ONKO TIETOJEN KÄSITTELY RISKI VAI BISNES?

Keuken Tietosuojailta

1.3.2023

Markus Myhrberg

Lexia Asianajotoimisto Oy

LEXIA
Legal Excellence

AGENDA

Tietosuojasääntely-ympäristö

Henkilötietojen käsittely ja hyödyntäminen

Rekisterit, tietojen käsittelyperusteet ja tietojen elinkaari

Tietosuojasopimukset

Tietosuojavastaava

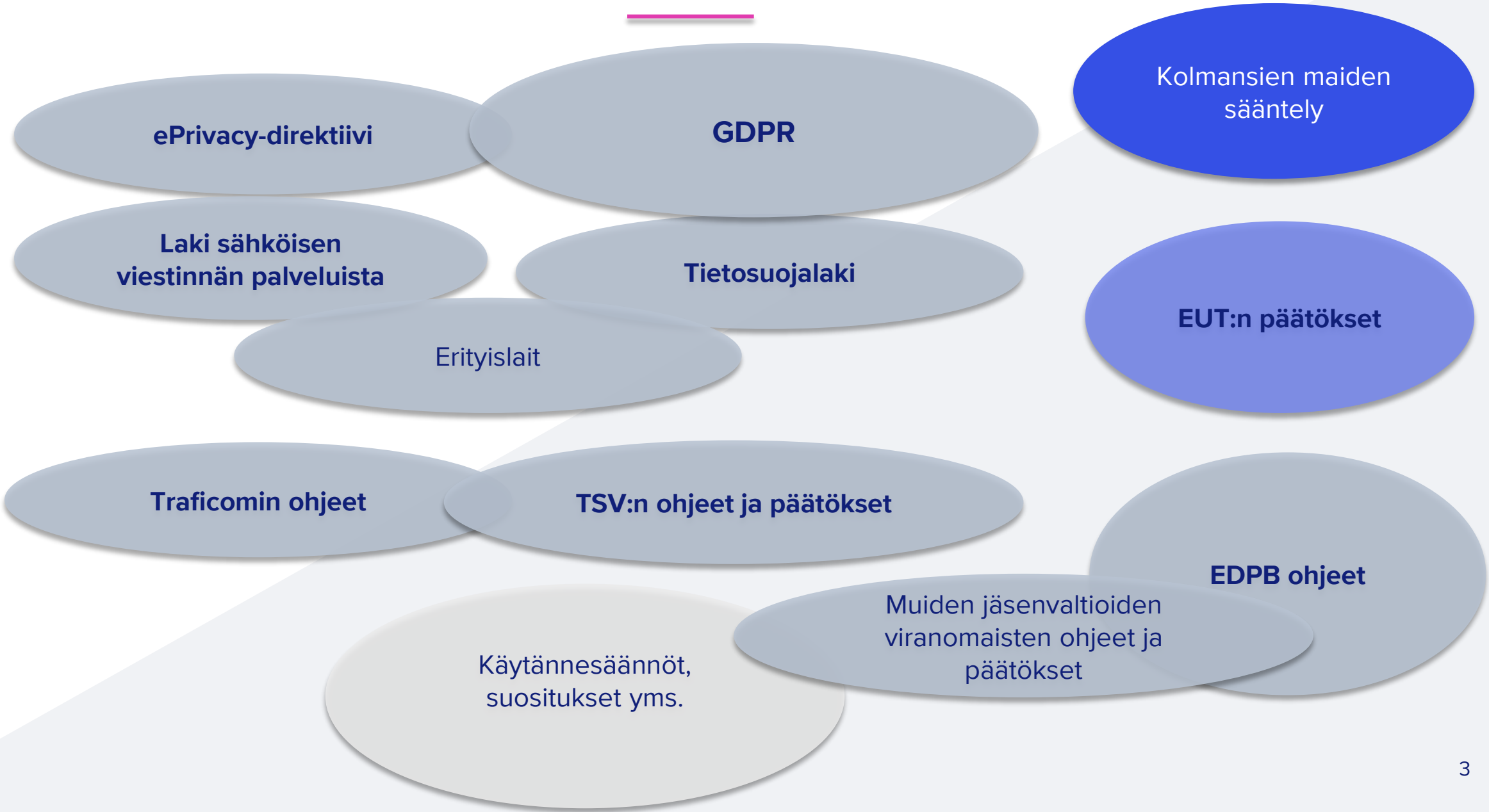
Tietoturvaloukkaukset

Sähköinen suoramarkkinointi

Evästeet

Dokumentaatio

SÄÄNTELY-YMPÄRISTÖ



KESKEINEN TIETOSUOJASÄÄNTELY

Yleinen tietosuoja-asetus (GDPR)
ePrivacy-direktiivi

- **Tietosuojalaki**
- **Työelämän tietosuojalaki**
- **Laki sähköisen viestinnän palveluista**
- **Erityislainsäädäntö**

TIETOSUOJA-ASETUS (GDPR): KESKEISET PERIAATTEET JA REUNAEHDOT

KESKEISET KÄSITTEET

HENKILÖTIETO

KÄSITTELY

REKISTERI

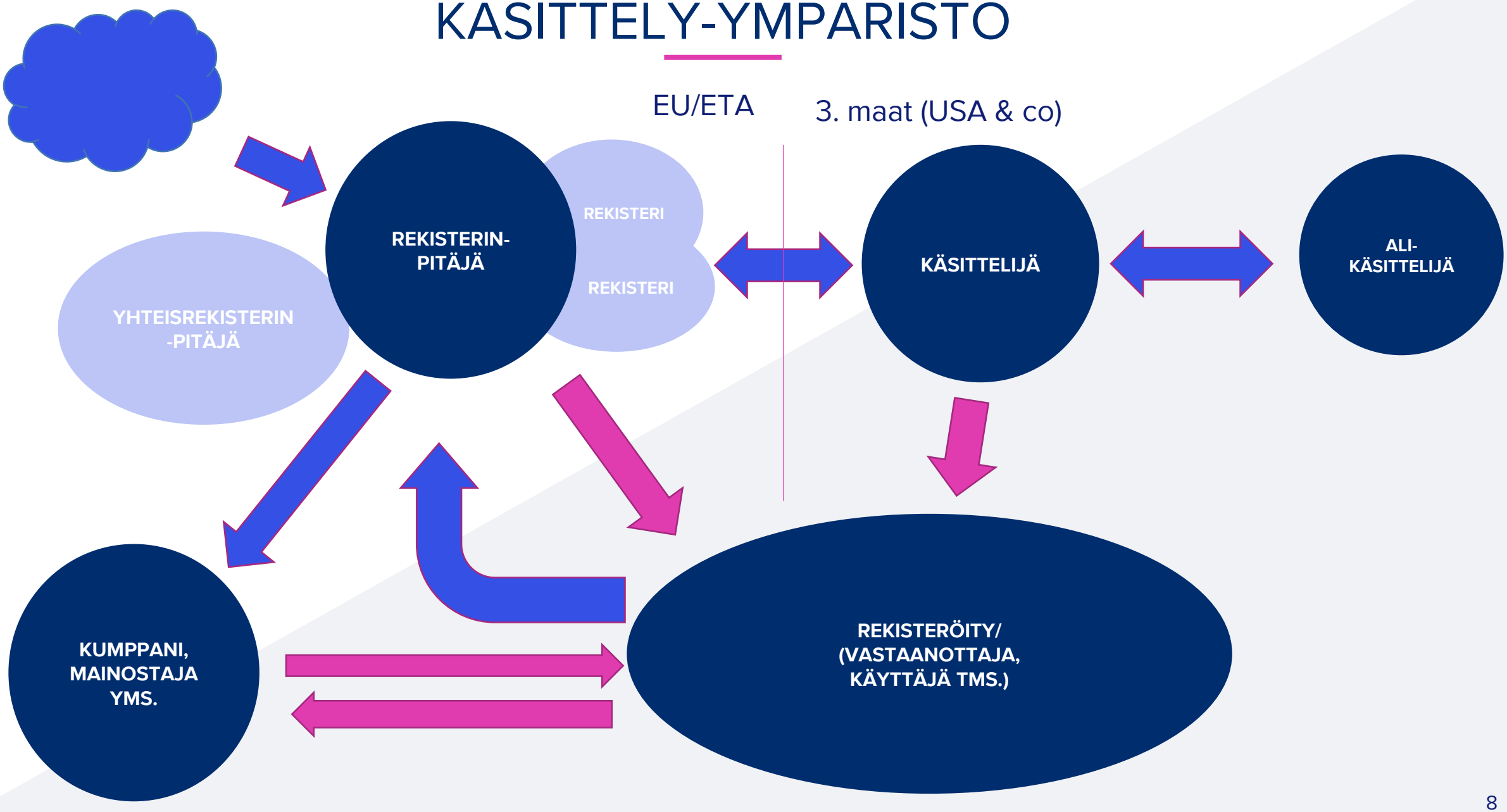
REKISTERIN-
PITÄJÄ

KÄSITTELIJÄ

KÄSITTELY

”Toiminto, joka kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten 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.”

KÄSITTELY-YMPÄRISTÖ



REKISTERINPITÄJÄN VELVOLLISUUDET

Kaiken toiminnan lähtökohtana **riskiperusteinen lähestymistapa**

Oletusarvoinen ja sisäänrakennettu tietosuoja

Noudattamisvelvollisuus ja **osoittamis**velvollisuus

KÄSITTELYSSÄ NOUDATETTAVAT PERIAATTEET

- **Noudatettava** henkilötietojen käsittelyssä

1. Lainmukaisuus, kohtuullisuus, läpinäkyvyys
2. Käyttötarkoitussidonnaisuus
3. Tietojen minimointi

- Pystyttävä **osoittamaan** noudattaminen

4. Täsmällisyys
5. Säilytyksen rajoittaminen
6. Eheys ja luottamuksellisuus

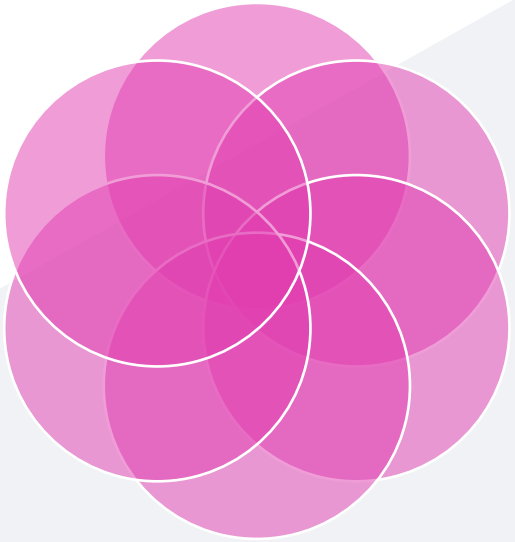
KÄSITTELYPERUSTE

Määrittele etukäteen
Muista osoitusvelvollisuus

Suostumus

Sopimus

Oikeutettu etu



Julkisen vallan käyttäminen

Lakisääteinen velvoite

Elintärkeiden etujen suojaaminen

SUOSTUMUS

Vapaaehtoinen, **yksilöity**, **tietoinen** ja **yksiselitteinen tahdonilmaisu**

- Suostumus on annettava **selkeästi suostumusta ilmaisevalla** toimella

- Suostumusta ei voida antaa
  - vaikenemalla;
  - valmiiksi rastitetuilla ruuduilla; tai
  - jättämällä jokin toimi toteuttamatta.

- Sähköisessä palvelussa pyynnön oltava:
  - selkeä ja tiiviisti esitetty eikä se saa tarpeettomasti häiritä sen palvelun käyttöä

- Rekisteröidyllä on oikeus peruuttaa suostumuksensa milloin tahansa (seuraukset?)

- Tiettyihin toimiin vaaditaan nimenomainen suostumus

ASIAKASTIETOJEN KÄSITTELY

- Olemassa olevista asiakkaista saa käsitellä tietoja, jotka **sopimuksen** kannalta tarpeellisia
  - Sopimus ensisijainen käsittelyperuste (suostumus vain tarvittaessa)

- Mitä muita tietoja tarpeen käsitellä asiakassuhteen kannalta?
  - **Markkinoinnin osalta oikeutettu etu** (myös potentiaaliset asiakkaat)
  - Asiakasviestintä > Sopimus/oikeutettu etu?
  - Oikeutetun edun perusteella mm. asiakassuhteen hoito
    - Tasapainotesti, perustelujen dokumentointi

- Milloin asiakassuhde **syntyy**?
  - Sopimus, ostotapahtuma, rekisteröityminen palveluun…

- Milloin **asiakassuhde päättyy**?

- > Tietojen säilytysprosessin ja säilytysajan määrittäminen
  - Käsittelytarkoituksen ja –perusteen muutos asiakassuhde/potentiaalinen asiakas

REKISTERÖITYJEN OIKEUDET

- Oikeus saada läpinäkyvää ja ajantasaista tietoa
- Oikeus päästä tietoihin
- Oikeus tietojen oikaisuun
- Oikeus siirtää tiedot järjestelmästä toiseen
- Oikeus tietojen poistamiseen (”oikeus tulla unohdetuksi”)
- Oikeus käsittelyn rajoittamiseen
- Vastustamisoikeus
- Oikeus vastustaa profilointia ja automaattista päätöksentekoa
- Oikeus saada ilmoitus tietoturvaloukkauksesta
- Oikeus luottaa tietoturvan korkeaan tasoon

MITEN HUOMIOIN OMASSA TOIMINNASSANI?

- Järjestelmät, toimintatavat, ohjeistukset jne.
- Prosessi ja vastuut?

CASE – REKISTERÖITYJEN OIKEUDET

- Alektum Oy oli säännönmukaisesti jättänyt vastaamatta rekisteröidyn tietosuojaoikeuksia koskeviin pyyntöihin.
  - Velvollisuus vastata rekisteröidyn oikeuksia koskeviin pyyntöihin kuukauden kuluessa.
  - Jos pyyntöjä on monta tai ne ovat monimutkaisia, rekisterinpitäjänä toimiva organisaatio voi ilmoittaa tarvitsevansa lisäaikaa enintään kaksi kuukautta.
- Alektum Oy selitti lisäksi yhden kantelijan kohdalla vastaamatta jättämistä sillä, ettei se kertomansa mukaan enää käsitellyt rekisteröidyn henkilötietoja.
  - Yrityksen olisi pitänyt vastata pyyntöön ja kertoa, että yritys ei enää käsittele rekisteröidyn henkilötietoja.
- Seuraamuskollegio: Yritys ei ollut perehtynyt riittävästi tietosuoja-lainsäädännön vaatimuksiin ja toiminta on ilmentänyt piittaamattomuutta lainsäädännöstä.
- Sakon suuruuteen vaikutti myös se, että yritys ei noudattanut velvollisuutta tehdä yhteistyötä valvontaviranomaisen kanssa + kyse oli henkilöiden oikeusturvasta (kyseessä perintäyhtiö).
- Seuraamusmaksun suuruus 750 000 euroa (ei ole vielä lainvoimainen).

REKISTERÖITYJEN INFORMOINTI

Läpinäkyvää ja **helposti saatavilla olevaa** informointia

Helposti ymmärrettävässä, tiiviissä muodossa ja yksinkertaisella kielellä

Tietosuoja-asetus → laajempi informointivelvollisuus → **tietosuojaseloste/-käytäntö**

Kattavalla informoinnilla voi pienentää tarvetta **tarkastusoikeuden** käyttämiseen

Suunnittele omaan toimintaan sopiva **tietosuojaviestintä**

REKISTERÖITYJEN INFORMOINTI

- Rekisterinpitäjän identiteetti ja yhteystiedot
- Käsittelyn tarkoitukset ja oikeusperusteet
- Tietolähteet
- Tietojen siirtäminen ja vastaanottajat, siirrot EU/ETA ulkopuolelle
- Rekisteröidyn oikeuksien toteuttaminen
- Henkilötietojen säilytysaika tai, jos ei mahdollista, määrittämiskriteerit
- Tietosuojavastaava
- Valitus valvontaviranomaiselle
- Automaattisen päätöksenteko / profilointi

CASE –MINIMOINTI, KÄSITTELYPERUSTEET, SÄILYTYSAIKA

- ParkkiPate Oy oli kieltäytynyt toimittamasta tietoja ennen kuin se on varmistunut pyynnön esittäjän henkilöllisyydestä. Vaadittu toimittamaan muun muassa henkilötunnuksensa ja osoitteensa
  - Ei kuitenkaan ole alun perin ollut tiedossaan henkilötunnuksia, ei voi verrata > **tietoja käsitelty laajemmin kuin tarpeen**

- Valokuvat ja jäljennökset valvontamaksulomakkeista kirjanpitotarkoituksiin (käsittelyperuste)
  - ”kirjanpitolain lakisääteiset velvoitteet ja mahdolliset tulevat oikeudelliset jatkotoimet ovat estäneet tietojen poistamisen”
- TSV: Kuvat ajoneuvosta tai valvontamaksulomakkeet **eivät ole sellaisia kirjanpitolain** mukaisia tositteisiin liittyviä tietoja, joita pitäisi säilyttää kirjanpitolaissa säädetyn ajan perusteella
- Tietoja **ei** myöskään **voida säilyttää määrittelemätöntä** aikaa sen nojalla, että rekisterinpitäjä mahdollisesti tulevaisuudessa päättää saattaa asian tuomioistuimen ratkaistavaksi. Henkilötietojen **säilytysaika tai sen määrittämiskriteerit on määriteltävä, ja oltava mahdollisimman lyhyt**

- Puutteita havaittiin myös tavoissa, joilla rekisterinpitäjä **informoi** rekisteröityjä henkilötietojen käsittelystä

- Useita kanteluita
- Seuraamusmaksun suuruus 75 000 euroa, hallinto-oikeus muutti 70 000 eur (ei tahallisia)

HENKILÖTIEDON ELINKAARI

GDPR:n mukaiset velvoitteet ja vastuut rekisterinpitäjälle ja käsittelijälle
Tietosuoja-asetuksen mukaiset oikeudet rekisteröidylle

- ✓ Määrittele käsittelyperuste ja käsittelyn tarkoitus
- ✓ Määritä käsittelyn kesto ja tietojen säilytysaika
- ✓ Tunnista velvollisuudet tietoja käsiteltäessä
- ✓ Tunnista, missä vaiheessa käsittelyperuste poistuu
- ✓ Poista tai anonymisoi tiedot käsittelyperusteen lakattua

KÄSITTELYSOPIMUKSET (DPA)

- Rekisterinpitäjän ja käsittelijän välillä on oltava henkilötietojen käsittelyä koskeva sopimus (Data processing agreement, controller-processor)
  - Ei tarvitse olla erillinen sopimus, voi olla liite (tai itse sopimustekstissäkin)

- Asetus **velvoittaa sopimaan** kirjallisesti useista seikoista
  - Sovittava mm. käsittelyn kohteesta, kestosta, tarkoituksesta ja osapuolten velvollisuuksista & oikeuksista, ohjeistuksesta, tietoturvasta, rekisteröidyn oikeuksista, auditoinnista, salassapidosta sekä tietojen poistamisesta

- Vastuukysymysten ja riskienhallinnan näkökulmasta myös **suositeltavaa sopia** aiempaa tarkemmin myös tietosuojaan liittyvistä seikoista
  - Vastuunrajoitukset
  - Kustannukset, raportointi yms.

LUOVUTUSSOPIMUKSET (DTA)

- Rekisterinpitäjien välinen sopimus (data transfer agreement, controller-controller)
- GDPR:ssä ei suoria vaatimuksia
- Käyttötarkoitussidonnaisuus
  - Käyttötarkoituksen tulee olla sellainen, johon voidaan luovuttaa
- Velvollisuudet ja vastuunrajoitukset
  - *Osapuolet sitoutuvat noudattamaan toiminnassaan soveltuvaa ja kulloinkin voimassa olevaa henkilötietojen käsittelyyn ja tietosuojaan liittyvää lainsäädäntöä*
  - *Kumpikin osapuoli vastaa itsenäisesti ja erillisesti rekisteröityjen oikeuksista suhteessa käsittelemiinsä henkilötietoihin*
- Rekisteröityjen informointi
- Suostumukset (erityiset henkilötietoryhmät, alaikäiset yms.)

HENKILÖTIETOJEN SIIRTÄMINEN EU/ETA:N ULKOPUOLELLE

SUOJAN RIITTÄVYYTTÄ KOSKEVA PÄÄTÖS

Euroopan komission tietosuojan riittävyyttä koskeva päätös (Esim. Argentiina, Kanada, Israel, Japani, Uusi-Seelanti, Sveitsi, UK)

~~US Privacy Shield mekanismi~~ ✕

ASIANMUKAISET SUOJATOIMET

Malli-/vakiosopimuslausekkeet (SCCs)
Yrityksiä sitovat säännöt (BCR)
Hyväksytyt käytännesäännöt / sertifikaatit

POIKKEUKSET

Nimenomainen suostumus
Sopimusliitännäinen (tai sopimuksentekoa edeltävä välttämättömyys)
Välttämättömyys elintärkeiden etujen suojaamiseksi
Välttämättömyys oikeudellisten vaateiden vuoksi

HENKILÖTIETOJEN SIIRTO YHDYSVALTOIHIN

- Euroopan unionin tuomioistuin (EUT) antoi heinäkuussa 2020 ratkaisun koskien tietosuojaa ja henkilötietojen siirtoa Yhdysvaltoihin (”Schrems II”)
- EUT:n ratkaisun mukaan Yhdysvaltojen kanssa sovittu Privacy Shield- järjestelmä ei täytä tietosuoja-asetuksessa asetettuja vaatimuksia
- Henkilötietojen siirtäminen Privacy Shield-järjestelmän perusteella **ei ole ollut** sallittua 16.7.2020 lähtien.
    - Privacy Shield 2.0 tulossa?
- Tuomioistuin otti ratkaisussa kantaa myös vakiosopimuslausekkeisiin henkilötietojen siirtojen perusteena kolmansiin maihin

HENKILÖTIETOJEN SIIRTO EU/ETA:N ULKOPUOLELLE

- Henkilötietojen siirto ns. **komission vakiosopimuslausekkeita (standard contractual clauses, SCC)** hyödyntäen **on sallittua**
  - Vakiosopimuslausekkeiden käyttöä sellaisenaan ei kuitenkaan välttämättä riittävää
  - Arvio tietosuojan toteuttamisesta tapauskohtaisesti huomioiden kohdemaan lainsäädäntö ennen mallisopimuslausekkeiden käyttöä **> lisätoimenpiteet** (supplemental measures)
    - dokumentointi

- Käyttöön **uudet vakiosopimuslausekkeet**
  - Päivitetty vastaamaan EU:n yleisen tietosuoja-asetuksen (GDPR) vaatimuksia
  - Voimaan 27.6.2021 → 18 kuukautta aikaa päivittää sopimukset → siirtymäaika päättynyt 27.12.2022
  - https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_fi
  - https://tietosuoja.fi/komission-hyvaksymat-vakiolausekkeet

- Kv. tietojensiirtoon liittyvä vaikutustenarviointi (Data transfer impact assessment)

TRANS-ATLANTIC DATA PRIVACY FRAMEWORK

- EU ja USA ilmoittivat 25.3.2022 sopineensa ”periaatteessa” korvaavasta ratkaisusta. Tarkat yksityiskohdat, mm. aikataulu, ovat vielä hämärän peitossa.
- Tiedotteen nimi on “European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework”.
- Tällä sovitaan ratkaisuista ja puitteista, jotka merkitsevät Yhdysvaltain puolelta sitoutumista uudistusten toteuttamiseen signaalitiedustelutoiminnan osalta.
- Tämä vahvistaa yksityisyyden ja kansalaisvapauksien suojaa.
- Tällä viitekehyksen avulla tieto voi liikkua vapaasti ja turvallisesti EU:n kansalaisten ja USA:ssa toimivien yritysten välillä.
- Näillä uusilla säännöillä ja suojatoimenpiteillä rajoitetaan Yhdysvaltain tiedustelupalvelun pääsyä tietoihin. Signaalitiedustelutietoa voidaan kerätä vain, jos se on tarpeen laillisten kansallisten turvallisuustavoitteiden edistämiseksi, eikä se saa vaikuttaa suhteettomasti yksilön yksityisyyden ja kansalaisvapauksien suojaan.

Data Privacy Framework

SEURAAVAT ASKELEET

- USA:n hallitus ja Euroopan komissio jatkavat nyt yhteistyötään, joilla päätös saadaan muutettua sitoviksi oikeudellisiksi asiakirjoiksi
- USA:ssa tämä tarkoittaa mm. presidentin allekirjoittamaa toimeenpanomääräystä (Executive Order 7.10.2022)
- Nämä lait ja asiakirjat on hyväksyttävä molempien osapuolten, jotta tämä uusi transatlanttinen tietosuojakehys voidaan ottaa käyttöön
- Samalla luodaan uusi kaksitasoinen oikeussuojamekanismi eurooppalaisten valitusten tutkimiseksi ja ratkaisemiseksi, sisältäen muun muassa riippumattoman tietosuojavalvontatuomioistuimen
- 13.12.2022 Euroopan komissio julkaisi päätösluonnoksen Yhdysvaltojen tietosuojan tason riittävyydestä. Päätösluonnoksen voimaantulo edellyttää hyväksymismenettelyn läpikäymisen.

TIETOSUOJAVASTAAVAN NIMITTÄMINEN

- Tietosuojavastaava on nimitettävä, jos organisaatio
  - käsittelee laajamittaisesti arkaluonteisia tietoja
  - seuraa ihmisiä laajamittaisesti, säännöllisesti ja järjestelmällisesti
  - on julkishallinnon toimija (pois lukien tuomioistuimet).

- Tietosuojavastaava voidaan nimittää myös silloin, kun tietosuoja-asetus ei siihen velvoita
  - Jos organisaatio nimittää tietosuojavastaavan vapaaehtoisesti, tietosuojavastaavan nimittämiseen, asemaan ja tehtäviin sovelletaan tietosuoja-asetuksen vaatimuksia samalla tavoin kuin silloin, kun nimittäminen on pakollista

- Tietosuojavastaava on organisaation sisäinen asiantuntija tietosuoja-asioissa sekä rekisteröityjen ja tietosuojaviranomaisen yhteyshenkilö
  - Tietosuojavastaavan on oltava riippumaton, eikä hänellä voi olla eturistiriitoja tietosuojavastaavan tehtävien kanssa

- Tietosuojavastaavan yhteystiedot on ilmoitettava tietosuojavaltuutetun toimistolle
- Tietosuojavastaavan yhteystietojen on oltava suoraan ja helposti myös yleisön saatavilla.

MIKÄ ON TIETOSUOJAVASTAAVA?

- Tietosuojavastaava
  - seuraa tietosuojasääntöjen noudattamista koko organisaatiossa ja tuo esiin havaitsemiaan puutteita
  - antaa tietoja ja neuvoja tietosuojasääntöjen mukaisista velvollisuuksista johdolle ja henkilötietoja käsitteleville työntekijöille
  - antaa pyydettäessä neuvoja tietosuojan vaikutustenarvioinnin tekemisestä ja valvoo vaikutustenarvioinnin toteutusta
  - on rekisteröityjen yhteyshenkilö henkilötietojen käsittelyyn liittyvissä asioissa
  - on tietosuojavaltuutetun toimiston yhteyshenkilö ja tekee yhteistyötä tietosuojavaltuutetun toimiston kanssa

OHJEITA TIETOSUOJAVASTAAVAN NIMITTÄNEELLE

- TSV:n ohjeita tietosuojavastaavan nimittäneelle organisaatiolle:
  - ❑ Tietosuojavastaavalla on oltava riittävästi työaikaa, -välineitä ja osaamista tehtävän suorittamiseen. Tietosuojavastaavalla pitäisi olla myös mahdollisuus kouluttautua.
  - ❑ Tietosuojavastaava tai hänen tiiminsä otetaan mahdollisimman aikaisessa vaiheessa mukaan kaikkien tietosuojakysymysten käsittelyyn.
  - ❑ Tietosuojavastaavan suositellaan olevan paikalla aina silloin, kun tehdään tietosuojaan vaikuttavia päätöksiä. Kaikki olennaiset tiedot toimitetaan tietosuojavastaavalle viipymättä, jotta hän voi antaa asianmukaisia neuvoja.
  - ❑ Tietosuojavastaavalla on oltava mahdollisuus raportoida suoraan johdolle. Tietosuojavastaava kutsutaan säännöllisesti ylemmän tai keskitason johdon kokouksiin.
  - ❑ Tietosuojavastaavan näkemykselle annetaan aina asianmukainen painoarvo. Mahdollisissa erimielisyystilanteissa on hyvä dokumentoida perusteet, joiden vuoksi tietosuojavastaavan neuvoa ei noudateta.
  - ❑ Jos tietoturvaloukkaus tai muu tietosuojaan liittyvä ongelma ilmenee, tietosuojavastaavaa kuullaan mahdollisimman nopeasti.
  - ❑ Tietosuojasäännösten noudattaminen on rekisterinpitäjän tai henkilötietojen käsittelijän vastuulla. Tietosuojavastaavat eivät ole henkilökohtaisesti vastuussa yleisen tietosuoja-asetuksen rikkomisesta.

TIETOTURVALOUKKAUKSET

- Mikä on henkilötietojen tietoturvaloukkaus?
  - Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.

- Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi
  - hävinnyt tiedonsiirtoväline, kuten USB-tikku
  - varastettu tietokone
  - hakkerointi
  - haittaohjelmatartunta
  - kyberhyökkäys
  - tulipalo datakeskuksessa
  - tiliotteen postitus väärälle henkilölle.

TIETOTURVALOUKKAUKSISTA ILMOITTAMINEN

- Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa valvontaviranomaiselle, jos
  - loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille
- Suomessa valvontaviranomaisena toimii tietosuojavaltuutetun toimisto

- Henkilötietojen tietoturvaloukkauksesta on ilmoitettava tietosuojavaltuutetun toimistolle
  - ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta

- Tietosuojavaltuutetun sivulla tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta yksityiskohtainen täytettävä lomake

- Ilmoitus rekisteröidylle korkean riskin tilanteessa ilman aiheetonta viivästystä

SÄHKÖINEN SUORAMARKKINOINTI

SÄHKÖINEN SUORAMARKKINOINTI

- *Laki sähköisen viestinnän palveluista (SVPL, 917/2014)*

- **Sähköiseen suoramarkkinointiin** saatava **suostumus luonnolliselta henkilöltä** (opt-in)
  - Jos käytössä automaattinen soittojärjestelmä, fax, sähköposti, tekstiviesti, puhe-, ääni- ja kuvaviestit
  - Puhelinmarkkinointi on sallittu ilman suostumusta, ellei erikseen kielletty
  - Kohdentaminen esim. evästetiedon perusteella somessa tai sivuilla ei ole suoramarkkinointia

- Suostumuksen oltava yksiselitteinen

- Ei oikeutta luvan kysymiseen sähköisesti
  - Lupa sähköpostimarkkinointiin ei siis voi kysyä sähköpostilla…

SÄHKÖINEN SUORAMARKKINOINTI

- Yrityksillä on **kielto-oikeus** (opt-out)
  - myynti@yritys.fi > kielto-oikeus (eli ei tarvita suostumusta → suoramarkkinointia yhteisölle saa harjoittaa, jollei tämä ole sitä nimenomaisesti kieltänyt)
  - **etunimi.sukunimi@yritys.fi osoite on luonnollisen henkilön → aseman ja tehtävien perusteella** voidaan kuitenkin lähettää ilman etukäteistä suostumusta asemaan tai tehtäviin liittyvää sähköistä suoramarkkinointia
    - Huom! Matkapuhelimen osalta ei yhtä selkeää poikkeusta

- Kielto-oikeutta voitava käyttää helposti ja ilman erillistä maksua
  - Kerrottava tietosuojaselosteessa
  - Markkinointiviestien yhteydessä esim. unsubscribe- linkki tai ”hallinnoi uutiskirjetilauksia”

- Uusi ePrivacy-asetus voi tuoda muutoksia → tarkkaile tilannetta (kansallinen implementointi)

SÄHKÖINEN SUORAMARKKINOINTI

- Aiemmin saatu yhteystieto
  - jos palveluntarjoaja tai tuotteen myyjä **on myynnin yhteydessä saanut asiakkaan sähköiset** osoitetiedot tilauksen yms. perusteella, **voi osoitetta** käyttää samaan tuoteryhmään tai muuten vastaavien tuotteiden ja palveluiden suoramarkkinointiin (ilman eri suostumusta)
    → sama yhteystieto, jolla aiemmin tilattu
  - vain yritys, joka on saanut tiedot

- Tarjottava etukäteinen ja tapahtumakohtainen **kielto-oikeus**
  - Ilman erillistä maksua ja helposti

SÄHKÖINEN SUORAMARKKINOINTI

- Sähköisen suoramarkkinoinnin oltava **tunnistettavaa**
  - Sähköpostin otsikossa
  - Myös tekstiviestit

- **Asiakasviestintä ei ole** suoramarkkinointia
  - Asiakassuhteen ylläpitämiseksi tarvittava yhteydenpito
  - Ei saa sisältää markkinointia
  - Esim. viestintä, jossa asiakas saa tietoja jo aiemmin valitsemansa palvelun tilasta
  - Myös markkinatutkimukset sääntelyn ulkopuolella

CASE - SÄHKÖINEN SUORAMARKKINOINTI JA REKISTERÖIDYN OIKEUDET

- Suoramarkkinointiviestejä oli lähetty **ilman ennakkolupaa**. Lisäksi osa vastaanottajista oli pyytänyt suoramarkkinoinnin lopettamista, mutta he olivat **kielloista huolimatta** saaneet markkinointiviestejä.
  - Vastustamisoikeus suoramarkkinointiin ei ollut toteutunut.

- Rekisterinpitäjä katsoi kohdistaneensa sähköistä suoramarkkinointia yhteisöihin, jolloin ei olisi vaadittu ennalta annettua suostumusta. Rekisterinpitäjän **olisi kuitenkin tullut selvittää kyseisen henkilön asema yrityksessä ja arvioida, liittyykö suoramarkkinointi olennaisesti henkilön työtehtäviin.**
  - Rekisterinpitäjän olisi pitänyt pyytää suostumus rekisteröidyltä

- Lisäksi muihin rekisteröidyn oikeuksia koskeviin **pyyntöihin ei ollut vastattu ilman aiheetonta viivettä ja** enintään kuukauden kuluessa. Rekisterinpitäjä ei ollut myöskään toteuttanut pyyntöjä (tai ei pystynyt osoittamaan tätä)

- Huomautus henkilötietojen käsittelystä ilman suostumusta sekä rekisteröidyn oikeuksien laiminlyömisestä. Velvollisuus korjata toimintatapansa sekä määräys toteuttaa rekisteröidyn oikeudet.
- Seuraamusmaksun suuruus 7000 euroa

CASE – SUORAMARKKINOINTI ROBOTTIPUHELUIDEN AVULLA

- Kustannusyritys harjoitti lehteä koskevaa suoramarkkinointia automatisoidulla soittojärjestelmällä ilman puheluiden vastaanottajien suostumusta.
- Robottipuheluissa ei ole varmistuttu siitä, että rekisteröity pystyy käyttämään tietosuojaoikeuksiaan.
- Lisäksi rekisterinpitäjä ja sen lukuun suoramarkkinointipuheluita toteuttanut alihankkijayritys eivät olleet laatineet yleisen tietosuoja-asetuksen edellyttämää käsittelysopimusta suoramarkkinoinnin toteuttamiselle.
- Yritykselle määrättiin 8500 euron seuraamusmaksu.

EVÄSTEET JA MUUT TEKNISET SEURANTAKEINOT

EVÄSTEET

- Käyttäjän toimintaa verkossa voidaan seurata useilla eri toiminnoilla
  - Kohdennettu (suora)markkinointi → käyttäen hyväksi **evästeitä ja muita teknisiä seurantakeinoja**
    - Voidaan rakentaa käyttäjäprofiileja ja kohdentamaan tehokkaammin suoramarkkinointia

- Eväste (cookie) on pieni tekstitiedosto, jonka internetselain tallentaa käyttäjän laitteelle
  - Voidaan tallentaa käyttäjän laitteelle pysyvästi (stored cookie) tai se voidaan poistaa palvelun käytön jälkeen (session cookie)
  - Sääntely koskee myös muita seurantakeinoja pikselit, beacons, tagit jne. > suostumus

- Ensimmäisen osapuolen evästeet
  - Ovat peräisin käytetyltä verkkosivustolta ja ainoastaan kyseinen verkkosivusto voi käyttää evästetietoja

- Kolmannen osapuolen evästeet
  - Ovat peräisin muilta organisaatioilta, joiden palveluita verkkosivusto käyttää
  - Monet selaimet estävät > uudet/toiset toimintamallit
    - Hyödynnä ensimmäisen osapuolen dataa
    - Rakenna omaa asiakastietokantaasi
    - Pidä kontaktilistasi ajan tasalla
    - Suunnittele strategia tietokannan hyödyntämiseen
    - Muista juridiset pelisäännöt….

EVÄSTEET

Laki sähköisten viestinnän palveluista

- Evästeiden **tai muiden palvelun käyttöä kuvaavien tietojen käytöstä tulee informoida ja saada suostumus**

- Käyttö sallittua, jos käyttäjä on antanut **suostumuksensa** ja palvelun tarjoaja antaa ymmärrettävät ja kattavat tiedot tallentamisesta tai käytön tarkoituksesta
  - **Suostumus GDPR:n mukaan**
    - Yksilöity, selkeä, vapaaehtoinen…

- **Suostumusta ei tarvita** tallentamista tai käyttöä varten, joka on **välttämätöntä palvelun tarjoajalle sellaisen palvelun tarjoamiseksi, jota tilaaja tai palvelun käyttäjä on nimenomaisesti pyytänyt**
  - (Autentikointi, syötteet, tietoturva, saavutettavuus…)

- Tallentaminen ja käyttö on sallittua vain palvelun vaatimassa laajuudessa ja sillä ei saa rajoittaa yksityisyyden suojaa enempää kuin on välttämätöntä

EVÄSTEET

- **Suostumuksen pyytäminen ja toteutustapa suostumusten hallinnointiin** on palveluntarjoajan vastuulla

- Tyypillisimmin suostumusta pyydetään valintoja sisältävällä bannerilla

- Jotta suostumusta voidaan pitää asianmukaisena, tulisi suostumuksen sisältää ainakin seuraavia asioita:

    - Evästeiden ja vastaavien **tekniikoiden käytöstä on kerrottu selkeästi ja kattavasti** (erillinen cookie policy/evästeseloste, tiedot bannerissa tms.)
    - **Eritelty sivustolla tai palvelussa käytössä olevat erityyppiset evästeet ja muut tekniikat**, niiden käyttötarkoitus ja voimassaoloaika
    - Kerrottu, mikäli jollain kolmansilla osapuolilla on oikeus käsitellä evästetietoja (+ viitaukset näiden evästeselosteisiin)

- Traficomin ohjeistus palveluntarjoajille julkaistu syyskuussa 2021
https://www.traficom.fi/fi/toimintamme/saantely-ja-valvonta/evasteet?toggle=Ev%C3%A4steohjeistus%20palveluntarjoajille

EVÄSTEET

- Käyttäjien toimintojen seuraaminen evästeiden ja muiden seurantateknologioiden avulla on myös GDPR:n mukaista **henkilötietojen käsittelyä siltä osin, kun seurantaa toteutetaan käyttäjän tunnistavalla tavalla**
  - Mikäli mainostaja, mainosverkosto tai julkaisija pystyy suoraan tai epäsuoraan liittämään käytön tiettyyn henkilöön → **”pelkän” evästeen lisäksi myös henkilötieto**

- Varmistuttava kunkin tahon oikeudesta ylläpitää tietoja
  - Laadittava ja pidettävä saatavilla lainsäädännön edellyttämiä tietoja/annettava informaatiota → **tietosuojaseloste**
    - Rekisteröityjen oikeuksien käyttäminen

- Google Analytics

CASE – GOOGLE ANALYTICS

- Helmikuussa 2022 Euroopan tietosuojaviranomaiset totesivat Google Analyticsin käytön verkkosivuilla tietosuojalainsäädännön vastaiseksi.
  - Päätöksen antoi johtavana valvontaviranomaisena Ranskan valvontaviranomainen CNIL.
  - CNIL määräsi ranskalaisen verkkosivuston ylläpitäjän saattamaan henkilötietojen käsittelynsä tietosuoja-asetuksen mukaiseksi ja tarvittaessa lopettamaan Google Analytics -palvelun käytön nykyisillä ehdoilla.
  - Asiaa käsiteltiin eurooppalaisten tietosuojaviranomaisten välisessä yhteistyössä rajat ylittävässä menettelyssä, jossa TSV oli mukana osallistuvana valvontaviranomaisena.
- Euroopan tietosuojaviranomaiset ovat yhdessä arvioineet ehtoja, joilla Google Analyticsillä kerättyjä henkilötietoja on siirretty Yhdysvaltoihin sekä siirrosta rekisteröidyille aiheutuvia riskejä.
  - Päätöksen mukaan Googlen käyttöönottamat suojatoimet henkilötietojen siirroille Google Analyticsin kautta eivät ole riittäviä, eivätkä ne estä Yhdysvaltojen tiedustelupalvelun pääsyä tietoihin.
  - Google Analyticsin käyttö aiheuttaa tämän vuoksi riskin verkkosivuston käyttäjille, joiden tietoja kerätään ja siirretään Yhdysvaltoihin.

MITÄ PITÄÄ HUOMIOIDA?

- Selvitä, mitä evästeteknologiaa käytössä, millaista dataa kertyy, mihin evästeitä ja niiden perusteella kerättyä dataa käytetään ja onko kolmansilla tahoilla pääsyä dataan
- Evästeiden käytöstä pitää **informoida**
- Muiden kuin välttämättömien evästeiden käytölle tarvitaan GDPR:n mukainen **ennakkosuostumus**
- Suostumus rajaa sen, mitä evästeitä ja mihin tarkoituksiin niitä voidaan käyttää
- Suostumus pitää olla todennettavissa
- Suostumus pitää olla peruutettavissa
- Siltä osin kuin evästeiden avulla kerätään henkilötietoja, pitää noudattaa GDPR:n vaatimuksia henkilötietojen käsittelystä

TULEVA EPRIVACY-ASETUS

Tulevan ePrivacy-asetuksen kannalta tarkentuu mm. **viesteihin liittyvä metatieto** ja **evästeisiin vaaditun suostumuksen antamisen muoto**

- Asetus kieltäisi edelleen kaiken sähköisen suoramarkkinoinnin, johon loppukäyttäjänä oleva luonnollinen henkilö ei ole antanut suostumustaan
  - BtoB sallittua, aseman tai tehtävän perusteella tapahtuma > kansallinen tulkinta?

- Evästeiden käyttöä koskevaa sääntelyä yksinkertaistettaisiin (ehdotus)
  - Perusanalytiikkaevästeet sallittuja ilman suostumusta
  - Kolmansien osapuolten evästeiden asema vaakalaudalla (jo nyt suostumuksen ottaminen haastavaa)
  - Apple ja Google yms. muuttaneet jo käytäntöjä > uudet toimintamallit

- Normien rikkomisesta seuraisi sakko, joka voi olla suuruudeltaan jopa 4% yrityksen kokonaisliikevaihdosta
  - Linjassa EU:n tietosuoja-asetuksen kanssa

TIETOSUOJADOKUMENTAATIO JA TOIMINTATAVAT

CASE - RISKIEN TUNNISTAMINEN, TIETOSUOJAPERIAATTEIDEN NOUDATTAMINEN JA VAIKUTUSTENARVIOINTI

- Taksi Helsinki oli ottanut takseissa käyttöönsä ääntä ja kuvaa tallentavan kameravalvontajärjestelmän, mutta ei ollut arvioinut henkilötietojen käsittelyyn liittyviä riskejä ja vaikutuksia ennen käyttöönottoa
- Takseissa olevissa ilmoituksissa **ei kerrottu äänen tallentamisesta tai miten asiakkaat olisivat voineet saada tiedon siitä,** ja kanta-asiakasohjelman yhteydessä suoritetusta **automaattisesta päätöksenteosta ja profiloinnista ei kerrottu** tietosuojaselosteessa. Tietojen ei voitu katsoa olevan rekisteröityjen helposti saatavilla
- Äänitietojen käsittely **ei** myöskään ollut tietosuoja-asetuksen tietojen **minimoinnin periaatteen** mukaista
- Oikeutetun edun käyttöä käsittelyperusteena **ei oltu dokumentoitu**
- Puuttui **tietosuojaa koskeva vaikutustenarviointi (DPIA)** turvakameravalvonnasta, sijaintitietojen käsittelystä sekä kanta-asiakasohjelman yhteydessä harjoitetusta automaattisesta päätöksenteosta ja profiloinnista.
- Apulaistietosuojavaltuutettu määräsi korjaavia toimenpiteitä, kuten dokumentoimaan oikeutetun edun käsittelyperusteena ja laatimaan vaikutustenarvioinnin.

- Seuraamusmaksun suuruus oli 72 000 euroa, hallinto-oikeus alensi seuraamusmaksun määrän 60 000 euroon

TIETOSUOJADOKUMENTAATIO AJAN TASALLE

→ ARVIOI TARVE SUHTEESSA OMAAN TOIMINTAAN

- ? TIETOVARANTOJEN JA TIETOVIRTOJEN DOKUMENTOINTI
- ? TIETOSUOJA- JA KÄSITTELYSELOSTEET, EVÄSTESELOSTE
- ? TIETOJENKÄSITTELYSOPMUKSET
- ? TIETOSUOJA- JA TIETOTURVAPOLITIIKAT, SISÄISET OHJEISTUKSET
- ? PROSESSIKUVAUKSET (ML. TIETOTURVA-LOUKKAUKSET)
- ? VAIKUTUSTENARVIOINNIT (DPIA, DTIA)
- ? SUOSTUMUSTEN JA PÄÄTÖSTEN DOKUMENTOINTI
- ? TIETOSUOJAVASTAAVA / TIETOSUOJAORGANISAATIO

TAPOJA TÄYTTÄÄ TIETOSUOJAVELVOLLISUUKSIA

NYKYTILA-ANALYYSI, SUUNNITTELU

- Tee analyysi nykytilasta
- Mitä, missä, miksi, minne, kuinka kauan, miten dokumentoitu,
- Kartoita tietovirrat ja –varannot
- Ota huomioon suunnittelussa (palvelu, teknologia yms.)
- Muista säännölliset päivitykset

DOKUMENTOIDUT PROSESSIT

- Tunnista velvollisuutesi ja dokumentoi käsittelyyn liittyvien prosessien sekä tietosuojaperiaatteiden käytännön toteuttaminen
- Tunne myös alihankkijasi prosessit ja tee kirjallinen sopimus (DPA)

TIETOSUOJAVASTAAVA/-TIIMI

- Arvioi tarve; voidaan nimittää myös silloin, kun siihen ei ole velvollisuutta
- Ohjeistaa, seuraa tietosuojalain-säädännön jalkauttamista ja toimii yhteyspisteenä
- Tai ainakin tietosuojasta vastaava henkilö/tiimi

RISKIANALYYSIT JA VAIKUTUSTENARVIOINTI

- Asetus perustuu riskiperusteiselle lähestymistavalle
- Vaikutusten arviointi (DPIA) tarpeen mukaan (esim. profiloinnin osalta)
- Muista oletusarvoisen ja sisäänrakennetun tietosuojan periaate

TIETOTURVA

- Organisatorinen ja tekninen
- Tee toimenpidesuunnitelma tietosuojaloukkauksen varalle
- Käytännön tason ohjeistus, salassapito
- Kouluttaminen – myös uudet työtekijät

TIETOSUOJA-SELOSTEET/KÄYTÄNNÖT

- Rakenna luottamusta huolehtimalla avoimuudesta ja läpinäkyvyydestä
- Pidä saatavilla selosteet ja julkaise organisaation tietosuojapolitiikka
- Huolehdi myös muista rekisteröidyn oikeuksista

LEXIA ASIANAJOTOIMISTO

MARKUS MYHRBERG
markus.myhrberg@lexia.fi
@markusmyhrberg