Tietosuoja-asetuksen sudenkuopat

Betonin kesäseminaari 7.6.2018

Niina Harjunheimo, EK, asiantuntija

Mikä tietosuoja-asetus?

Tietosuoja-asetus = ”uusi henkilötietolaki”

Yleinen tietosuoja-asetus 2016/679	• Henkilötietojen suojaa koskeva yleissäädös • Tuli sovellettavaksi sellaisenaan 25.5.2018
Kansallinen tietosuojalaki (HE 9/2018)	• Tietosuoja-asetusta täydentävä kansallinen yleislaki • Tarkoitus tulla voimaan mahdollisimman pian
Kansallinen erityislainsäädäntö (uudistustyö kesken)	• Kansallinen erityislainsäädäntö henkilötietojen suojasta arvioitava tietosuoja-asetuksen valossa ja tarvittaessa uudistettava (mm. laki yksityisyyden suojasta työelämässä)

Mistä tietosuoja-asetuksella säädetään?

- Asetus määrittää:
  - mikä tieto on henkilötietoa eli minkä kaiken tiedon käsittelyssä on noudatettava asetuksen sääntelyä
  - millä perusteilla henkilötietoja voi käsitellä
  - mitä velvollisuuksia henkilötietojen käsittelyyn liittyy
  - mitkä ovat rekisteröityjen eli niiden henkilöiden, joiden tietoja käsitellään, oikeudet
  - miten asetusta valvotaan ja mitkä ovat seuraamukset asetuksen sääntelyn rikkomisesta

Milloin tietosuoja-asetusta on sovellettava?

- Asetusta sovelletaan *henkilötietojen käsittelyyn*, joka on osittain tai kokonaan automaattista, sekä manuaaliseen käsittelyyn, jos henkilötiedot muodostavat rekisterin osan tai niiden on tarkoitus muodostaa rekisterin osa.

  - Henkilötieto = tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, kuten esimerkiksi asiakkaaseen tai työntekijään, liittyvä tieto (esim. nimi, henkilötunnus, puhelinnumero tai sijaintitieto)
  - Käsittelyä on esimerkiksi tietojen kerääminen, tallentaminen, säilyttäminen, muokkaaminen, luovuttaminen tai tuhoaminen

- Tunnistettu tai tunnistettavissa oleva luonnollinen henkilö, johon tiedot liittyvät, on *rekisteröity*

Ketä tietosuoja-asetus velvoittaa?

- *Rekisterinpitäjä* vastaa siitä, että henkilötietojen käsittelyssä noudatetaan asetuksen sääntelyä. *Henkilötietojen käsittelijä* vastaa oman käsittelynsä asetuksenmukaisuudesta.

  - Rekisterinpitäjä = luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoituksen ja keinot. Esimerkiksi yritys on rekisterinpitäjä asiakkaidensa ja työntekijöidensä henkilötietojen käsittelyn osalta.
  - Henkilötietojen käsittelijä = luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Henkilötietojen käsittelijöitä ovat esimerkiksi yritykset, jotka tarjoavat palkkahallinnon palveluja tai pilvipalveluja, joissa säilytetään ja käsitellään toisen yrityksen asiakastietoja.

Tietosuoja-asetuksen keskeiset vaatimukset

Periaatteet = käsittelyn keskeiset pelisäännöt

- Tiedot kerättävä tiettyä ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla
  - = Määritettävä, mitä tarkoituksia varten henkilötietoja käsitellään (esim. asiakassuhteen hoitamiseksi, työsuhteisiin liittyvien asioiden hoitamiseksi) ja huolehdittava, ettei tietoja käsitellä tai luovuteta näiden tarkoitusten kanssa yhteensopimattomiin tarkoituksiin.

- Tietojen oltava asianmukaisia ja rajoitettuja siihen, mikä on tarpeellista niihin tarkoituksiin, joita varten niitä käsitellään
  - = Tarkoitusten kannalta tarpeellisia henkilötietoja saa käsitellä, turhia henkilötietoja ei ole sallittua käsitellä.

- Tiedot säilytettävä muodossa, josta rekisteröity on tunnistettavissa vain niin kauan kuin on tarpeen käsittelyn tarkoitusten toteuttamista varten
  - = Huolehdittava, ettei sellaisia henkilötietoja säilytetä, jotka eivät enää ole tarpeellisia!

Periaatteet = käsittelyn keskeiset pelisäännöt

- Tietojen oltava täsmällisiä ja tarvittaessa päivitettyjä

- Tietoja käsiteltävä tavalla, jolla varmistetaan henkilötietojen käsittelyn asianmukainen turvallisuus ja henkilötietojen suojaaminen

- Tietoja käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
  - = Käsittelylle oltava aina asetuksessa tai kansallisessa laissa määritetty käsittelyperuste (mm. rekisterinpitäjän oikeutettu etu tai suostumus) ja henkilötietojen käsittelystä annettava selkeätä tietoa rekisteröidyille.

Laillisen käsittelyn perusteet

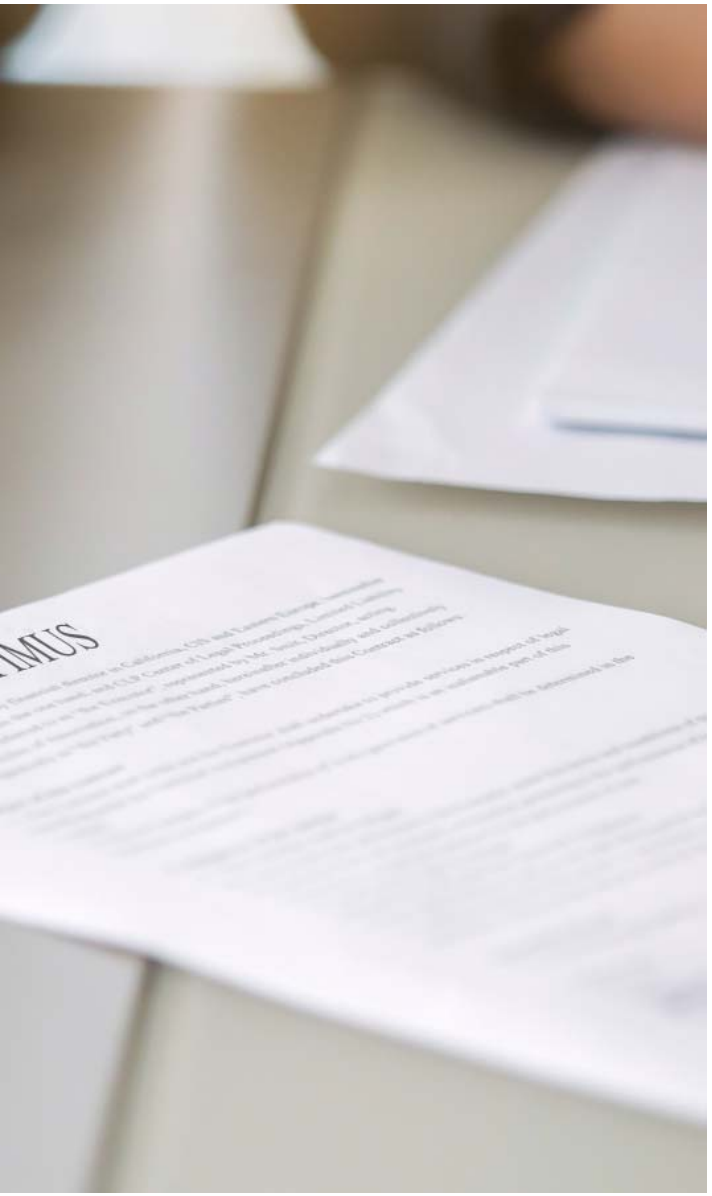
- Henkilötietoja voi käsitellä seuraavilla perusteilla:
  - rekisteröidyn suostumus
  - rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu
  - sopimuksen täytäntöönpano
  - lakisääteisen velvoitteen noudattaminen
  - yleistä etua koskevan tehtävän suorittaminen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen
  - rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaaminen

- Esimerkiksi asiakastietojen käsittely mahdollista perustaa rekisterinpitäjän oikeutettuun etuun, rekisteröidyn suostumukseen tai sopimukseen. Jos perusteena sopimus tai oikeutettu etu, suostumusta ei tarvita!

Erityiset henkilötietoryhmät

- Erityisiä henkilötietoryhmiä saa käsitellä vain asetuksessa tai kansallisessa laissa määritetyin poikkeusehdoin, kuten esim. nimenomaisen suostumuksen perusteella tai jos käsittely johtuu välittömästi rekisterinpitäjälle laissa säädetystä tehtävästä.

- Erityiset henkilötietoryhmät:
  - tiedot, joista ilmenee rotu tai etninen alkuperä,
  - tiedot, joista ilmenee poliittinen mielipide, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys,
  - terveyttä koskevat tiedot jne.



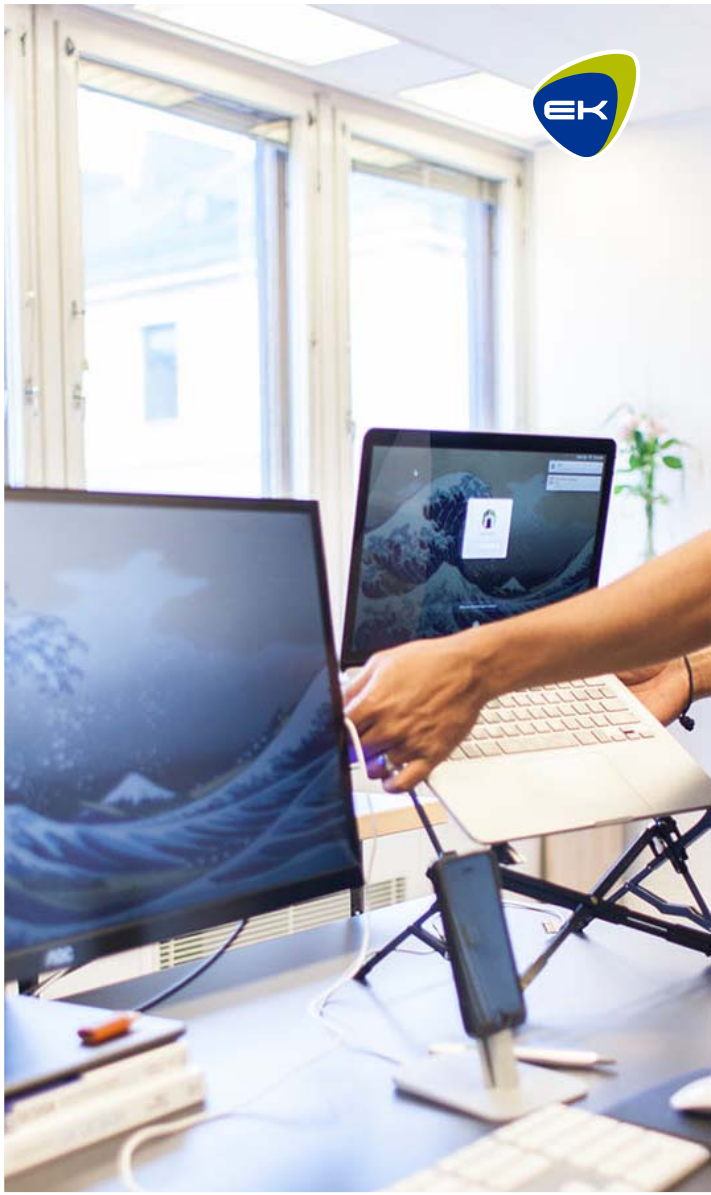
Uusi velvoite: osoitusvelvollisuus

- Rekisterinpitäjän kyettävä osoittamaan periaatteiden ja asetuksen sääntelyn noudattaminen

- Velvoitteen täyttämiseksi tärkeätä mm.
  - käsittelytoimien dokumentointi
  - sisäinen ohjeistus ja
  - tarvittaessa sisäinen koulutus henkilötietojen käsittelystä

Seloste käsittelytoimista

- Rekisterinpitäjän laadittava ja säilytettävä seloste käsittelytoimista. Selosteeseen sisällytettävä seuraavat tiedot:
  - rekisterinpitäjän nimi ja yhteystiedot
  - käsittelyn tarkoitukset
  - kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä
  - tietojen vastaanottajien ryhmät, joille tietoja on luovutettu tai luovutetaan
  - tarvittaessa tiedot henkilötietojen siirtämisestä EU-alueen ulkopuolelle
  - mahdollisuuksien mukaan suunnitellut määräajat eri tietoryhmien poistamiselle
  - mahdollisuuksien mukaan yleinen kuvaus käsittelyn turvallisuutta koskevista teknisistä ja organisatorisista turvatoimista



Käsittelyn turvallisuus

- Rekisterinpitäjän toteutettava henkilötietojen käsittelyyn liittyvää *riskiä vastaavan turvallisuustason* varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet (mm. käyttäjätunnukset vain tietyillä henkilöillä, salasanat).

- Rekisterinpitäjän lisäksi toteutettava toimenpiteet sen varmistamiseksi, että henkilöt, joilla on pääsy henkilötietoihin, käsittelevät niitä vain rekisterinpitäjän ohjeiden mukaisesti.

Ilmoitukset tietoturvaloukkauksista

Viranomaiselle

- ilmoitus tehtävä, jos loukkaus todennäköisesti johtaa *riskeihin* rekisteröidyn oikeuksille
- ilmoitus tehtävä ilman aiheetonta viivytystä, viimeistään 72 tunnin kuluttua havaitsemisesta
- ilmoituksessa mm. kuvattava loukkaus, loukkauksen seuraukset sekä toimenpiteet, joita toteutettu loukkauksen johdosta

Rekisteröidylle

- ilmoitus tehtävä ilman aiheetonta viivytystä, jos loukkaus todennäköisesti johtaa *korkeaan riskiin* rekisteröidyn oikeuksille
- poikkeukset: toteutettu asianmukaiset suojatoimenpiteet ja toimenpiteitä sovellettu loukkauksen kohteena oleviin tietoihin tai loukkauksen johdosta toteutettu toimenpiteet, joiden vuoksi korkea riski ei enää toteudu

- Tietoturvaloukkaus: tapahtuma, jonka seurauksena henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai pääsy tietoihin.

Sopimukset ulkoistuksista

- Jos henkilötietojen käsittelyä ulkoistetaan (esim. palkka-hallinto), henkilötietojen käsittelijöiden kanssa laadittava kirjallinen sopimus. Sopimukseen sisällytettävä mm. seuraavia tietoja:
  - käsittelyn kohde ja kesto
  - käsittelyn luonne ja tarkoitus
  - henkilötietojen tyyppi ja rekisteröityjen ryhmät
  - rekisterinpitäjän velvollisuudet

- Lisäksi sopimuksessa määritettävä mm. että:
  - käsittelijä käsittelee henkilötietoja ainoastaan rekisterinpitäjän antamien ohjeiden mukaisesti
  - käsittelijä toteuttaa asetuksen edellyttämät käsittelyn turvallisuutta koskevat toimenpiteet.

Henkilötietojen siirrot EU:n ulkopuolelle

- Henkilötietojen siirrot EU:n ulkopuolelle ovat sallittuja asetuksessa määritetyillä perusteilla.

- Henkilötietoja voidaan siirtää EU:n ulkopuolelle mm. seuraavilla perusteilla:
  - tietosuojan riittävyyttä koskeva komission päätös
  - yritystä koskevat sitovat säännöt, jotka valvontaviranomainen on hyväksynyt
  - komission hyväksymät tietosuojaa koskevat mallisopimuslausekkeet
  - valvontaviranomaisen vahvistamat ja komission hyväksymät tietosuojaa koskevat vakiolausekkeet
  - rekisterinpitäjän tai henkilötietojen käsittelijän ja tietojen vastaanottajan väliset sopimuslausekkeet, jotka valvontaviranomainen on hyväksynyt

- Henkilötietojen siirto on sallittua myös mm. jos rekisteröity on antanut siirtoon nimenomaisen suostumuksen sen jälkeen, kun hänelle on ilmoitettu, että siirto voi aiheuttaa rekisteröidylle riskejä.

Rekisteröityjen oikeudet

Informaatio henkilötietojen käsittelystä

- Rekisteröidyille annettava selkeää ja helposti ymmärrettävää informaatiota henkilötietojen käsittelystä riittävän aktiivisella tavalla
  - keräyshetkellä, jos tiedot kerätään rekisteröidyiltä itseltään
  - muutoin kohtuullisen ajan kuluessa ja viimeistään silloin, kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran, jos tietoja käytetään viestintään rekisteröidyn kanssa.

- Informointi tehtävä riittävän aktiivisella tavalla!

Informaatio henkilötietojen käsittelystä

- Tietoihin sisällytettävä seuraavat tiedot:
  - rekisterinpitäjän nimi ja yhteystiedot
  - käsittelyn tarkoitukset ja oikeusperuste, ml. oikeutettu etu, jos käsittely perustuu siihen
  - mitä henkilötietoryhmiä käsittely koskee ja mistä lähteistä tietoja saadaan
  - jos tietoja luovutetaan, tietojen vastaanottajien ryhmät
  - tarvittaessa tiedot henkilötietojen siirtämisestä EU:n ulkopuolelle
  - tietojen säilytysaika tai jos se ei ole mahdollista, ajan määrittämiskriteerit
  - tietoa rekisteröidyn oikeuksista sekä oikeudesta peruuttaa suostumus
  - tietoa rekisteröidyn oikeudesta tehdä valitus valvontaviranomaiselle
  - tarvittaessa tieto automaattisesta päätöksenteosta, ml. profiloinnista, sekä siihen liittyvästä logiikasta

Rekisteröidyn tarkastusoikeus

- Rekisteröidyllä pääsääntöisesti oikeus saada tietää, käsitteleekö rekisterinpitäjä häntä koskevia henkilötietoja, ja jos käsittelee, oikeus tarkistaa mitä häntä koskevia tietoja rekisterinpitäjä käsittelee.

- Tarkastusoikeuden toteuttamisen pelisäännöt:
  - ei määrämuotoa pyynnön esittämiselle
  - rekisteröity tunnistettava ja mahdollista pyytää lisätietoa henkilöllisyyden vahvistamiseksi, jos perusteltu syy epäillä pyynnön esittäneen henkilöllisyyttä
  - mahdollista pyytää täsmentämään riittävällä tavalla, mitä tietoa tai käsittelytoimia pyyntö koskee
  - pyyntöön reagoitava kuukauden sisällä (määräaikaa mahd. pidentää kahdella kuukaudella, jos pyyntö monimutkainen tai pyyntöjä paljon)
  - oikeuden toteuttamisen lähtökohtana maksuttomuus (mahdollista periä maksu tai kieltäytyä toteuttamasta pyyntöä, jos pyynnöt perusteettomia tai kohtuuttomia)
  - jäljennös tiedoista annettava lähtökohtaisesti kirjallisesti tai sähköisesti
  - oikeus ei saa vaikuttaa haitallisesti muiden oikeuksiin ja vapauksiin (mm. tarpeeseen suojata liikesalaisuudet) – rekisterinpitäjän arvioitava!

Kokonaiskuva rekisteröityjen oikeuksista

Tarkastusoikeus

- Oikeus saada rekisterinpitäjältä vahvistus käsitelläänkö rekisteröityä koskevia henkilötietoja.
- Jos henkilötietoja käsitellään, oikeus saada tieto mm. käsittelyn tarkoituksista ja kyseessä olevista henkilötietojen ryhmistä sekä jäljennös käsiteltävistä henkilötiedoista

Oikeus tietojen oikaisemiseen

- Oikeus vaatia, että rekisterinpitäjä oikaisee rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot ja täydentää puutteelliset henkilötiedot

Oikeus tietojen poistamiseen

- Oikeus vaatia, että rekisterinpitäjä poistaa rekisteröityä koskevat henkilötiedot mm. jos tietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai rekisteröity peruuttaa suostumuksen eikä käsittelyyn ole muuta laillista perustetta
- Jos rekisterinpitäjä on julkistanut tiedot ja velvollinen poistamaan ne, sen toteutettava kohtuulliset toimenpiteet ilmoittaakseen tietoja käsitteleville rekisterinpitäjille, että rekisteröity on pyytänyt kyseisiä rekisterinpitäjiä poistamaan henkilötietoihin liittyvät linkit ja jäljennökset

Kokonaiskuva rekisteröityjen oikeuksista

Oikeus käsittelyn rajoittamiseen

- Oikeus vaatia käsittelyn rajoittamista mm. jos rekisteröity kiistää tietojen paikkaansa pitävyyden (kunnes ehditty varmistaa tiedon oikeellisuus) tai käsittely on lainvastaista, mutta rekisteröity kieltää tietojen poistamisen ja vaatii sen sijaan rajoitusta

Oikeus siirtää tiedot

- Oikeus saada henkilötiedot, jotka rekisteröity toimittanut rekisterinpitäjälle, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, ja siirtää tiedot toiselle rekisterinpitäjälle, jos käsittely perustuu *suostumukseen tai sopimukseen* ja käsittely suoritetaan automaattisesti
- Em. tilanteissa oikeus saada henkilötiedot siirrettyä suoraan rekisterinpitäjältä toiselle, jos se teknisesti mahdollista

Vastustamisoikeus

- Oikeus henkilökohtaiseen erityiseen tilanteeseen liittyvällä perusteella vastustaa henkilötietojen käsittelyä, ml. profilointia, joka perustuu rekisterinpitäjän oikeutettuun etuun, yleistä etua koskevan tehtävän suorittamiseen tai julkisen vallan käyttämiseen
- Jos henkilötietoja käsitellään suoramarkkinointia varten, rekisteröidyllä oikeus vastustaa käsittelyä milloin tahansa

Valvontaviranomainen ja hallinnolliset sakot

- Asetus antaa valvontaviranomaiselle (tietosuojavaltuutetulle) nykyistä vahvemmat valvontatoimivaltuudet. Valvontaviranomaisen mahdollista mm.
  - määrätä rekisterinpitäjä saattamaan käsittelytoimet asetuksen mukaiseksi tarvittaessa tietyllä tavalla ja tietyn määräajan kuluessa
  - asettaa väliaikainen tai pysyvä rajoitus käsittelylle, ml. käsittelykielto.

- Hallinnollinen sakko mahdollista määrätä valvontaviranomaisen muiden toimenpiteiden lisäksi tai sijaan. Päätettäessä sakon määräämisestä ja määrästä huomioitava mm. asetuksen säännösten rikkomisen luonne, vakavuus, kesto sekä tahallisuus tai tuottamuksellisuus.

- Sakkojen enimmäismäärät:
  - 10 miljoonaa euroa tai 2 % maailmanlaajuisesta vuosittaisesta kokonaisliikevaihdosta tai
  - 20 miljoonaa euroa tai 4 % maailmanlaajuisesta vuosittaisesta kokonaisliikevaihdosta

Yhteenveto: henkilötietojen käsittelyn pelisäännöt

Henkilötietojen käsittelyn pelisäännöt

Ennen käsittelyn aloittamista

- Määritä käsittelyn tarkoitukset, tarpeelliset tiedot, tietojen säilyttämis- ja hävittämiskäytännöt sekä käsittelyn peruste
- Suunnittele riittävät toimet turvallisuuden varmistamiseksi
- Tarvittaessa tee vaikutustenarviointi ja nimitä tietosuojavastaava
- Laadi seloste ja mahdollinen muu dokumentointi sekä ohjeistus henkilötietojen käsittelylle
- Jos ulkoistat käsittelyä, laadi asetuksen mukainen sopimus
- Kun keräät henkilötietoja, informoi rekisteröityjä asetuksen mukaisesti

Käsittelyn aikana

- Pidä tiedot ajantasaisina ja oikeina ja hävitä määritettyjen käytäntöjen mukaisesti tarpeettomat tiedot
- Ylläpidä käsittelyn turvallisuutta
- Huolehdi tarvittaessa ilmoitukset tietoturvaloukkauksista viranomaiselle ja rekisteröidylle
- Hallinnoi mahdollisia luovutuksia ja tietojen siirtoja EU:n ulkopuolelle
- Huolehdi, että voit osoittaa asetuksen noudattamisen (mm. ylläpidä dokumentointi sekä ohjeistus henkilötietojen käsittelylle)
- Ylläpidä rekisteröityjen oikeuksia (mm. tarkastusoikeus)

Käsittelyn perusteen lakattua

- Varmista henkilötietojen hävittäminen tai myöhempi hävitys, jos tietoja on säilytettävä pidempään

Tarkistuslista

Tarkistuslista

- Noudatetaanko organisaatiosi henkilötietojen käsittelyssä asetuksessa määritettyjä periaatteita? Vaikuttaako asetus tämänhetkisiin laillisen käsittelyn perusteisiin? Muista, että suostumus ei ole ainoa käsittelyn peruste!

- Käsitelläänkö organisaatiossasi erityisiä henkilötietoryhmiä (arkaluonteisia henkilötietoja)? Varmista, että käsittelylle löytyy peruste.

- Onko henkilötietojen käsittelyä koskeva dokumentaatio (ml. seloste käsittelytoimista, sisäinen ohjeistus) riittävän kattavaa ja ajan tasalla – tärkeätä uuden osoitusvelvollisuuden takia!

- Ovatko käsittelyn turvallisuutta ja tietojen suojaamista koskevat toimenpiteet riittävät? Onko organisaatiossasi mietitty prosessi mahdollisista tietoturvaloukkauksista ilmoittamista varten?

Tarkistuslista

- Onko mahdollisia henkilötietojen käsittelyn ulkoistuksia koskevia sopimuksia tarpeen päivittää? Siirretäänkö organisaatiosi käsittelemiä henkilötietoja EU:n ulkopuolelle?

- Annetaanko rekisteröidyille tarpeeksi selkeätä tietoa henkilötietojen käsittelystä riittävän aktiivisella tavalla – tärkeätä läpinäkyvyyden vaatimuksen takia!

- Pystytäänkö organisaatiossasi vastaamaan rekisteröityjen mahdollisiin pyyntöihin mm. henkilötietojen tarkastamisesta?

- Priorisoi ja huolehdi, että asetuksen vaatimukset huomioidaan jatkossa käsiteltäessä henkilötietoja ja mm. tehtäessä it-järjestelmiä koskevia hankintoja!

Lisätietoa

- EK:n nettisivut: www.ek.fi/tietosuoja
- Tietosuojavaltuutetun nettisivut: http://www.tietosuoja.fi

Kiitos!

niina.harjunheimo@ek.fi

p. 0400 154452