Tietosuoja-asetus

Aktuaariyhdistyksen vuosikokous 20.9.2017

Sisältö

- Tilannekatsaus sääntelyyn
- Rekisterinpitäjä ja henkilötietojen käsittelijä
- Henkilötieto ja henkilörekisteri
- Henkilötietojen käsittely
  - Käsittelyn oikeusperusteet
  - Tietosuojaperiaatteiden huomioiminen
  - Tietoturva ja riskienhallinta
- Uusia elementtejä
  - Sisäänrakennettu ja oletusarvoinen tietosuoja
  - Osoitusvelvollisuus
  - Tietosuojavastaava
  - Hallinnolliset sakot
- Rekisteröityjen oikeudet
- Matemaatikon näkökulmasta
  - Henkilötietojen pseudonymisointi
  - Tilastot
  - Big Data

Sääntelytilanne

- **Tietosuoja-asetusta sovelletaan 25.5.2018 lähtien**
- Parhaillaan menossa kansallisen tietosuojalainsäädännön uudelleenarviointi ja sovittaminen asetuksen sisältöön
- OM:n työryhmä 17.2.2016-16.2.2018
  - Mietintö lausuntokierroksella 8.9 asti
    - Uusi tietosuojalaki voimaan asetuksen kanssa samaan aikaan
  - Selvitys kansallisesta liikkumavarasta ja erityissääntelystä
    - Ministeriöiden lainvalmistelutyön koordinointi
  - Selvitys tietosuojaviranomaisia koskevasta sääntelystä

TELA

Asetus, tietosuojalaki, erityislait, käytännesäännöt

- Tietosuoja-asetusta sovelletaan luonnollisia henkilöitä koskevaa jäsenneltyyn henkilötietojen käsittelyyn
  - Sekä automaattinen että manuaalinen käsittely
- Uusi tietosuojalaki yleisellä tasolla, luetaan rinnakkain asetuksen ja erityislakien kanssa
- Henkilötietojen käsittelyä finanssialalla koskevat käytännesäännöt
  - Luonnos valmis ja esitellään tietosuojavaltuutetulle viikolla 39/2017
- Tietosuojaohjeistus työeläkealalle valmisteilla ETK:ssa
  - Tavoiteaikataulu 12/2017
- TSV Aarnio: Valmisteilla eurooppalaisen tietosuojan käsikirja

Mikä muuttuu?

Lainsäädäntö yksityiskohtaisemmaksi
- 99 artiklaa
- Lisäksi paljon tarkennuksia johdantolausekkeissa (resitaalit)

Henkilötietojen käsittelyn edellytykset tiukkenevat
- Rekisteröityjen oikeudet vahvistuvat, uusia oikeuksia

Rekisterinpitäjien ja henkilötietojen käsittelijöiden velvollisuudet ja kustannukset lisääntyvät
- Suunnittelu-, dokumentointi- ja arviointivelvoitteet
- Käsittelijän rooli muuttuu, myös vastuu rikkomuksista
- Riskit kasvavat

Seuraamusjärjestelmä ankaroituu
- Tietosuojaviranomaisille oikeus määrätä suuriakin sakkoja

Rekisterinpitäjä

- Luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee käsittelyn tarkoitukset ja keinot
  - Esim. vakuutusyhtiö, eläkelaitos, ETK
- Jos käsittelyn tarkoitukset ja keinot määritellään kansallisessa laissa, rekisterinpitäjä voidaan vahvistaa lainsäädännön mukaisesti
  - Esim. tulorekisterissä Tulorekisteriyksikkö

Henkilötietojen käsittelijä

- Käsittelee henkilötietoja rekisterinpitäjän lukuun (ei yksit. Työntekijä)
- Rekisterinpitäjä saa käyttää vain sellaisia käsittelijöitä, jotka toteuttavat riittävät suojatoimet niin, että käsittely täyttää asetuksen vaatimukset
- Käsittelijä ei saa käyttää ”alihankkijaa” ilman rekisterinpitäjän kirjallista ennakkolupaa
- Henkilötietojen käsittelijän suorittama käsittely **määritettävä sopimuksella**
- Sopimussuhteelle nimenomaisia sisältövaatimuksia
  - Määritettävä mm. miten rekisteröityjen oikeudet käytännössä toteutetaan
- Sopimuksissa syytä määritellä tarkasti mistä kumpikin osapuoli vastaa
- Rekisteröity voi kohdistaa korvausvaatimuksensa sekä rekisterinpitäjään että käsittelijään (myös hallinnolliset sanktiot kumpaan tahansa)

Henkilötieto

- Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (rekisteröity) liittyvät tiedot
- Tunnistettavissa oleva henkilö
  - Luonnollinen henkilö joka voidaan suoraan tai epäsuorasti tunnistaa tunnistetietojen perusteella
  - Laaja määritelmä, kattaa laajasti tietoja:
    - Nimi, syntymäaika- ja paikka, henkilötunnus, sukupuoli
    - Sijaintitieto, osoite, puhelinnumero
    - Varallisuutta ja tuloja koskevat tiedot
    - Verkkotunnistetiedot
    - Yksi tai useampi henkilölle tunnusomainen fyysinen, fysiologinen, geneettinen, psyykkinen, taloudellinen, kulttuurinen tai sosiaalinen tekijä
    - Vakuutussopimuksiin liittyvät keskeiset tiedot
    - Kuva ja tallennettu puhe
- Ei yrityksiä koskevat tiedot

Rekisteri

- Rekisterin määritelmä
  - Mikä tahansa jäsennelty henkilötietoja sisältävä tietojoukko
  - Tiedot saadaan tietyin perustein
  - Voi olla keskitetty, hajautettu tai toiminnallisesti jaettu
- Erilaisia henkilörekistereitä
  - Asiakasrekisteri
  - Vakuutusrekisteri
  - Korvausrekisteri
  - Eläkerekisteri
  - Markkinointirekisteri
  - Henkilöstörekisteri
  - Sisäpiirirekisteri
  - Lainsäädännössä säädettyjen eri tehtävien hoidosta syntyvät rekisterit

Henkilötietojen käsittely

- Toiminto tai toiminnot, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin
  - Kerääminen
  - Tallentaminen
  - Järjestäminen ja jäsentäminen
  - Säilyttäminen
  - Muokkaaminen tai muuttaminen
  - Haku, kysely
  - Tietojen luovuttaminen siirtämällä, levittämällä tai asettamalla ne muutoin saataville
  - Tietojen yhteensovittaminen tai yhdistäminen
  - Rajoittaminen, poistaminen tai tuhoaminen

Käsittelyn lainmukaisuus

- Selvitettävä mikä on käsittelyn oikeusperuste
- Käsittely voi perustua:
  - ✓ rekisteröidyn **suostumukseen** yhtä tai useampaa tarkoitusta varten
  - ✓ **sopimuksen** täytäntöönpanoon tai sopimusta edeltävien toimenpiteiden toteuttamiseen rekisteröidyn pyynnöstä
  - ✓ **lakisääteisen velvoitteen** noudattamiseen
  - ✓ rekisteröidyn tai muun henkilön elintärkeän edun suojaamiseen
  - ✓ yleistä etua koskevan tehtävän suorittaminen tai rekisterinpitäjälle kuuluvan **julkisen vallan käyttäminen**
  - ✓ rekisterinpitäjän tai kolmannen osapuolen **oikeutettuun etuun** (punninta rekisteröidyn etujen kanssa)

Tietosuojaperiaatteet 1/2

- Henkilötietoja käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
- Henkilötietojen käyttötarkoitussidonnaisuuden periaate
  - Henkilötiedot kerättävä tiettyä nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteen sopimattomalla tavalla
  - Laajamittainen ja kontrolloimaton data-analytiikka mahdollista lähinnä vain anonymisoidun tiedon osalta
- Tietojen minimoinnin periaate
  - Varmistettava, että tietojen säilytysaika mahdollisimman lyhyt, asetettava määräajat henkilötietojen poistolle tai niiden säilyttämisen tarpeellisuuden määräaikaistarkastelua varten
- Henkilötietojen oltava täsmällisiä ja tarvittaessa päivitettyjä

TELA

Tietosuojaperiaatteet 2/2

- Säilytyksen rajoittamisen periaate
  - Säilytettävä muodossa, josta rekisteröity tunnistettavissa ainoastaan niin kauan kuin tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten
- Eheyden ja luottamuksellisuuden periaate
  - Varmistetaan henkilötietojen asianmukainen turvallisuus
- ***Rekisterinpitäjä vastaa tietosuojaperiaatteiden noudattamisesta ja rekisterinpitäjän on pystyttävä osoittamaan, että periaatteita on noudatettu (sanktioitu)***

Tietoturva ja riskienhallinta

- Aiempaa laajempi velvollisuus huolehtia tietoturvasta
- Rekisterinpitäjän ja henkilötietojen käsittelijän toteutettava **asianmukaiset tekniset ja organisatoriset toimenpiteet** varmistaakseen **riskeihin nähden** asianmukainen turvallisuustaso
- Esimerkkilista toimenpiteistä, joilla turvallisuuteen voidaan vaikuttaa
  a. Henkilötietojen pseudonymisointi ja salaus
  b. Kyky taata järjestelmien turvallisuus
  c. Kyky palauttaa nopeasti saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa
  d. Säännöllisen testauksen prosessi, jolla arvioidaan teknisten ja organisatoristen toimenpiteiden tehokkuutta

Tietomurrot

- Velvollisuus ilmoittaa tietoturvaloukkauksista sekä viranomaisille että rekisteröidyille
- Tietomurtoilmoituksille hyvin alhainen kynnys
- Lyhyt toteutusaika: pääsääntöisesti 72 tunnin kuluessa tietoturvaloukkauksen ilmitulosta
- Laaja tietosisältö

Ilmoitusvelvollisuudella kustannusvaikutuksia ja vaikutuksia rekisterinpitäjän maineeseen

TELA

Sisäänrakennettu ja oletusarvoinen tietosuoja

- Rekisterinpitäjän toteutettava käsittelytapojen määrittämisen ja itse käsittelyn yhteydessä asianmukaiset tekniset ja organisatoriset toimenpiteet, siten että toteutetaan tehokkaasti ja pannaan täytäntöön tietosuojaperiaatteet ja suojataan rekisteröityjen oikeudet
- Voidaan ottaa huomioon
  - Uusin tekniikka ja toteuttamiskustannukset
  - Käsittelyn luonne, laajuus, asiayhteys, tarkoitus sekä riskit
- Oletusarvoisesti käsitellään vain kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja

Sisäänrakennettu tietosuoja on uusi velvollisuus

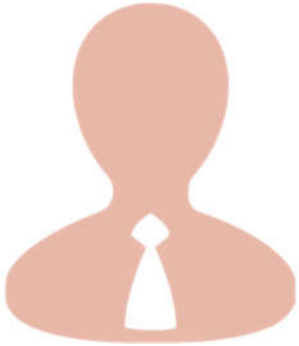
TELA

Osoitusvelvollisuus

- Organisaation tulee kyetä osoittamaan, että se on huolehtinut tietosuoja-asetuksen mukaisista velvoitteista (“documented compliance”)
- Käytännössä osoitusvelvollisuus edellyttää käsittelyyn liittyvien prosessien sekä tietosuojaperiaatteiden käytännön toteuttamisen dokumentointia
  - Tunnistetaan tietosuoja-asetuksen asettamat velvoitteet omalle toiminnalle
  - Dokumentoidaan tarvittaessa toimintaperiaatteet velvollisuuksien toteutumiselle

Tietosuojavastaava

- Koskee sekä rekisterinpitäjiä että käsittelijöitä
- Velvollisuus nimittää tietosuojavastaava, jos
  - Kyse julkissektorin toimijasta
  - Liiketoiminnan keskeisenä osana on käsitellä henkilötietoja tavalla, joka edellyttää rekisteröityjen säännöllistä ja systemaattista valvontaa
  - Keskeisenä liiketoiminnan osana käsitellään laajoja määriä arkaluonteisia tai rikosoikeudellisiin sanktioihin liittyviä tietoja
- Auttaa toteuttamaan lainsäädännön velvoitteet
- Voi olla henkilöstön jäsen
- Konserni voi nimittää yhden tietosuojavastaavan



Hallinnolliset sakot

- Ministeriön ja tietosuojavaltuutetun mukaan tietosuojaviranomaisen keskeisenä tavoitteena ei ole sanktioiden määrääminen
- Sanktiot toimivat pelotteena
- Tarkoitus käyttää törkeissä tilanteissa
  - Otettava huomioon rikkomuksen luonne, vakavuus, kesto, tahallisuus tai tuottamuksellisuus…
- Sakot jaettu luokkiin
  - Enintään 10 000 000 euroa tai 2% yrityksen edellisen vuoden maailmanlaajuisesta kokonaisliikevaihdosta, sen mukaan kumpi johtaa suurempaan summaan
  - Enintään 20 000 000 euroa tai 4% yrityksen edellisen vuoden maailmanlaajuisesta kokonaisliikevaihdosta, sen mukaan kumpi johtaa suurempaan summaan

Rekisteröityjen oikeudet

- **Läpinäkyvä informointi,** toimitettava tietoa rekisteröidylle
  - Rekisteriseloste vs. tietosuojaseloste
  - Ylläpidettävä käsittelyä koskevaa kuvausta
- Oikeus saada pääsy tietoihin
  - Rekisterinpitäjän vastattava tietopyyntöön viipymättä tai viimeistään kuukauden kuluessa
  - Viestintä ja rekisteröidyn pyyntöihin perustuvat toimenpiteet ovat maksuttomia
- Oikeus tietojen korjaamiseen
- Oikeus tietojen poistamiseen (”**oikeus tulla unohdetuksi**”)
- Oikeus käsittelyn rajoittamiseen
- Oikeus vastustaa suoramarkkinointia
- Oikeus vastustaa automaattista päätöksentekoa ja profilointia
- Oikeus siirtää tiedot järjestelmästä toiseen

Oikeus tietojen poistamiseen (”oikeus tulla unohdetuksi”)

- Täsmälliset kriteerit tilanteisiin, joissa yksilö haluaa tietojensa käsittelyn loppuvan
  - Tavoitteena itsemääräämisoikeuden ja yksityisyyden suojan toteutuminen erityisesti online-ympäristössä
- Pääsääntönä henkilötietojen poistaminen viipymättä, kun ei enää perustetta käsittelylle, kuten
  - Henkilötiedot eivät enää ole tarpeellisia (voidaan säilyttää 10-20 vuotta, mutta pystyttävä perustelemaan!)
  - Rekisteröity peruuttaa suostumuksensa
  - Rekisteröity vastustaa käsittelyä eikä ”ylimenevää” oikeusperustetta käsittelylle ole
- Ei sovelleta, jos henkilötietojen käsittely tarpeen esim.
  - Lainsäädäntöön perustuvan, henkilötietojen käsittelyä edellyttävän lakisääteisen velvoitteen noudattamiseksi tai jos käsittely tapahtuu yleistä etua koskevan tehtävän suorittamista tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämistä varten
  - Yleisen edun mukaisia arkistointitarkoituksia tai tilastollisia tarkoituksia varten
  - Oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi

Mikä on profilointia?

- **Profilointi** = henkilötieto + automaattinen käsittely + (arviointi/analysointi/ennakointi)
- Kaikenlaiset toimenpiteet, joilla pyritään:
  - Käyttäjä-, asiakas- tai palvelussuhteen hoitamiseen tai kehittämiseen automaattisten arvioiden perustella
  - Palvelujen tai markkinoinnin kohdentamiseen tai toteuttamiseen automatisoidun analytiikan pohjalta
  - Toiminnan analysointiin ja ennakointiin IT:n tukemana
  - Liityntä työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henk. koht. mieltymyksiin tai kiinnostuksen kohteisiin, sijaintiin, liikkeisiin…

Matemaatikon näkökulmasta…

Henkilötietojen pseudonymisointi

- Henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja, edellyttäen että tällaiset lisätiedot säilytetään erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön tapahdu
- Henkilötietojen psedonymisoimiseen liittyy usein käsitys siitä, että yhden tai useamman attribuutin poistaminen tai korvaaminen toisella riittäisi tekemään tietoaineistosta anonyymin
- Pelkkä tunnisteen muuttaminen ei estä tunnistamasta rekisteröityä, jos tietoaineistoon jää välillisiä tunnisteita tai riittävästi attribuutteja, joiden ainutkertaisen yhdistelmän avulla rekisteröity voidaan edelleen tunnistaa
- Suorien tunnisteiden poistaminen/korvaaminen koodilla tai muulla on rekisterinpitäjän suorittama suojatoimenpide

- PSEUDONYMISOITU TIETO ON HENKILÖTIETOA!

Tilastointi asetuksessa

- Tietosuoja-asetusta sovelletaan, kun henkilötietoja käsitellään tilastotarkoituksia varten
- Henkilötietojen käsittelyä tilastotarkoitusta varten ei pidetä yhteensopimattomana alkuperäisten tarkoitusten kanssa
- Kun henkilötietoja käsitellään tilastollisissa tarkoituksissa, voidaan poiketa eräistä rekisteröidyn oikeuksista
  - Oikeus saada pääsy tietoihin
  - Oikeus tietojen oikaisemiseen
  - Oikeus käsittelyn rajoittamiseen
  - Vastustamisoikeus
- Poikkeusten oltava tarpeellisia ja perusteltuja, lisäksi oltava suojatoimia
- Rekisteröidyn tiedonsaantioikeutta tärkeää korostaa, kun poiketaan rekisteröidyn oikeuksista

Tilastolliset tarkoitukset

- Tilastolliset tarkoitukset
  - Mikä tahansa henkilötietojen keräämis- ja käsittelytoimenpide, joka tarpeen tilastotutkimuksia varten tai tilastollisten tulosten tuottamiseksi
  - Käsittelyn tuloksena yhdistelmätietoja
  - Tulosta ei hyödynnetä ketään luonnollista henkilöä koskevissa toimenpiteissä tai päätöksissä
  - Tilastollisia tuloksia voidaan käyttää myöhemmin eri tarkoituksiin
  - Myöhempien käsittelytarkoitusten tulee olla yhteensopivia alkuperäisen käsittelytarkoituksen kanssa

Tilastointi tietosuojalaissa

- Asetuksen mukaista poikkeusmahdollisuutta ehdotetaan käytettäväksi
- Poikkeaminen sallittua ainoastaan tarvittaessa
- Oikeus tarkastaa itseään koskevat tiedot voidaan sulkea pois, kun otetaan huomioon tilastoinnin tarkoitukset ja vähäinen puuttuminen yksityisyyden suojaan
- Poikkeaminen sillä edellytyksellä, että
  1) Tilastoa ei voida tuottaa tai sen tarkoituksena olevaa tiedontarvetta toteuttaa ilman henkilötietojen käsittelyä
  2) Kyseisen tilaston tuottamisella on asiallinen yhteys rekisterinpitäjän toimintaan
  3) Tietoja ei luovuteta tai aseteta saataville siten, että tietty henkilö on niistä tunnistettavissa, ellei tietoja luovuteta julkista tilastoa varten

Big Data (massadata)

- Erittäin suurten strukturoimattomien datamassojen kerääminen, tallentaminen ja jalostaminen strukturoiduksi informaatioksi analysointia varten
- Erikoispiirteitä valtavat volyymit, uuden datan tuottamisen huippunopeus sekä datan ja sen lähteiden vaihtelevuus
- Uudenlaiset tavat kerätä ja hyödyntää tietoja
- Keskeinen idea on tietojen myöhempi käsittely tavalla ja tarkoituksiin, joita ei ole määritelty tietojen keräämishetkellä
  - Haasteena/keskeistä tietosuojaperiaatteiden tehokas soveltaminen
- ”Kysymys ei ole siitä, pitäisikö massadataan soveltaa tietosuojalainsäädäntöä, vaan siitä, kuinka sitä voidaan soveltaa innovatiivisesti uusissa ympäristöissä” (Euroopan tietosuojavaltuutettu 20.2.2016)

Lopuksi

- Tietosuoja-asetuksen positiiviset vaikutukset
  - Asiakkaiden ja palveluiden käyttäjien luottamuksen lisääntyminen
- Vaikutukset yrityksille
  - Kirjanpito henkilötietojen käsittelytoimista
  - Hallinnolliset velvollisuudet lisääntyvät merkittävästi
- Ylimmän johdon sitouttaminen keskeistä
- Prosessien luominen mm. rekisteröityjen oikeuksien toteuttamiseksi
- Yhteistyö, viestintä ja koulutus: Tietosuoja rakennetaan osaksi palveluita ja prosesseja!

KIITOS!

Outi Aalto
outi.aalto@tela.fi