Kela|Fpa

Tietosuojavaatimusten perusteet yhteistyökumppanin esihenkilöille

– mitä tulee ottaa huomioon, kun käsitellään Kelan etuustietoja Kelmussa

Esitys on tuotettu yhteistyössä: Kela ja asianajaja Jukka Lång, Dittmar & Indrenius

Johdanto

Mitä tietosuoja on ja miksi se on tärkeää?

- Jokaisella on oikeus henkilötietojensa suojaan (Suomen perustuslain 10 §).
- Yksityisyyden suoja (>tietosuoja) on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä.
- Tietosuojasta säädetään EU:n yleisessä tietosuoja-asetuksessa sekä kansallisessa tietosuojalaissa.
- Tietosuoja osoittaa, **milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä**.
- Tietosuojan asianmukainen järjestäminen on paitsi lain edellytysten täyttämistä, myös osa **vastuullista toimintaa**.
- **Tietoturva** on yksi käytännön toimenpide, jolla pyritään tietosuojan toteutumiseen. Se on ennen kaikkea tiedon eheyden ja luottamuksellisuuden turvaamista teknisin ja organisatorisin keinoin.

Kela|Fpa

Tietosuojan peruskäsitteet

- **Henkilötietoja** ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön.
- **Henkilötietojen käsittelyä** ovat kaikki ne toimenpiteet, jotka kohdistuvat henkilötietoihin.
- **Rekisteröity** on henkilö, jota henkilötieto koskee.
- **Rekisterinpitäjäksi** kutsutaan henkilöä, yritystä, viranomaista tai yhteisöä, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjällä on kokonaisvastuu henkilötietojen käsittelystä.
  - Yhteistyökumppanit toimivat rekisterinpitäjinä käsitellessään Kelalta saatuja henkilötietoja.
- **Henkilötietojen käsittelijä** on taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.
  - Henkilötietojen käsittelijä toimii rekisterinpitäjän ohjeiden mukaisesti ja sen alaisuudessa.

Kela|Fpa

Yhteistyökumppanin tiedonsaantioikeus

- Yhteistyökumppanilla on oikeus vastaanottaa Kelalta henkilötietoja (mm. asiakkaiden etuustiedot) toimintansa asianmukaiseksi toteuttamiseksi.
- Tiedonsaantioikeus perustuu lainsäädäntöön
  - Yhteistyökumppanilla on oikeus saada erityislainsäädännön perusteella välttämättömät tiedot, joita se tarvitsee tehtäviensä hoitamiseen.
  - Viranomaisten välinen tietojen luovuttaminen tietojärjestelmien välillä teknisten rajapintojen avulla perustuu lakiin julkisen hallinnon tiedonhallinnasta 22 § (906/2019)
- Erityislait, esimerkiksi asiakastietolaki, mahdollistavat **välttämättömien tietojen** saannin Kelan etuustietopalvelu Kelmun kautta. Yhteistyökumppanin on varmistettava asiakkaiden yksityisyyden suoja saatujen tietojen osalta noudattamalla **tietosuoja-asetuksen asettamia velvoitteita**.
- Tietojen luovuttamista määritellään myös osapuolten välisessä **sopimuksessa Kelan etuustietojen luovuttamisesta teknisen käyttöyhteyden avulla.**

Kela|Fpa

Kelan luovuttamat tiedot ovat salassa pidettäviä. Yhteistyökumppani myöntää Suomi.fi-valtuuden työntekijöilleen vasta sen jälkeen, kun työntekijät ovat saaneet **riittävän ohjeistuksen tietosuojasta ja vähintään perehtyneet tähän Kelan materiaaliin.** Yhteistyökumppani sitoutuu valvomaan ja vastaamaan siitä, että sen palveluksessa olevat, käyttöoikeuden saaneet henkilöt, käyttävät tietojärjestelmää ja sen kautta saatuja tietoja osapuolten tekemän sopimuksen mukaisesti.

Kela|Fpa

Tietosuoja-asetuksen asettamat velvoitteet

- Yhteistyökumppanit käsittelevät Kelalta vastaanottamaansa henkilötietoa **rekisterinpitäjän asemassa**, ja niiden on huolehdittava:
  - Henkilötietojen käsittelyä koskevien **tietosuojaperiaatteiden** noudattamisesta ja noudattamisen osoittamisesta
  - Lainmukaisesta **käsittelyperusteesta**
  - **Rekisteröityjen oikeuksien** toteuttamisesta
  - Teknisten ja organisatoristen toimenpiteiden toteuttamisesta tietosuojan ja tietoturvan varmistamiseksi
  - Tietosuojaa koskevien toimintaperiaatteiden täytäntöönpanosta
    - Esimerkiksi sisäiset ohjeet, toimintamallit ja koulutusten järjestäminen

Tietosuojaperiaatteet

Tietosuojaperiaatteita on noudatettava aina, kun käsitellään henkilötietoja.

Rekisterinpitäjän on myös pystyttävä osoittamaan, että tietosuojaperiaatteet toteutuvat tehokkaasti henkilötietojen käsittelyssä.

Kela|Fpa

Mitä tietosuojaperiaatteita on?

Lainmukaisuus, kohtuullisuus ja läpinäkyvyys

Käyttötarkoitussidonnaisuus

Tietojen minimointi

Täsmällisyys

Säilytyksen rajoittaminen

Tietojen eheys ja luottamuksellisuus

Osoitusvelvollisuus

Tietosuojaperiaatteet 1/2

1. **Lainmukaisuus, kohtuullisuus ja läpinäkyvyys**
   - Henkilötietojen käsittelyn on täytettävä tietosuojalainsäädännössä asetetut vaatimukset. Käsittelyllä tulee olla lainmukainen peruste, ja sen on oltava asianmukaista ja kohtuullista suhteessa määritettyyn tarkoitukseen. Läpinäkyvyydellä tarkoitetaan, että rekisteröidylle on kerrottava henkilötietojen käsittelystä ja siihen liittyvistä oikeuksista selkeästi ja ymmärrettävällä tavalla ennen käsittelyä ja sen aikana.
2. **Käyttötarkoitussidonnaisuus**
   - Henkilötietoja saa käsitellä vain nimenomaista ja laillista tarkoitusta varten. Tietoja saa käyttää vain yhteistyökumppanin toimeenpantavaksi lainsäädännössä säädettyjen tehtävien hoitamiseen.
3. **Tietojen minimointi**
   - Vain niitä henkilötietoja, jotka ovat käsittelyn kannalta tarpeellisia saa käsitellä. Vain tarpeellisten tietojen katsominen kunkin asiakkaan kohdalla on yhteistyökumppanin sekä sen puolesta toimivan työntekijän vastuulla.
4. **Täsmällisyys**
   - Käsiteltävien henkilötietojen on oltava täsmällisiä ja päivitettyjä. Epätarkat ja virheelliset henkilötiedot on oikaistava tai poistettava viipymättä.

Kela|Fpa

Tietosuojaperiaatteet 2/2

5. Säilytyksen rajoittaminen

- Henkilötietoja saa säilyttää vain niin kauan kuin se on tarpeen tietojen käyttötarkoitusta varten. Rekisterinpitäjän on suunniteltava ja pystyttävä perustelemaan käytössä oleva säilytysaika. Henkilötietojen säilytysajat on dokumentoitava.

6. Tietojen eheys ja luottamuksellisuus

- Henkilötietojen käsittelyn on oltava luottamuksellista ja turvallista. Rekisterinpitäjän on arvioitava mahdollisia riskejä, organisaation tietosuoja- ja tietoturvaohjeistuksen tasoa sekä henkilötietojen teknistä suojausta. Katseluoikeus luovutettaviin tietoihin toteutetaan sopimuksen mukaisesti vahvaan tunnistautumiseen perustuen (sopimuksen voimaantulohetkellä käytetään Suomi.fi –tunnistusta).

7. Osoitusvelvollisuus

- Rekisterinpitäjän on kyettävä osoittamaan, että se noudattaa tietosuojasäännöksiä, ja se on huomioitava jo henkilötietojen käsittelyvaiheessa. Osoitusvelvollisuuden laajuus riippuu organisaation koosta, henkilötietojen määrästä ja siitä, minkälaisia henkilötietoja reksiterinpitäjä käsittelee. Jos rekisterinpitäjä ei pysty osoittamaan noudattavansa tietosuojavelvoitteita, voi siitä seurata hallinnollisia seuraamuksia.

Kela|Fpa

Osoitus ja informointi – Rekisteröidyille annettavat tiedot

Jotta rekisterinpitäjä osoittaa noudattavansa tietosuojavelvoitteita, sen on ilmoitettava rekisteröidyille seuraavat asiat:

- **Mikä** organisaatio vastaa käsittelystä
- **(Ketkä** käsittelevät tietoja)
- **Mitkä** ovat organisaation & sen tietosuojavastaavan yhteystiedot
- **Miksi** (tarkoitus) tietoja käsitellään
- **Ketä** tiedot koskevat
- **Mitä** tietoja käsitellään
- **Mistä** tiedot saadaan
- **Kauanko** tietoja säilytetään
- **Miten** rekisteröityjä profiloidaan / päätöksiä automatisoidaan (logiikka)
- **Mitä** haittaa käsittelystä on yksittäiselle henkilölle
- **Onko** pyydetyt tiedot pakko antaa organisaatiolle
- **Kenelle** (organisaatiot) tietoja annetaan
- **Missä** maassa käsittely toteutetaan
- **Missä** maassa tietoja säilytetään
- **Mikä** käsittelyperuste oikeuttaa käsittelyn
- **Mitä** oikeuksia rekisteröidyillä on (Mitä yksittäisille henkilöille on tarkoitus/ pitää kertoa? Miten?)

Kela|Fpa

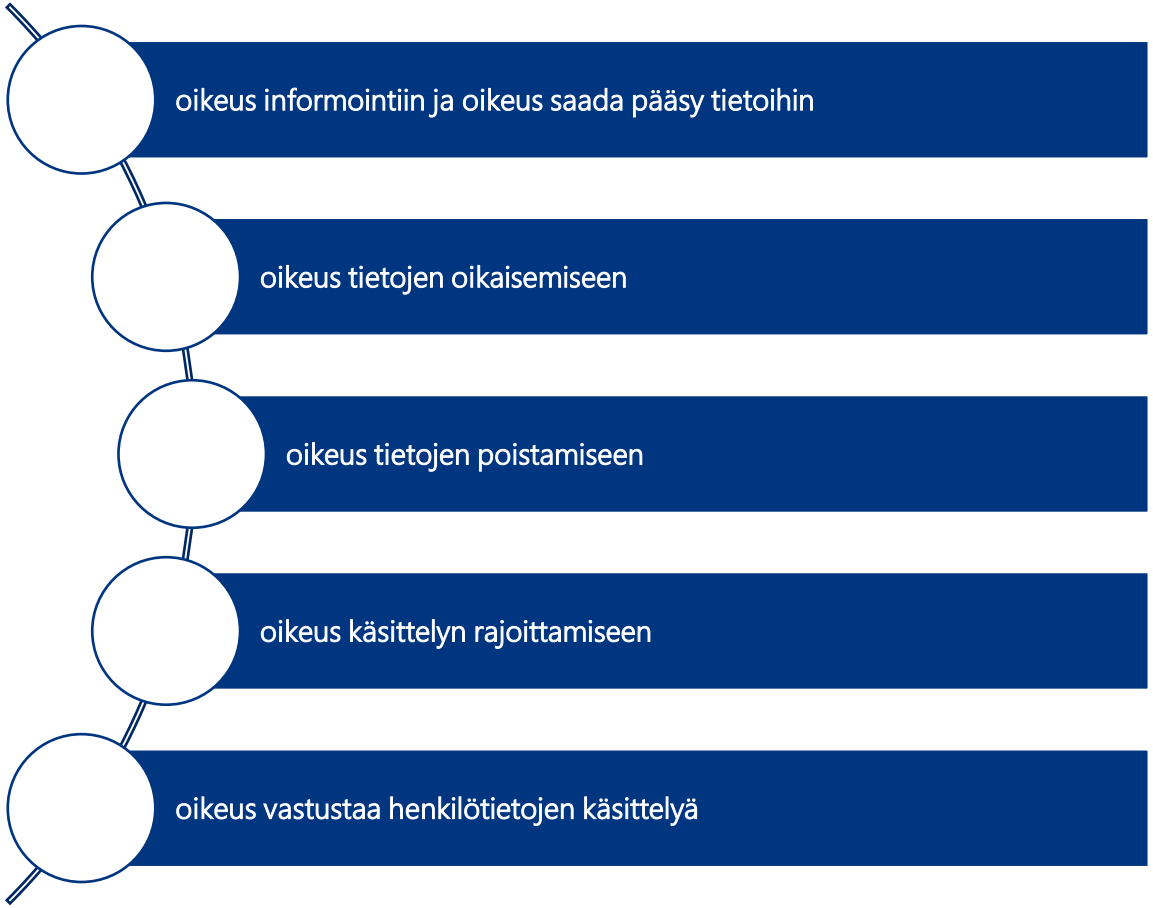
Käsittelyperusteet

- Rekisterinpitäjä saa käsitellä henkilötietoja vain, kun käsittelylle on lainmukainen peruste.
- Käsittelyperuste rajaa niitä tarkoituksia, joihin rekisterinpitäjä voi käsitellä (ml. luovuttaa) tietoja.
- Yhteistyökumppani ei saa luovuttaa saamiaan tietoja edelleen, mikäli lainsäädäntö ei muuta edellytä.
- Käsittelyperuste on tunnistettava ja määriteltävä ennen käsittelyn aloittamista, kaikkiin eri käsittelytoimiin liittyen.
- Käsittelyperustetta ei voi vaihtaa kesken käsittelyn.

Rekisteröidyn oikeudet

Kela|Fpa

Rekisteröidyn oikeuksien toteuttaminen



- Rekisterinpitäjän on toteutettava asianmukaiset toimenpiteen rekisteröityjen oikeuksien toteuttamiseksi.

- Oikeuksien käyttämistä on myös helpotettava suunnittelemalla ja toteuttamalla niiden soveltamisen mukaiset käytännön menettelyt.

Kela|Fpa

Rekisteröidyn oikeudet käytännössä

- **Oikeus informointiin ja oikeus saada pääsy tietoihin**
  - Rekisteröidyllä on oikeus tietää käsitelläänkö hänen henkilötietoja vai ei. Jos tietoja käsitellään, rekisteröidylle on esitettävä selvitys käsiteltävistä henkilötiedoista.
- **Oikeus tietojen oikaisemiseen**
  - Rekisteröidyllä on oikeus saada virheelliset tai puutteelliset henkilötiedot oikaistua.
- **Oikeus tietojen poistamiseen**
  - ”Oikeus tulla unohdetuksi” tarkoittaa, että rekisteröity voi pyytää henkilötietojensa poistamista silloin, kun pakottavaa syytä niiden jatkokäsittelylle ei ole.
- **Oikeus käsittelyn rajoittamiseen**
  - Rekisteröidyllä on oikeus rajoittaa henkilötietojensa käsittelyä tietyissä tilanteissa. Kun käsittelyä rajoitetaan, rekisterinpitäjällä tai henkilötietojen käsittelijällä on oikeus säilyttää henkilötietoja, muttei jatkaa niiden käsittelyä.
- **Oikeus vastustaa tietojen käsittelyä**
  - Rekisteröidyllä voi olla tietyissä tilanteissa oikeus vastustaa henkilötietojensa käsittelyä eli pyytää, että niitä ei käsiteltäisi ollenkaan. Käsittelyä voi vastustaa henkilökohtaisen erityisen tilanteen perusteella.

Kela|Fpa

Rekisteröidyn oikeuksien käyttäminen

- Rekisterinpitäjän on rekisteröidyn oikeuksista informoimisen lisäksi mahdollistettava näiden oikeuksien toteuttaminen.
  - Informointi on toteutettava helposti ymmärrettävissä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä.
- Henkilötietojen käsittelytoimet tulee järjestää siten, että rekisteröityjen oikeuksien käyttämistä koskeviin pyyntöihin voidaan reagoida tehokkaasti.
- Rekisteröidyn oikeudet olisi suositeltavaa huomioida myös rekisterien ja käsittelyjärjestelmien teknisessä suunnittelussa.
- Rekisteröidyn tunnistamisen toteuttamistapa on erittäin tärkeä.
  - Rekisterinpitäjällä on oikeus kieltäytyä, jos se pystyy osoittamaan, ettei se pysty tunnistamaan rekisteröityä.

Tietoturvan asianmukainen järjestäminen

Tietosuoja-asetuksen tietoturvavelvoite

- Tietosuoja-asetuksen 32 artikla koskee **käsittelyn turvallisuuteen** liittyvää velvoitetta.
- Rekisterinpitäjän on toteutettava ne **asianmukaiset tekniset ja organisatoriset toimenpiteet**, jotka ovat tarpeellisia riittävän turvallisuustason varmistamiseksi suhteessa käsittelyyn liittyviin riskeihin.
  - Asianmukaiset toimenpiteitä voivat olla esimerkiksi henkilötietojen pseudonymisointi sekä toimenpiteiden säännöllinen testaaminen ja auditointi.
  - **Sopimusperusteiset tietojen suojaamista koskevat ehdot** on määritelty osapuolten välisessä sopimuksessa.
- Käsittelyn sisältämiin **riskeihin** on kiinnitettävä asianmukaisten toimenpiteiden arvioinnissa huomiota.

Kela|Fpa

Tietojen suojaaminen – yleistä

- Henkilötietoja sisältäviä asiakirjoja tai tiedostoja ei saa käsitellä niin, että ulkopuolinen voi nähdä tiedot.
- Tulosteiden ja kopioiden ottamisesta tulee lähtökohtaisesti pidättyä. Henkilötietoja sisältäviä asiakirjoja ei saa hävittää tavallisessa paperinkeräyksessä.
- Vain henkilöillä, jotka tarvitsevat henkilötietoja työtehtäviensä hoitamiseen, tulee olla pääsy tietoihin.
- Työtehtäviin perustuen myönnetty käyttövaltuus on poistettava, kun yhteistyökumppania edustavan työntekijän tehtävät muuttuvat tai hän siirtyy pois organisaation palveluksesta.
- Tietokone on lukittava aina siltä poistuttaessa.
- Kelmu-katseluyhteys on suljettava/kirjauduttava ulos käytön jälkeen.
- Salaamattomalla sähköpostilla ei saa lähettää salassapidettäviä tietoja tai henkilötunnuksia.

Tietojen suojaaminen – sopimusperusteiset tietojen suojausta koskevat ehdot

1. Yhteistyökumppanilla on nimetty tietosuoja- ja tietoturva-asioiden vastuuhenkilö ja tämän yhteystiedot ilmoitetaan Kelalle.
2. Tietoturvallisuuden menettelytavat tulee ohjeistaa ja tietojen luovuttamisessa käytettävää katseluyhteyttä käyttävien tulee perehtyä tähän Kelan teettämään koulutusmateriaaliin ennen Kelmun käyttöä. Kertaluonteisen koulutuksen lisäksi tarvittavasta koulutuksesta ja tiedottamisesta tulee huolehtia tarvittavin väliajoin.
3. Käyttöoikeuksien hallinta on järjestetty tietoturva huomioon ottaen. Käyttäjän käyttöoikeus tulee hyväksyä esihenkilön tai muun käyttöoikeuksia myöntävän toimesta. **Olennaista on huolehtia käyttöoikeuksien välttämättömyydestä työtehtävien kannalta sekä toisaalta käyttöoikeuksien poistamisesta työtehtävien muuttuessa tai työsuhteen päättyessä**.
4. Yhteistyökumppanin tulee luoda tietojen käytön valvontamenettelyt.
5. Tietojen luottamuksellisuus, eheys ja käytettävyys varmistettava niin, että lainsäädännön edellyttämät huolellisuus- ja suojaamisvelvoitteet toteutuvat.
6. Asiakkaille tiedotetaan (Kelan) tietojen käyttämisestä.
7. Väärinkäytösten seuraamuksista tulee tiedottaa yhteistyökumppanin henkilökunnalle.

Kela|Fpa

Tietoturvaloukkaukset

Mikä on tietoturvaloukkaus?

- Tietoturvaloukkauksella tarkoitetaan tilannetta, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei pitäisi olla käyttöoikeutta.
- Esimerkkejä:
  - sähköpostin lähettäminen väärään osoitteeseen
  - asiakirjojen päätyminen väärään paikkaan
  - tietokoneen varastaminen tai katoaminen
  - USB-tikun katoaminen
  - hakkerointi
  - haittaohjelmatartunta
- Tietoturvaloukkauksen seurauksena rekisteröityjen oikeudet vaarantuvat.

Miten tulee toimia tietoturvaloukkauksen sattuessa?

- Raportoi sattuneesta tai epäilemästäsi tietoturvaloukkauksesta välittömästi organisaatiosi sisällä.
- Rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta:
  - **Valvontaviranomaiselle** ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta; ja
  - **Rekisteröidyille**, jos se todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, ilman aiheetonta viivytystä.
- Aikarajat eivät pitene viikonlopuista tai pyhistä.
- Tietoturvaloukkaukset on aina dokumentoitava.

Kela|Fpa

Vastuut tietosuoja-asetuksen alla

Vastuu- ja vahinkotyypit

1. Hallinnollisen velvoitteen rikkomiseen perustuva vastuu (sakko)
2. Lakiin perustuva vahingonkorvausvastuu henkilölle aiheutuvasta taloudellisesta tai muusta vahingosta
3. Sopimusrikkomukseen perustuva vastuu sopimuskumppanille aiheutuneesta (taloudellisesta) vahingosta
4. Rikosoikeudellinen vastuu

Hallinnolliset seuraamukset

- Valvontaviranomainen voi antaa tietojenkäsittelyn keskeyttävän **kiellon**.
- Valvontaviranomaisella voi olla myös oikeus langettaa **rikkomuksen vakavuuden perusteella määräytyvä seuraamusmaksu**
  - Sakon määrää tietosuojavaltuutetun toimiston seuraamuskollegio.
  - Sakon määrään vaikuttavat esimerkiksi vahingon rajoittamiseksi tehdyt toimenpiteet ja omien prosessien sertifiointi.
  - Kansallisen tietosuojalain perusteella seuraamusmaksu **ei tällä hetkellä voi kohdistua julkishallinnon tahoon**, mutta asiantilaan valmistellaan muutosta ja myös Suomessa kohteeksi voi joutua julkishallinnon käyttämä palveluntarjoaja.
- Valvontaviranomaisella käytettävissä laaja keinovalikoima
  - Käsittelykiellon lisäksi esimerkiksi huomautuksen antaminen, käsittelyn rajoittaminen tai vastaavat toimenpiteet.

Kela|Fpa

Lakiperusteinen vahingonkorvausvastuu rekisteröidylle aiheutuneesta vahingosta

- Jos rekisterinpitäjä rikkoo tietosuoja-asetusta ja siitä aiheutuu rekisteröidylle aineellista tai aineetonta vahinkoa, vahingosta on oikeus saada korvausta.
  - Aineellinen tai aineeton vahinko: sekä taloudelliset vahingot että mahdollinen kärsimys korvataan.
- Suojan kohteena ovat sekä rekisteröidyt että muut **vahinkoa kärsineet**.
- Vahingon aiheuttaneen työntekijän tai virkamiehen korvausvastuu kanavoituu lähtökohtaisesti rekisterinpitäjän roolissa olevalle työnantajaorganisaatiolle.

Vahingonkorvausvelvollisuuden ulottuvuudet

- **Vahingonkorvaus rekisteröidyille ja määrättyjen sanktioiden maksaminen tietosuojaviranomaiselle**
  - Peruste syntyy lain nojalla.
  - Käytännössä saattaa edellyttää vuosien prosessin yleisissä tuomioistuimissa.

- **Sopimusperusteinen vahingonkorvaus kahden rekisterinpitäjän välisessä sopimussuhteessa**
  - Tietosuoja-asetus perustaa rajoitetun takautumisoikeuden sopimuskumppanin puolesta rekisteröidylle maksettavista vahingonkorvauksista.
  - Korvausulottuvuutta määrittää rekisterinpitäjien välinen sopimus.

Yksilön rikosoikeudellinen vastuu

- Oikeudettomasta henkilötietojen käsittelystä voi seurata yksilölle rikosoikeudellinen vastuu.
- Henkilötietojen käyttötarkoituksen tai määritettyjen käyttövaltuuksien vastaista henkilötietojen käsittelyä pidetään urkintana, josta voidaan tuomita henkilökohtaiseen vankeusrangaistukseen.

Yhteenveto

Muista erityisesti:

1. Se, että jokin tieto on olemassa ei tarkoita, että sitä saa käyttää mihin tahansa
2. Varmista, että ymmärrät käsittelyn tarpeen: mitä käsittelyllä todella tavoitellaan ja miksi?
   - **Yhteistyökumppanilla on oikeus saada erityislainsäädännön perusteella välttämättömät tiedot, joita se tarvitsee tehtäviensä hoitamiseen.**
3. Jos olet epävarma, ota selvää ja/tai turvaudu periaatemyönteiseen tulkintaan.
4. Vastuiden hallinta edellyttää velvoitteiden tunnistamista.
   - **Käyttöoikeuksien hallinta on keskeistä. Olennaista on huolehtia käyttöoikeuksien välttämättömyydestä työtehtävien kannalta sekä toisaalta käyttöoikeuksien poistamisesta työtehtävien muuttuessa tai työsuhteen päättyessä.**
5. Tietojen käsittelemiseksi on kouluttauduttava ja varmistauduttava omasta osaamisesta.

Kela|Fpa

Kiitos!

Kela|Fpa