojatoimet ja jos rekisteröityjen saatavilla on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja.

Ajantasainen tieto kriteerit täyttävistä maista

ec.europa.eu ›
European Commission › Strategy ›
Justice and fundamental rights ›
Data protection ›
Data transfers outside the EU

[Siirry sivulle »](#)

Omat muistiinpanot:

[illegible]

JATKUU SEURAAVALLA SIVULLA

Asianmukaisina suojatoimina pidetään

- yrityksiä koskevia sitovia sääntöjä
- komission antamien tai hyväksymien tietosuojaa koskevien vakiolausekkeiden käyttöä siirtoa koskevissa sopimuksissa
- valvontaviranomaisen hyväksymiä ja rekisteröimiä käytännesääntöjä
- tietosuojaa koskevia vakiolausekkeitä
- tiettyjä sertifiointeja, jotka tietosuojaviranomainen vahvistaa ja komissio hyväksyy.

Erityistilanteissa henkilötietojen siirto EU-alueen ulkopuolelle on myös sallittua, jos jokin seuraavista edellytyksistä täyttyy:

- rekisteröity on antanut nimenomaisen suostumuksensa ehdotettuun siirtoon sen jälkeen, kun hänelle on ilmoitettu, että tällaiset siirrot voivat aiheuttaa rekisteröidylle riskejä tietosuojan tason riittävyyttä koskevan päätöksen ja asianmukaisten suojatoimien puuttumisen vuoksi
- siirto on tarpeen rekisteröidyn ja rekisterinpitäjän välisen sopimuksen täytäntöönpanemiseksi tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä (katso luku 4)
- siirto on tarpeen rekisterinpitäjän ja toisen henkilön tai oikeushenkilön välisen, rekisteröidyn edun mukaisen sopimuksen tekemiseksi tai täytäntöönpanemiseksi
- siirto on tarpeen tärkeää yleisen edun vuoksi (katso luku 4)
- siirto on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi
- siirto on tarpeen rekisteröidyn tai muiden henkilöiden elintärkeiden etujen suojaamiseksi, jos rekisteröity on fyysisesti tai juridisesti estynyt antamasta suostumustaan.

⁵ Katso tietosuoja-asetuksen artiklat 44–49.

Omat muistiinpanot:

Tietosuojavastaavalla on oltava ainakin seuraavat tehtävät:

- antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle sekä henkilötietoja käsitteleville työntekijöille tietoja ja neuvoja, jotka koskevat niiden tämän asetuksen ja muiden unionin tai jäsenvaltioiden tietosuojasäännösten mukaisia velvollisuuksia
- seurata, että yrityksessä noudatetaan tätä asetusta, muita EU:n ja jäsenvaltion tietosuoja-lain säännöksiä
- seurata rekisterinpitäjän tai henkilötietojen käsittelijän toimintaa
- seurata vastuunjakoja ja sitä, että tiedon käsittelyyn osallistuvaa henkilöstöä koulutetaan
- antaa pyydettäessä neuvoja tietosuoja koskevasta vaikutustenarvioinnista ja valvoa sen toteutusta
- toimia valvontaviranomaisen yhteyshenkilönä käsittelyyn liittyvissä kysymyksissä, mukaan lukien ennakkuuleminen ja kuuleminen muissa mahdollisissa kysymyksissä.

Tietosuojavastaavan on tehtäviään suorittaessaan otettava asianmukaisesti huomioon käsittelyyn liittyvä riski sekä käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset. Yritys on loppujen lopuksi vastuussa henkilötietojen tietosuoja-asetuksen mukaisesta käsittelystä. Tätä vastuuta ei voi siirtää tietosuojavastaavalle.

9 Katso tietosuoja-asetuksen artiklat 38 ja 39.

Omat muistiinpanot:

15. KÄSITTELYN TURVALLISUUS

Omat muistiinpanot:

Rekisterinpitäjän ja henkilötietojen käsittelijän on asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä varmistettava, että käsittelyn turvallisuustaso vastaa riskiä.

Näitä toimenpiteitä ovat esimerkiksi:

- henkilötietojen pseudonymisointi ja sala
- kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus
- kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa
- menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin. Rekisterinpitäjän ja henkilötietojen käsittelijän on varmistettava, että jokainen, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti.

6 Katso tietosuoja-asetuksen artikla 32.

Vaikutustenarviointi

Jos tietojen käsitteleminen aiheuttaa henkilölle korkean riskin, tulee rekisterinpitäjän laatia vaikutustenarviointi. Tällöin yrityksen tulisi pyytää neuvoja tietosuojavastaavalta, jos sellainen on nimitetty. Tietosuojavastaavasta kerrotaan tarkemmin luvussa 14.

Vaikutustenarviointi vaaditaan erityisesti silloin, kun

- henkilöiden ominaisuuksia arvioidaan automatisoidun käsittelyn perusteella järjestelmällisesti ja kattavasti ja sillä on vaikutusta henkilön oikeuksiin (profilointi)
- laajamittainen käsittely kohdistuu erityisiin henkilötietoryhmiin tai rikostuomioita tai rikkomuksia koskeviin tietoihin.
- valvotaan avointa aluetta järjestelmällisesti ja laajamittaisesti esimerkiksi kameroilla.

6 Katso tietosuoja-asetuksen artikla 35

17. SANKTIOT JA SAKOT

Jos henkilölle aiheutuu tietosuoja-asetuksen rikkomisesta aineellista tai aineetonta vahinkoa, hänellä on oikeus saada rekisterinpitäjältä tai henkilötietojen käsittelijältä korvaus. Kukin tietojenkäsittelyyn osallistunut rekisterinpitäjä on vastuussa vahingosta.

Jos rekisterinpitäjä tai henkilötietojen käsittelijä on maksanut täyden korvauksen aiheutuneesta vahingosta, rekisterinpitäjällä tai henkilötietojen käsittelijällä on oikeus periä muilta samaan tietojenkäsittelyyn osallistuneilta rekisterinpitäjiltä tai henkilötietojen käsittelijöiltä se osuus korvauksesta, joka vastaa niiden mukaista vastuuta vahingosta.

Rekisterinpitäjä tai henkilötietojen käsittelijä on vapautettava vastuusta, jos se pystyy osoittamaan, ettei se ole millään tavoin vastuussa vahingon aiheuttaneesta tapahtumasta.

Jos samaan tietojenkäsittelyyn osallistuu useampi kuin yksi rekisterinpitäjä tai henkilötietojen käsittelijä ja jos ne ovat vastuussa käsittelystä aiheutuneesta mahdollisesta vahingosta, kukin rekisterinpitäjä tai henkilötietojen käsittelijä on vastuussa koko vahingosta. Näin voidaan varmistaa, että rekisteröity saa tosiasiallisen korvauksen.

 Katso tietosuoja-asetuksen artiklat 82 ja 83.

Rikkomuksista hallinnollisia sakkoja

Kun päätetään hallinnollisen sakon määräämisestä ja sen määrästä, on otettava huomioon seuraavat seikat:

-  mitä velvollisuuksia on rikottu
-  rekisteröityjen lukumäärä, joihin rikkomus vaikuttaa
-  rekisteröidyille aiheutuneen vahingon suuruus
-  tapa jolla teko tuli valvontaviranomaisen tietoon (ilmoittiko rekisterinpitäjä itse vai joku muu)
-  muut asiaan liittyvät raskauttavat tai lieventävät tekijät.

Hallinnollinen sakko on enimmillään 20 miljoonaa euroa tai neljä prosenttia yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

-  tietosuoja-asetuksen peruseriaatteen
-  rekisteröityjen oikeudet
-  tietojen siirrosta EU:n ulkopuolelle aiheutuvat velvoitteet

 Katso tietosuoja-asetuksen artikla 83.

Omat muistiinpanot:

18. KÄYTÄNNÖN TOIMENPITEITÄ YRITTÄJILLE

Asetuksen noudattamiseksi yrittäjän tulee kirjoittaa dokumentaatiota seuraavista aiheista:

- Varmista, että sinulla on asetuksen mukainen käsittelyperuste, joka oikeuttaa käsittelemään henkilötietoja. Näitä ovat esimerkiksi sopimus ja oikeutettu etu (luku 4).
- Laadi selosteet käsittelytoimista (luku 10).
- Dokumentoi, kuinka rekisteröityjä on informoitu (luvut 7-9).
- Laadi sopimukset käsittelyn ulkoistamisesta tai tietojen siirtämisestä (luku 12).
- Varmista ja dokumentoi henkilötietojen käsittelyn turvallisuus, virustorjunta, palomuri ja toimitilojen turvallisuus (luku 15).
- Laadi tarvittaessa työntekijöiden kanssa salassapitosopimukset.
- Selvitä, tarvitsetko tietosuojavastaavan (luku 14).
- Selvitä, tuleeko sinun laatia tietosuoja koskeva vaikutustenarviointi (luku 15).
- Varaudu tiedottamaan rekisteröityä kattavasti ja ymmärrettävästi (luvut 7 ja 8).
- Selvitä, noudatetaanko henkilötietojen siirroissa EU:n ulkopuolelle tietosuoja-asetusta (luku 13).
- Valmistaudu tilanteeseen, jossa joudut kertomaan tietomurrosta rekisteröidyille ja valvontaviranomaiselle. (luku 16).
- Valmistaudu rekisteröidyn oikeuksien käyttöön, kuten oikeuteen saada pääsy tietoihin, oikeuteen tulla unohdetuksi, oikeuteen siirtää tiedot järjestelmästä toiseen ja vastustamisoikeuteen (luku 6).
- Rekisterinpitäjän tulisi säilyttää dokumentaatiota hallussaan ja päivittää sitä tarpeen tullen.

Omat muistiinpanot:



TIETOSUOJA-ASETUKSEEN VOI VARAUTUA VAKUUTUKSELLA

Kumppanisisältö



Tietosuoja-asetus asettaa rekisterinpitäjälle eli yrityksellesi velvollisuuksia, joihin voit varautua myös vakuutuksella. Kun sinulla on Fennian tietoturvakvakuutus, sinulla on paremmat valmiudet vastata näihin velvollisuuksiin ja mahdollisesta tietoturvaloukkauksesta aiheutuviin taloudellisiin vahinkoihin:

- järjestelmien luottamuksellisuuden, eheyden, käytettävyyden ja vikasietoisuuden varmistaminen sekä valmius palauttaa nopeasti tietojen saatavuus tietoturvaloukkauksen jälkeen
- tietoturvaloukkauksesta ilmoittaminen valvontaviranomaisille ja rekisteröidyille
- vahingonkorvausvastuu rekisteröidylle
- hallinnolliset sakot.

Vakuutukseen sisältyy Fennian 24h tietoturvapalvelu. Se auttaa ongelmien selvittämisessä ja tietojärjestelmien nopeassa palauttamisessa. Palvelu sisältää

- teknisen tietoturva-asiantuntijan palvelut
- lakimiehen neuvontapalvelun ilmoittamisvelvollisuuksien täyttämiseen.

Tärkeä osa vakuutusta on myös vastuuvakuutus. Sen perusteella selvitetään korvausvastuu ja hoidetaan neuvottelut vahinkoa kärsineiden kanssa. Vastuuvakuutuksesta korvataan myös

- mahdolliset oikeudenkäyntiin liittyvät kulut
- vahingonkorvaukset vahinkoa kärsineille.

Lue lisää verkkosivuiltamme ja jätä yhteydenottopyyntö: fennia.fi/tietoturvakvakuutus

YRITTÄJYYDEN PUOLESTA



SUOMEN YRITTÄJÄT

Mannerheimintie 76 A, 3. krs, 00250 Helsinki

PL 999, 00101 Helsinki

(09) 229 221

toimisto@yrittajat.fi

www.yrittajat.fi