Espoon hiippakunta

Tietosuoja-asetus

Sari Anetjärvi
lakimiesasessori

Yleinen tietosuoja-asetus

- Yleinen tietosuoja-asetus (EU 679/2016) tulee kansallisesti Suomessa voimaan 25.5.2018. Se korvaa nykyisen henkilötietolain.
- Hallitus on tehnyt esityksen tietosuojalaiksi, jolla täsmennetään ja täydennetään tietosuoja-asetusta.
- Asetusta sovelletaan henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista, sekä sellaisten henkilötietojen käsittelyyn muussa kuin automaattisessa muodossa, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa.
- Erityislainsäädäntöä, esim. kirkkoon liittyvää, voi olla kunhan se on sopusoinnussa asetuksen kanssa.

Tietosuoja-asetuksen tavoite

Tietosuoja-asetuksen tavoitteena on

- varmistaa, että ihmisten oikeus henkilötietojen suojaan ja sitä kautta yksityisyyteen toteutuu myös digitaaliaikana
- vastata teknologian nopean kehityksen haasteisiin ja vahvistamaan ihmisten oikeutta valvoa henkilötietojaan
- vahvistaa säännöt henkilötietojen vapaalle liikkuvuudelle EU:n sisällä.

- Asetuksen myötä rekisterinpitäjille ja henkilötietojen käsittelijöille tulee nykyiseen nähden uusia tehtäviä ja velvollisuuksia sekä rekisteröidyille uusia oikeuksia.

Henkilötieto

- Henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (jäljempänä 'rekisteröity') liittyviä tietoja
  - tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella
- Henkilötieto voi olla esimerkiksi
  - paikkatieto, joka kertoo jotakin tietystä henkilöstä;
  - kuva, joka yhdistettynä esimerkiksi osoitetietoihin kertoo jotakin tietystä henkilöstä tai tämän elinolosuhteista
  - IP-osoite, jos tämä voidaan liittää tiettyyn käyttäjään tai käyttäjätunnus.

Henkilötietojen käsittely

- toiminto, joka kohdistetaan henkilötietoihin tai henkilötietojen kokoelmiin
- joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti
- tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista

Milloin henkilötietoja saa käsitellä?

- rekisteröity on antanut **suostumuksensa** henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten
- Suostumus on annettava selkeästi suostumusta ilmaisevalla toimella, kuten kirjallisella, sähköisellä tai suullisella lausumalla.
- Lausumasta on käytävä ilmi rekisteröidyn vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla hän hyväksyy henkilötietojensa käsittelyn.
- Suostumuksen on katettava kaikki käsittelytarkoitukset. Suostumusta ei voi antaa vaikenemalla, valmiiksi rastitetuilla ruuduilla tai jättämällä jonkin toimen toteuttamatta.
- Jos rekisteröidyn on annettava suostumuksensa sähköisen pyynnön perusteella, pyynnön on oltava selkeä ja tiiviisti esitetty, eikä se saa tarpeettomasti häiritä sen palvelun käyttöä, jota varten se annetaan.

Milloin henkilötietoja saa käsitellä?

- käsittely on tarpeen sellaisen *__sopimuksen__ täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä
- käsittely on tarpeen rekisterinpitäjän __lakisääteisen velvoitteen__ noudattamiseksi
- käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön __elintärkeiden etujen__ suojaamiseksi

Milloin henkilötietoja saa käsitellä?

- käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen **oikeutettujen etujen** toteuttamiseksi, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti rekisteröidyn ollessa lapsi.

- Erittäin monenlainen henkilötietojen käsittely perustuu oikeutettujen etujen toteuttamiseen.
- Oikeutettu etu voi olla olemassa esimerkiksi silloin, kun rekisteröidyn ja rekisterinpitäjän välillä on asiakas- tai palvelussuhde.

Milloin henkilötietoja saa käsitellä?

- käsittely on tarpeen **yleistä etua** koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi, kun

1) kysymys on henkilön asemaa, tehtäviä sekä niiden hoitoa julkisyhteisössä, elinkeinoelämässä, järjestötoiminnassa tai muussa vastaavassa toiminnassa kuvaavista tiedoista siltä osin kuin käsittelyn tavoite on yleisen edun mukainen ja käsittely on oikeasuhtaista sillä tavoiteltuun oikeutettuun päämäärään nähden;

2) käsittely on tarpeen ja oikeasuhtaista viranomaisen toiminnassa yleisen edun mukaisen tehtävän suorittamiseksi;

3) käsittely on tarpeen tieteellistä tai historiallista tutkimusta taikka tilastointia varten ja se on oikeasuhtaista sillä tavoiteltuun yleisen edun mukaiseen tavoitteeseen nähden; tai

4) henkilötietoja sisältävien tutkimusaineistojen, kulttuuriperintöaineistojen sekä näiden kuvailutietoihin liittyvien henkilötietojen käsittely arkistointitarkoituksessa on tarpeen ja oikeasuhtaista sillä tavoiteltuun yleisen edun mukaiseen tavoitteeseen ja rekisteröidyn oikeuksiin nähden.

Erityiset tiedot

Erityisiä tietoja ovat

- rotu tai etninen alkuperä
- poliittiset mielipiteet
- uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys
- geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten
- terveyttä koskevat tiedot
- seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot

- Erityisiä tietoja ei lähtökohtaisesti saa lainkaan käsitellä. (vrt. arkaluonteiset tiedot)

Milloin erityisiä tietoja saa käsitellä?

- rekisteröity on antanut nimenomaisen suostumuksensa
- 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 suostumustaan
- käsittely suoritetaan poliittisen, filosofisen, uskonnollisen tai ammattiliittotoimintaan liittyvän säätiön, yhdistyksen tai muun voittoa tavoittelemattoman yhteisön laillisen toiminnan yhteydessä ja asianmukaisin suojatoimin,
- käsittely koskee henkilötietoja, jotka rekisteröity on nimenomaisesti saattanut julkisiksi
- käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi tai aina, kun tuomioistuimet suorittavat lainkäyttötehtäviään

Milloin erityisiä tietoja saa käsitellä?

- käsittely on tarpeen tärkeää yleistä etua koskevasta syystä unionin oikeuden tai jäsenvaltion lainsäädännön nojalla, edellyttäen että se on oikeasuhteinen tavoitteeseen nähden, siinä noudatetaan keskeisiltä osin oikeutta henkilötietojen suojaan ja siinä säädetään asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn perusoikeuksien ja etujen suojaamiseksi
- käsittely on tarpeen ennalta ehkäisevää tai työterveydenhuoltoa koskevia tarkoituksia varten, työntekijän työkyvyn arvioimiseksi, lääketieteellisiä diagnooseja varten, terveys- tai sosiaalihuollollisen hoidon tai käsittelyn suorittamiseksi taikka terveys tai sosiaalihuollon palvelujen ja järjestelmien hallintoa varten unionin oikeuden tai jäsenvaltion lainsäädännön perusteella tai terveydenhuollon ammattilaisen kanssa tehdyn sopimuksen mukaisesti

Milloin erityisiä tietoja saa käsitellä?

- käsittely on tarpeen kansanterveyteen liittyvän yleisen edun vuoksi, kuten vakavilta rajat ylittäviltä terveysuhkilta suojautumiseksi tai terveydenhuollon, lääkevalmisteiden tai lääkinnällisten laitteiden korkeiden laatu- ja turvallisuusnormien varmistamiseksi sellaisen unionin oikeuden tai jäsenvaltion lainsäädännön perusteella, jossa säädetään asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn oikeuksien ja vapauksien, erityisesti salassapitovelvollisuuden, suojaamiseksi
- käsittely on tarpeen yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä ja historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten

Henkilötietojen käsittelyn periaatteet

- Henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi.
    - Läpinäkyvällä käsittelyllä tarkoitetaan sitä, että rekisteröidylle tulisi olla läpinäkyvää se, miten heitä koskevia tietoja kerätään ja käytetään sekä missä määrin henkilötietoja käsitellään tai on aikeissa käsitellä. Läpinäkyvyyden periaatteen mukaisesti henkilötietojen käsittelyyn liittyvien tietojen ja viestinnän on oltava helposti saatavilla ja ymmärrettävissä.
    - Luonnollisille henkilöille olisi tiedotettava henkilötietojen käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista ja oikeuksista sekä siitä, miten he voivat käyttää tällaista käsittelyä koskevia oikeuksiaan. Varsinkin henkilötietojen käsittelyn nimenomaiset tarkoitukset olisi määritettävä ja ilmoitettava henkilötietojen keruun yhteydessä yksiselitteisesti ja lainmukaisesti.

Henkilötietojen käsittelyn periaatteet

- Henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteen sopimattomalla tavalla (käyttötarkoitussidonnaisuus)
  - Tässä yhteydessä tietosuoja-asetuksessa on kuitenkin katsottu, että mikäli tietoja käytetään myöhemmin arkistointitarkoitusta varten taikka tietoja käytetään historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten ei käyttötarkoitussidonnaisuutta tarvitse olla.
- Henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään (tietojen minimointi)
  - Henkilötietoja olisi käsiteltävä vain, jos käsittelyn tarkoitusta ei voida kohtuullisesti toteuttaa muilla keinoin.
- Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä; on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä (täsmällisyys);
  - Rekisterinpitäjän olisi siten asetettava määräajat henkilötietojen poistoa tai niiden säilyttämisen tarpeellisuuden määräaikaistarkastelua varten, jotta voidaan varmistaa, ettei henkilötietoja säilytetä pidempään kuin on tarpeen.

Henkilötietojen käsittelyn periaatteet

- Henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan, kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. (säilytyksen rajoittaminen)
- henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia. (eheys ja luottamuksellisuus)
  - Henkilötietojen käsittelyssä olisikin muun muassa ehkäistävä luvaton pääsy henkilötietoihin tai niiden käsittelyyn käytettyihin laitteistoihin sekä tällaisten tietojen tai laitteistojen luvaton käyttö.

Rekisterinpitäjän osoitusvelvollisuus

- Tietosuoja-asetuksen mukaan rekisterinpitäjän vastaa siitä, että henkilötietojen käsittelyn periaatteita ja vaatimuksia noudatetaan.
- Tämän lisäksi rekisterinpitäjän on pystyttävä osoittamaan, että kyseisiä periaatteita ja vaatimuksia on noudatettu.

- Rekisterinpitäjän on huolehdittava siitä, että henkilötietojen käsittelyn periaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa.
- Rekisterinpitäjän on etukäteen arvioitava, mitä periaatteet käytännössä tarkoittavat ja miten ne toteutuvat omassa toiminnassa ja dokumentoida tämä arviointi.

Henkilörekisteri

- Henkilörekisterillä tarkoitetaan mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein.
- Tietojoukko voi olla keskitetty, hajautettu tai jaettu toiminnallisin tai maantieteellisin perustein.
- Esimerkiksi jäsenrekisteri ja käyttäjärekisteri ovat henkilörekistereitä.

Kuka pitää tai hoitaa rekisteriä?

- Rekisterinpitäjä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.
- Henkilötietojen käsittelijä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Rekisterinpitäjän vastuu

- Rekisterinpitäjä on vastuussa siitä, että se toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla varmistetaan ja käytännössä myös osoitetaan, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen vaatimuksia.
    - Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstön koulutusta, sisäisiä ohjeistuksia ja määräyksiä, salassapitosopimuksia ja -sitoumuksia, tilivalvontaa ja käytönvalvontaa, tietojen salausta, tietojen anonymisointia tai pseudonymisointia, tietojärjestelmien ja rekistereiden auditointeja, etäkäyttöyhteyksiä, käyttövalvontaa, teknisiä rajoituksia, tarkastus- ja valvontajärjestelmiä, tietotilinpäätösprosessia, käytännesääntöjen sekä sertifikaattien käyttöä.
- Toimenpiteiden riittävyys mitoitetaan riskiarvioinnin perusteella, jossa otetaan huomioon mm. käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä rekisteröityjen oikeuksiin ja vapauksiin kohdistuvat riskit. Toimenpiteitä on arvioitava ja tarkistettava säännöllisesti ja ne on päivitettävä tarvittaessa.

Rekisterinpitäjän vastuu

- Sisäänrakennetun ja oletusarvoisen tietosuojan periaate edellyttää, että tietosuojaan liittyvät tarpeet ja vaatimukset tunnistetaan ja huomioidaan jo ennen käsittelyn aloittamista.
- Käytännössä tietosuojan tarpeet tulisi selvittää ja määrittää jo henkilötietojen käsittelyn suunnitteluvaiheessa ja esim. hankintatilanteessa jo ennen tarjouspyynnön tekemistä, eli silloin, kun määritellään toimintoja, prosesseja ja järjestelmien ominaisuuksia. Tietojärjestelmät, joissa käsitellään henkilötietoja, rakennetaan niin, että ne oletusarvoisesti toteuttavat tietosuojan periaatteet ja asetuksen vaatimukset.

Rekisterinpitäjän vastuu

- Riskiperusteisen lähestymistavan mukaan konkreettiset toimenpiteet suhteutetaan henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin.
- Rekisterinpitäjän on tehtävä perusteellinen arvio henkilötietojen käsittelyyn liittyvistä riskeistä, jotta se tämän arvion perusteella voi määritellä tarvittavat suojatoimet ja riskiin vastaavat muut organisatoriset ja tekniset toimenpiteet.
- Riskeillä tarkoitetaan henkilötietojen käsittelystä rekisteröidylle mahdollisesti aiheutuvia fyysisiä, aineellisia tai aineettomia vahinkoja esimerkiksi silloin, kun käsittely saattaa johtaa syrjintään, identiteettivarkauteen tai petokseen, taloudellisiin menetyksiin, sosiaaliseen vahinkoon tai pseudonymisoinnin kumoutumiseen. Riski voi olla korkeampi silloin, kun käsitellään esimerkiksi erityisiä henkilötietoryhmiin kuuluvia tietoja, heikossa asemassa olevien (esimerkiksi lasten) tietoja tai kun käsitellään suuria määriä henkilötietoja ja käsittely koskee suurta rekisteröityjen määrää.

Seloste käsittelytoimista

- Rekisterinpitäjän, henkilötietojen käsittelijän ja näiden edustajan on ylläpidettävä kirjallista ja sähköisessä muodossa olevaa selostetta kaikista henkilötietojen käsittelytoimista. Velvollisuus ei koske yhteisöä, jossa on alle 250 työntekijää, paitsi jos sen suorittama käsittely todennäköisesti aiheuttaa riskin rekisteröidyn oikeuksille ja vapauksille, käsittely ei ole satunnaista tai käsittelyn kohteena on erityisen arkaluonteisia tietoja.
- Selosteesta on käytävä ilmi mm. henkilötietojen käsittelyn kannalta keskeisten tahojen yhteystiedot, käsittelyn kohteena olevien tietoryhmät ja tiedot henkilötietojen siirroista kolmansiin maihin.
- Siinä missä rekisteröidyille toimitettavat tiedot (eli rekisteriselosteet, ks. alla) ovat ulkoista käyttöä varten, tässä tarkoitettu seloste toimii ensisijaisesti rekisterinpitäjän, käsittelijän ja niiden edustajan sisäisenä työkaluna.

Vaikutusten arviointi ja ennakkokuuleminen

- Jos henkilötietojen käsittelyyn todennäköisesti kohdistuu korkea riski, on rekisterinpitäjän tehtävä tietosuojaa koskeva vaikutustenarviointi. Vaikutustenarvioinnissa arvioidaan käsittelyyn liittyvää riskiä ja rekisterinpitäjän keinoja vastata tähän riskiin.
- Vaikutustenarviointi on tehtävä erityisesti, jos käsittelyssä käytetään uutta teknologiaa tai jos käsitellään laajamittaisesti rikostuomioita tai rikkomuksia taikka erityisiin henkilötietoryhmiin kuuluvia tietoja. Vaikutustenarviointi on tehtävä myös tilanteissa, joissa on kyse järjestelmällisestä ja kattavasta automatisoituun päätöksentekoon perustuvasta arvioinnista sekä tilanteissa, joissa on kyse yleisölle avoimen alueen järjestelmällisestä ja laajamittaisesta valvonnasta.
- Jos vaikutustenarvioinnin perusteella henkilötietojen käsittelyyn liittyvä riskin taso on korkea, eikä rekisterinpitäjä ole toteuttanut toimenpiteitä riskin pienentämiseksi, on rekisterinpitäjän kuultava valvontaviranomaista ennen käsittelyn aloittamista (ennakkokuuleminen).

Rekisteröidylle toimitettavat tiedot

- Rekisterinpitäjän on suunniteltava toimintansa siten, että se voi pyynnöstä toimittaa rekisteröidylle henkilötietojen käsittelyä koskevat tiedot. Tietosuoja-asetuksen mukaan tiedot on pystyttävä esittämään tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa.
- Tarkoitettuja tietoja ovat ainakin rekisteriselosteet; tarkastusoikeuden kohteena olevat tiedot; tiedot henkilötietojen korjaamisesta, poistamisesta, rajoittamisesta, siirrosta; tiedot käsittelyn tai profiloinnin vastustamisesta ja ilmoitukset tietoturvaloukkauksista.
- Tiedot on toimitettava pääsääntöisesti kirjallisesti. Jos rekisteröity esittää pyynnön sähköisesti, tiedot on myös pääsääntöisesti toimitettava sähköisesti. Tiedot voidaan pyynnöstä antaa myös suullisesti, jos rekisteröidyn henkilöllisyydestä on voitu luotettavalla tavalla varmistua.

Rekisteröidylle toimitettavat tiedot

- Rekisteröidyn informoinnille ja toteutettaville toimenpiteille on asetettu määräaikoja. Tiedot annettava ilman aiheetonta viivytystä ja viimeistään kuukauden kuluessa pyynnön vastaanottamisesta. Määräaikaa voidaan tietyin edellytyksin jatkaa.
- Rekisteröidyn pyynnön perusteella toimitetut tiedot ja rekisterinpitäjän toimet rekisteröidyn oikeuksien toteuttamiseksi ovat pääsääntöisesti maksuttomia. Rekisterinpitäjä voi kuitenkin periä kohtuullisen maksun toimenpiteistään tai kieltäytyä pyynnön toteuttamisesta, jos rekisteröidyn pyyntö voidaan osoittaa kohtuuttomaksi tai ilmeisen perusteettomaksi. Kohtuuttomaksi tietopyynnöksi voitaisiin asetuksen mukaan katsoa esimerkiksi tapaukset, joissa rekisteröity tekisi toistuvia tietopyyntöjä ilmeisen perusteettomasti.

Tietosuojaselosteet

- Tietosuoja-asetuksessa on yksityiskohtaisesti kuvattu ne tiedot, jotka rekisterinpitäjän tulee toimittaa rekisteröidylle henkilötiedot saatuaan. Käytännössä kyse on rekisteriselosteesta tai vastaavanlaisesta dokumentaatiosta, jonka sisältö kuitenkin on laajempi kuin nykyisen henkilötietolain mukaisten rekisteriselosteiden tiedot.
- Tiedot on ilmoitettava rekisteröidylle, ellei asetuksesta muuta johdu. Tietoja ei esimerkiksi tarvitse antaa, jos rekisteröity on jo saanut nämä tiedot tai jos tiedot ovat salassa pidettäviä. Tietoja ei myöskään tarvitse antaa, jos tietojen toimittaminen osoittautuu mahdottomaksi tai vaatisi kohtuutonta vaivaa.
- Jos henkilötiedot saadaan rekisteröidyltä itseltään, rekisteröidylle ilmoitettavat tiedot toimitetaan, kun henkilötiedot kerätään. Jos henkilötiedot saadaan muulta lähteeltä, rekisterinpitäjän on toimitettava asetuksessa mainitut tiedot rekisteröidylle kohtuullisessa ajassa, mutta viimeistään kuukauden kuluessa.

Tietosuojaselosteen sisällöt

- rekisterinpitäjän ja tämän mahdollisen edustajan identiteetti ja yhteystiedot
- tapauksen mukaan mahdollisen tietosuojavastaavan yhteystiedot
- henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste
- kyseessä olevat henkilötietoryhmät;
- tapauksen mukaan henkilötietojen vastaanottajat tai vastaanottajaryhmät;
- tarvittaessa tieto siitä, että rekisterinpitäjä aikoo siirtää henkilötietoja kolmanteen maahan;
- henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit;
- rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut,

Tietosuojaselosteen sisältö

- rekisteröidyn oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten tietojen oikaisemista tai poistamista taikka käsittelyn rajoittamista ja vastustaa käsittelyä sekä oikeutta siirtää tiedot järjestelmästä toiseen;
- oikeus peruuttaa suostumus milloin tahansa tämän vaikuttamatta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen
- oikeus tehdä valitus valvontaviranomaiselle;
- mistä henkilötiedot on saatu sekä tarvittaessa se, onko tiedot saatu yleisesti saatavilla olevista lähteistä;
- automaattisen päätöksenteon, muun muassa profiloinnin olemassaolo

Oikeus saada pääsy tietoihin

- Rekisteröidyllä on kohtuullisin väliajoin oikeus saada pääsy henkilötietoihin, joita hänestä on kerätty sekä tietoihin hänen henkilötietojen käsittelyyn liittyen. ”Kohtuullista väliaikaa” ei ole asetuksessa tarkemmin määritelty.
- Kaikilla rekisteröidyillä olisi siten oltava oikeus tietää ja saada ilmoitus henkilötietojen käsittelyn tarkoituksista, käsittelyajasta, henkilötietojen vastaanottajista, käsiteltävien henkilötietojen automaattisen käsittelyn logiikasta ja kyseisen käsittelyn mahdollisista seurauksista sekä myös tietoa omista oikeuksistaan suhteessa rekisterinpitäjään.
- Rekisterinpitäjän pitää pyynnöstä ilmoittaa, käsitteleekö se kysyjää koskevia henkilötietoja. Jos henkilötietoja käsitellään, rekisteröidylle on annettava jäljennös rekisterissä olevista tiedoista, ellei ole lakisääteisiä perusteita olla antamatta pyydettyä tietoa.

Oikeus saada pääsy tietoihin

- Rekisteröidyn tiedonsaantioikeus koskee myös hänen henkilötietoihinsa kohdistuneita käsittelytoimia (kuka käsitellyt, mitä tietoja, milloin).
- Pyydetyt tiedot pitää ensisijaisesti luovuttaa sähköisessä muodossa.
- Rekisterinpitäjän on käytettävä kaikkia kohtuullisia keinoja tarkistaakseen sellaisen rekisteröidyn henkilöllisyyden, joka haluaa saada pääsyn tietoihin erityisesti verkkopalvelujen ja verkkotunnistetietojen yhteydessä. Rekisterinpitäjän täytyy riskilähtöistä lähestymistapaa käyttäen arvioida, millä tavalla kysyjän henkilöllisyyttä arvioidaan ja miten tiedot toimitetaan sähköisesti.

Oikeus tietojen oikaisemiseen

- Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot.
- Ottaen huomioon tarkoitukset, joihin tietoja käsiteltiin, rekisteröidyllä on oikeus saada puutteelliset henkilötiedot täydennettyä, esimerkiksi toimittamalla rekisterinpitäjälle lisäselvitystä.
- Rekisterinpitäjä on velvollinen ilmoittamaan tehdyistä henkilötietojen oikaisuista, poistoista tai käsittelyn rajoituksista jokaiselle, jolle henkilötietoja on luovutettu, paitsi jos tämä osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa.
- Rekisterinpitäjän on myös pyynnöstä ilmoitettava rekisteröidylle, keille tietoja on luovutettu.

Oikeus siirtää tiedot

- Jos henkilötietojen käsittelyn oikeusperusta on suostumus tai sopimuksen täytäntöönpano ja käsittely suoritetaan automaattisesti, rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle. Tiedot on toimitettava jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa.
- Rekisteröidyllä on myös oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle sen rekisterinpitäjän estämättä, jolle henkilötiedot on toimitettu.
- Kun rekisteröity käyttää tätä oikeuttaan, hänellä on oikeus saada henkilötiedot siirrettyä suoraan rekisterinpitäjältä toiselle, jos se on teknisesti mahdollista.
- Yleisesti koneluettava muoto tarkoittaa esimerkiksi, että rekisteröityi saa tietonsa linkkinä.

Vastustamisoikeus

- Rekisteröidyllä on oikeus vastustaa käsittelyä suoramarkkinointitarkoituksissa ja eräissä muissa tietosuoja-asetuksessa mainituissa tilanteissa, jolloin hänen henkilötietojaan ei saa enää käsitellä ko. tarkoituksissa.
- Asetus ei kokonaan kiellä profiloinnin käyttöä. Vahvana lähtökohtana on kuitenkin, että rekisteröidyillä on oikeus olla joutumatta profiloinnin kohteeksi.

Tietoturvaloukkauksesta ilmoittaminen

- Rekisterinpitäjällä on velvollisuus ilmoittaa tietoturvaloukkauksista tietosuojaviranomaiselle ja rekisteröidylle.
- Tietoturvaloukkauksella tarkoitetaan loukkausta, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.
- Rekisterinpitäjän on tehtävä loukkausta koskeva ilmoitus valvontaviranomaiselle mahdollisuuksien mukaan 72 tunnin kuluessa loukkauksen ilmitulosta, riippumatta siitä, onko loukkaus tapahtunut omassa vai käsittelijän toiminnassa. Rekisterinpitäjä voi jättää tietoturvaloukkausta koskevan ilmoituksen tekemättä ainoastaan, mikäli loukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä.

Tietoturvaloukkauksesta ilmoittaminen

- Henkilötietojen käsittelijän on ilmoitettava tietoturvaloukkauksista rekisterinpitäjälle ilman aiheetonta viivytystä loukkauksen tietoonsa saatuaan.
- Rekisterinpitäjä on velvollinen ilmoittamaan henkilötietojen tietoturvaloukkauksesta myös rekisteröidyille, jos loukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille.

Oikeus tulla unohdetuksi

- Rekisteröidyllä on oikeus vaatia tietojensa poistamista rekisteristä,
  - jos niitä ei enää tarvita käyttötarkoitukseen,
  - jos suostumus peruutetaan,
  - jos vastustetaan käsittelyä,
  - jos lainvastainen käsittely
- Jos rekisterinpitäjä on julkistanut henkilötietoja, sen on käytettävissä oleva teknologia ja toteuttamiskustannukset huomioon ottaen toteutettava kohtuulliset toimenpiteet ilmoittaakseen henkilötietoja käsitteleville rekisterinpitäjille poistamispyynnöstä.
- Oletusarvona on elinkaariajattelu.

Tietosuojavastaavan toiminta-ajatus

- Tietosuojavastaavan tehtävänä on organisaation erityisasiantuntijana auttaa rekisterinpitäjää tai tietojen käsittelijää saavuttamaan hyvä henkilötietojen käsittelytapa ja lainsäädännön edellyttämä korkea tietosuojan taso, joiden avulla voidaan turvata yksityiselämän suojan toteutuminen sekä rakentaa ja säilyttää luottamus rekisteröidyn ja rekisterinpitäjän välillä.

Tietosuojavastaava

- Jokaisen viranomaisen ja julkishallinnon elimen (sekä muidenkin organisaatioiden), on nimitettävä tietosuojavastaava.
- Tietosuojavastaava voi kuulua organisaation henkilöstöön tai hoitaa tehtäviään palvelusopimuksen perusteella.
- Konserni, samoin kuin useampi viranomainen tai julkishallinnon elin, voi nimittää yhteisen tietosuojavastaavan.
- Tietosuojavastaava voi tietosuojavastaavan tehtävän ohella suorittaa muita tehtäviä, mutta nämä tehtävät eivät saa aiheuttaa intressiristiriitoja. Tietosuojavastaavan on oltava riippumaton eikä hän saa ottaa vastaan ohjeita tehtäviensä hoitamisen yhteydessä. Tietosuojavastaava raportoi suoraan rekisterinpitäjän tai henkilötietojen käsittelijän ylimmälle johdolle.
- Nimitettäessä tietosuojavastaavaa on otettava huomioon henkilön ammattipätevyys ja erityisesti asiantuntemus tietosuojalainsäädännöstä ja alan käytänteistä.

Tietosuojavastaava

- Tietosuojavastaava on otettava asianmukaisesti ja riittävän ajoissa mukaan kaikkiin tietosuojakysymysten käsittelyyn. Hänelle on annettava riittävät resurssit sekä pääsy henkilötietoihin ja käsittelytoimiin. Hänellä on myös oikeus asiantuntemuksensa ylläpitämiseen esim. koulutuksiin osallistumalla.
- Rekisterinpitäjä tai henkilötietojen käsittelijä ei saa erottaa tai rangaista tietosuojavastaavaa sen vuoksi, että hän on hoitanut tehtäviään tietosuojavastaavana.
- Tietosuojavastaava antaa tietosuojaan liittyen tietoja neuvoja sekä työnantajalleen että muille työntekijöille. Hän seuraa tietosuoja-asetuksen noudattamista ja hänen vastuulleen kuuluu myös tietosuojan tietoisuusohjelman rakentaminen ja kouluttaminen henkilöstölle. Tietosuojavastaava toimii yhteistyössä valvontaviranomaisten kanssa.
- Tietosuojavastaava ei ole vastuussa henkilötietojen käsittelyn lainmukaisuudesta, vaan vastuussa on organisaation johto.

Tietosuojavastaavan nimittäminen

- Tietosuojavastaava on oltava nimitettynä 25.5.2018. Hyvä olisi hoitaa asia jo aiemmin.
- Seurakuntien ja seurakuntayhtymien on nyt harkittava, miten järjestetään tietosuojavastaavan tehtävät.
- Tietosuojavastaavan tehtäväkokonaisuuden pohdinnassa on syytä ottaa huomioon, että alussa tehtäviä on enemmän, kun organisaation tietosuojan tilanne käydään läpi. Jatkossa tehtävät vähenevät selvästi.
- Jokaisen seurakunnan ei kannata hoitaa asiaa yksin, vaan olisi hyvä pohtia yhteisiä ratkaisuja.

Kansallinen valvontaviranomainen

- Tietosuoja-asetuksessa tarkoitettuna kansallisena valvontaviranomaisena oikeusministeriön yhteydessä on tietosuojavaltuutettu.
- Tietosuojavaltuutetulla on toimisto, jossa on yksi tai useampi apulaistietosuojavaltuutettu sekä tarpeellinen määrä tietosuojavaltuutetun tehtäväalaan perehtyneitä esittelijöitä ja muuta henkilöstöä.
- Tietosuojavaltuutetun ja apulaistietosuojavaltuutetun nimittää valtioneuvosto viideksi vuodeksi kerrallaan.
- Tietosuojavaltuutetun toimistossa on asiantuntijalautakunta, jonka tehtävänä on tietosuojavaltuutetun pyynnöstä antaa lausuntoja henkilötietojen käsittelyä koskevan lainsäädännön soveltamiseen liittyvistä merkittävistä kysymyksistä.

Kansallinen valvontaviranomainen

- Rekisteröidyllä on oikeus saattaa asia tietosuojavaltuutetun käsiteltäväksi, jos rekisteröity katsoo, että häntä koskevien henkilötietojen käsittelyssä rikotaan sitä koskevaa lainsäädäntöä.
- Tietosuojavaltuutettu voi asettaa päätöksensä ja tämän tietojen luovuttamista koskevan määräyksensä tehosteeksi uhkasakon. Uhkasakon asettamisesta ja tuomitsemisesta maksettavaksi säädetään uhkasakkolaissa (1113/1990).
- Tietosuojavaltuutetun päätökseen saa hakea muutosta valittamalla hallinto-oikeuteen.

Sopimusvaatimukset

- Jos rekisterinpitäjä ja henkilötietojen käsittelijä ovat eri tahoja, niiden välillä on oltava kirjallinen sopimus. Sopimuksessa vahvistetaan mm. käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät ja rekisterinpitäjän velvollisuudet ja oikeudet.
- Rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöön panemiseksi niin, että käsittely täyttää tietosuoja-asetuksen vaatimukset.
- Esimerkiksi tarjouskilpailussa on toimittajan valinnassa kiinnitettävä huomiota toimittajan mahdollisuuksiin toteuttaa tietosuoja-asetuksen ja rekisterinpitäjän asettamia tietosuojavaatimuksia.

Vahingonkorvaus

- Henkilöllä, jolle on aiheutunut tietosuoja-asetuksen rikkomisen vuoksi vahinkoa, on oikeus saada täysi korvaus vahingosta joko rekisterinpitäjältä tai henkilötietojen käsittelijältä.
- Rekisterinpitäjällä on lähtökohtaisesti ns. ankara vastuu ja henkilötietojen käsittelijän vastuu on toissijaista. Käsittelijä on vastuussa vahingosta vain, jos se ei ole noudattanut tietosuoja-asetuksessa käsittelijälle nimenomaisesti asetettuja velvoitteita tai jos se ei ole noudattanut rekisterinpitäjän lainmukaista ohjeistusta.

Hallinnollinen seuraamusmaksu

- Rekisteröidylle suoritettavan vahingonkorvauksen lisäksi rekisterinpitäjä ja henkilötietojen käsittelijä voivat joutua maksamaan hallinnollisen seuraamusmaksun tietosuoja-asetuksen rikkomisen perusteella.
- Seuraamusmaksua ei voida määrätä valtion viranomaisille, valtion liikelaitoksille, kunnallisille viranomaisille, itsenäisille julkisoikeudellisille laitoksille, eduskunnan virastoille eikä tasavallan presidentin kanslialle. Tähän joukkoon kuulunee myös ev.lut. kirkko ja sen seurakuntataloudet.
- Hallinnollisen sakon määrä voi olla korkeintaan 20 000 000 euroa tai 4% yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

Miten valmistautua?

- Organisaatiossa on sen toiminnan näkökulmasta selvitettävä asetuksen edellyttämät muutokset.
- On kartoitettava henkilötietojen käsittelyyn liittyvien prosessien tila ja kehittämistarpeet sekä saattaa toiminnot, prosessit ja sopimukset sellaiseen tilaan, että ne vastaavat asetuksessa säädettyjä ehtoja.
- On kartoitettava, mitä henkilörekisterejä organisaatiossa on.
- On tarkistettava sopimustilanne palveluntuottajien / alihankkijoiden / toimittajien kanssa.
- On dokumentoitava tietosuojatyö.
- On tehtävä riskiarvio, johon kuuluvat mm. tietojärjestelmien muutostarpeet, sopimusvastuut, sanktio- ja vahingonkorvauksiin liittyvät riskit
- On huolehdittava henkilöstön osaamisesta, esimerkiksi koulutusten tai sisäisten ohjeiden avulla.
- On nimitettävä tietosuojavastaava.

Rekisterinpitäjän osoitusvelvollisuuden täyttämisen dokumentaatio

- tietosuojapolitiikka
- henkilötietojen käsittelyä koskevat kirjalliset ohjeet
- tietosuojatyön prosessikuvaukset
- rekisteri- eli tietosuojaselosteet, rekisteröidyille
- seloste käsittelytoimista valvontaviranomaiselle