Tarkenna fokusta! Lainsäädäntökokonaisuus ja IAB:n GDPR -ohjeistus

IAB tietosuojaseminaari 10.4.2018

Elli Laine

Tietosuojasääntelyn kokonaisuus

- Perustuslaki ja EU:n perusoikeuskirja
- ~~Henkilötietolaki (Henkilötietodirektiivi)~~
- EU:n tietosuoja-asetus (GDPR, 2018)
  - Suomessa annettu hallituksen esitys (9/2018) asetusta täydentävästä tietosuojalaista
- Tietoyhteiskuntakaari (Laki sähköisen viestinnän palveluista 1.6.2018 alkaen)
  - Perustuu sähköisen viestinnän tietosuojadirektiiviin
- Sähköisen viestinnän tietosuoja-asetus (ePrivacy Regulation) valmisteilla
  - Neuvottelut aloitetaan ilmeisesti syksyllä 2018

iab finland
Muutoksen tekijöille.

GDPR

GDPR – Kerrataan vielä

- Asetustasoinen säädös, jotka voimassa saman sisältöisenä koko EU:n alueella
  - *Korvaa henkilötietodirektiivin (1995)*
- Pääsääntöinen harmonisointi, jonkin verran kansallista liikkumavaraa
  - *Suomessa ehdotettu säädettäväksi uusi tietosuojalaki, joka täydentää tietosuoja-asetusta (Hallituksen esitys 9/2018 julkaistu)*
- Hyväksyttiin virallisesti toukokuussa 2016
- Siirtymäaika **-> <u>suoraan sovellettavaa lainsäädäntöä 25.5.2018</u>**

iab finland
Muutoksen tekijöille.

GDPR: Viime hetken tarkastuslista rekisterinpitäjälle

- Kartoitettava henkilötietojen käsittelyn tilanne:
  - Mitä henkilötietoja käsitellään?
  - Ovatko kaikki tiedot tarpeellisia?
  - Mihin tarkoituksiin tietoja käsitellään?
  - Mitkä ovat lailliset käsittelyperusteet?
  - Mihin tietoja siirretään tai luovutetaan? Onko tehty tietojenkäsittelysopimuksia?
  - Kuinka kauan henkilötietoja säilytetään? Miten tiedot hävitetään? Onko olemassa käytäntöjä tietojen poistamiseen tai tuhoamiseen?
- Luotava **sisäiset rakenteet**, joilla varmistetaan, että tietosuoja-asetuksen vaatimuksia noudatetaan
  - Esimerkiksi sisäiset vastuualueet, dokumentointi, koulutus
  - Tuntevatko kaikki henkilötietojen käsittelyyn osallistuvat seuran edustajat asetuksen asettamat velvoitteet?
- Arvioitava tarvetta nimittää **tietosuojavastaava**

iab finland
Muutoksen tekijöille.

GDPR: Viime hetken tarkastuslista rekisterinpitäjälle

- Otettava käyttöön tietosuojaperiaatteet toteuttavia toimenpiteitä ja dokumentoitava kaikki olennaiset toimenpiteet
  - Toteuttaa myös osoitusvelvollisuutta, koska dokumentaatiossa voidaan perustella tulkintaan liittyvät valinnat
- Suunniteltava menettelyt **rekisteröityjen oikeuksien** toteuttamiseksi
  - Miten vastataan esimerkiksi pyyntöön saada pääsy tietoihin?
  - Kenellä on oikeus tulla unohdetuksi?
  - Kuka organisaatiossa vastaa rekisteröityjen pyyntöihin?
- Laadittava asetuksen edellyttämät **tietosuojaselosteet / informointikäytännöt**
  - Verkkoon ”kerrostetut” kuvaukset
  - Haaste: Vältä informaatioähky mutta kerro käsittelystä riittävän läpinäkyvästi
- Seuraa viranomaisten ohjeistusta

iab finland
Muutoksen tekijöille.

GDPR: Viime hetken tarkastuslista käsittelijälle

- Otettava käyttöön **tekniset ja organisatoriset toimenpiteet** riittävän tietosuojan ja tietoturvan tason varmistamiseksi
- Laadittava **käsittelysopimukset** rekisterinpitäjien kanssa ja muokattava oma toiminta vastaamaan velvoitteita joihin sopimuksissa on sitouduttu
  - Onko oikeutta siirtää henkilötietoja **EU- ja ETA-alueen ulkopuolelle**?
  - Onko oikeutta käyttää **alihankkijoita**? Miten vastaavat tietosuojavelvoitteet vyörytetään alihankkijoille?
  - Miten **tietoturvaloukkauksista** ilmoitetaan rekisterinpitäjälle?
  - Onko sovittu, että käsittelijä saa käyttää tietoja **myös omiin tarkoituksiinsa** (rekisterinpitäjänä)?
- Laadittava asetuksen edellyttämät selosteet käsittelytoimista
- Seuraa viranomaisten ohjeistusta

iab finland
Muutoksen tekijöille.

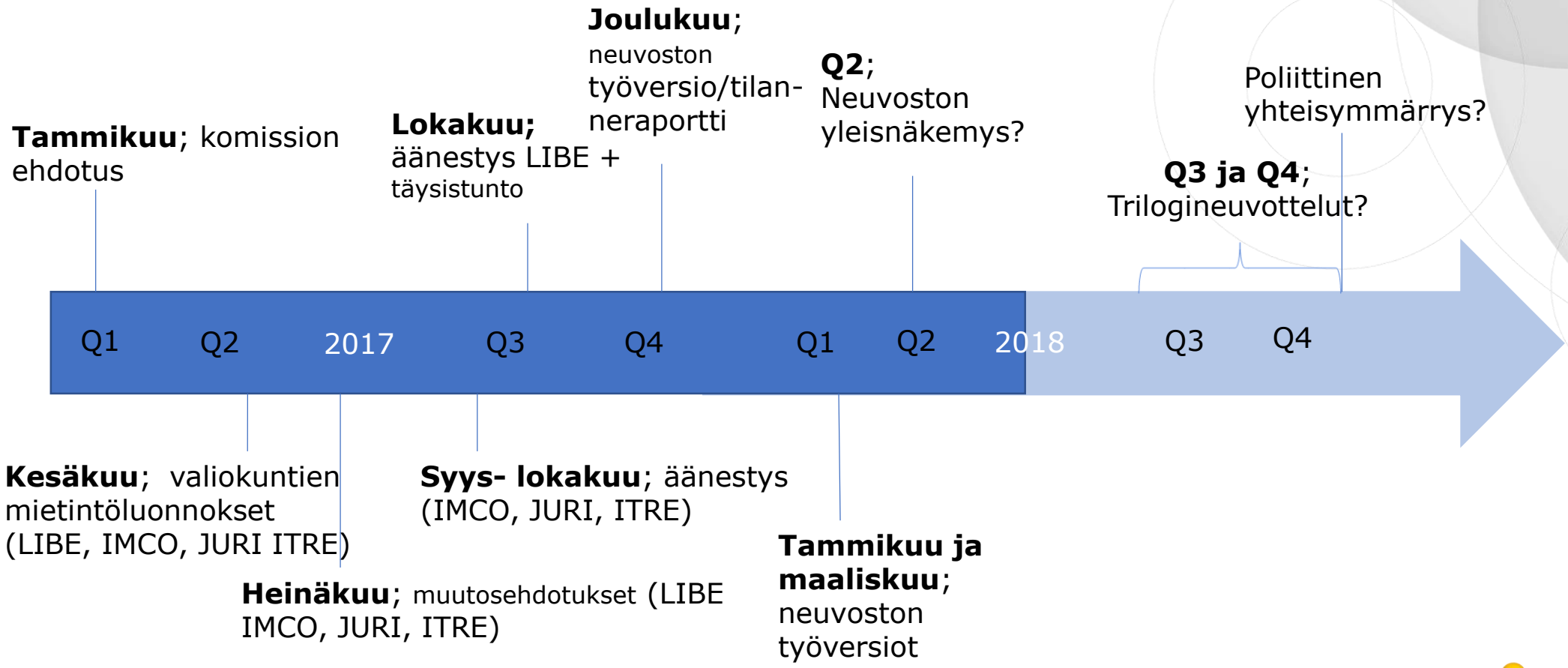
ePrivacy

ePrivacy – Mitä ja milloin?

- Asetustasoinen säädös, jotka voimassa saman sisältöisenä koko EU:n alueella
  - Korvaa Suomessa tietoyhteiskuntakaareen siirretyt entisen sähköisen viestinnän tietosuojalain pykälät
  - Esimerkiksi sääntely evästeistä, sähköisestä suoramarkkinoinnista ja sijaintitiedoista
- Kansallisen liikkumavaran määrä on vielä epäselvää
- Komissio ja parlamentti julkaisseet ehdotuksensa
  - Neuvoston lopullista versiota odotetaan vielä
- Trilogit syksyllä 2018? Asetus voimaan vuoden 2018 lopulla tai 2019-2020?
  - Siirtymäaika (kuten GDPR:n osalta)?

iab finland
Muutoksen tekijöille.

ePrivacy –asetuksen tilanne



iab finland
Muutoksen tekijöille.

ePrivacy: Mitä on odotettavissa?

- Sallitut käsittelyperusteet?
  - Nyt ePrivacy tarjoaa ainoastaan suostumuksen käsittelyperusteena
  - Entä oikeutettu etu ja muut GDPR:n mukaiset lailliset käsittelyperusteet?
- Miten suostumus evästeisiin annetaan?
  - Selaimen käyttöönoton yhteydessä?
  - Sivustokohtaisesti?
  - ”Ymmärtävätkö” nämä suostumukset toisiaan?

iab finland
Muutoksen tekijöille.

ePrivacy: Mitä on odotettavissa?

- Cookie Walls ja Tracking Walls –palomuurit jatkossa kiellettyjä?
  - Onko pakko tarjota palveluja jos käyttäjä ei anna suostumustaan evästeiden käyttöön?
  - Maksumuurit yleistyisivät jatkossa?
- Kolmansien osapuolten suorittama verkkoanalytiikka voi edellyttää käyttäjän nimenomaista suostumusta?
- Telemarkkinointi opt out:ista opt in –luvan varaiseksi?
- B2B –markkinointi opt out:ista opt in –luvan varaiseksi?
- ePrivacyn rikkomisesta ehdotettu vastaavia sanktioita kuin GDPR:ssä

iab finland
Muutoksen tekijöille.

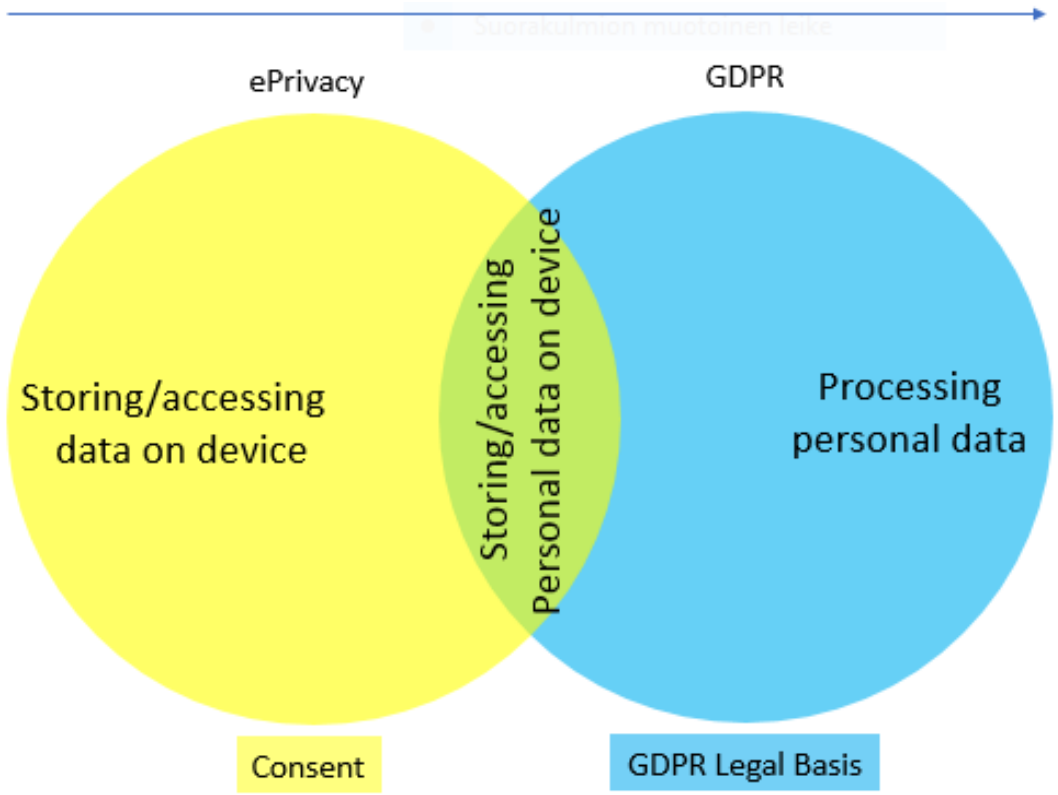
GDPR ja ePrivacy

GDPR:n ja ePrivacyn välinen hierarkia

- ePrivacy eli sähköisen viestinnän tietosuoja-asetus on tietosuoja-asetusta täydentävää erityislainsäädäntöä (***lex specialis***)
  - ePrivacy sääntelee erityisesti sähköisen viestinnän tietosuojaa
  - ePrivacy **täsmentää ja täydentää** GDPR:ää
  - GDPR:ää sovelletaan sen ohella siltä osin kuin ePrivacyssä ei ole säädetty toisin
- Valvovatko eri viranomaiset GDPR:n ja ePrivacy:n noudattamista?
- Miten yritys voi toimia lainmukaisesti kun ePrivacy on keskeneräinen?

iab finland
Muutoksen tekijöille.

GDPR:n ja ePrivacyn välinen hierarkia



- Evästeiden asettaminen edellyttää **suostumusta** ePrivacyn perusteella
- Henkilötietojen käsittely edellyttää GDPR:n laillista käsittelyperustetta (esimerkiksi suostumus tai oikeutettu etu)

iab finland
Muutoksen tekijöille.

IAB:n tietosuojatyöryhmän ohjeistukset

IAB:n ohjeistukset

- IAB Europe on tehnyt tulkintalinjauksia esimerkiksi henkilötiedon määritelmästä GDPR:n alla
- IAB Finlandin tietosuojatyöryhmä on valmistellut IAB Europen linjausten mukaista tietosuojaohjeistusta IAB:n jäsenistölle
  - Henkilötiedon määritelmä
  - Henkilötietojen käsittelyn roolit digimarkkinoinnissa
  - Käsittelysopimukset
- Ohjeistukset julkaistaan IAB:n verkkosivuilla

iab finland
Muutoksen tekijöille.

Henkilötiedon määritelmä

Henkilötiedot GDPR:n mukaan

- Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot
  - Jos henkilö on suoraan tai epäsuorasti tunnistettavissa erityisesti tunnistetietojen perusteella:

    nimi, henkilötunnus, sijaintitieto, ***verkkotunnistetieto****, tunnusomaiset fyysiset, geneettiset, psyykkiset, taloudelliset, kulttuuriset tai sosiaaliset tekijät*
  - Rekisterinpitäjän tai jonkun muun tunnistettavissa
  - Kohtuullisen todennäköisin keinoin
- Myös evästeet ja IP osoitteet (mutta arvioitava kontekstissa)
- Pseudonymisoidut tiedot ovat uusi henkilötietojen ryhmä
- **Laaja määritelmä!**

iab finland
Muutoksen tekijöille.

Pseudonymisoidut tiedot

- GDPR:n mukaan ”**pseudonymisoimisella**” tarkoitetaan henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja
  - Edellytyksenä on, että lisätiedot säilytetään erillään pseudonymisoidusta tiedosta
- Pseudonymisoituna tietona voidaan pitää myös tietoa, jota yritys ei voi yhdistää luonnolliseen henkilöön ilman lisätietoja
  - Esimerkiksi Adtech –yrityksen käsittelemä eväste ID, joka voitaisiin yhdistää tiettyyn henkilöön ainoastaan muiden tietojen avulla
- GDPR soveltuu pseudonymisoitujen tietojen käsittelyyn samaan tapaan kuin muidenkin henkilötietojen käsittelyyn
  - Pseudonymisoinnin avulla voidaan toteuttaa käsittelyn turvallisuuteen liittyviä velvoitteita ja osoitusvelvollisuuden täyttämistä

iab finland
Muutoksen tekijöille.

Evästeet henkilötietoina

- Evästeet voivat olla luonteeltaan:
  - Suoraan ilman lisätietoja henkilöön yhdistettävissä olevia **henkilötietoja**;
  - **Pseudonymisoituja** tietoja; tai
  - **Anonyymejä** tietoja joita ei voida yhdistää tunnistettavissa olevaan henkilöön edes lisätietojen avulla
- Ainoastaan verkkovierailun jälkeen poistettavat sessioevästeet voinee varmuudella rajata henkilötieto –määritelmän ulkopuolelle
- Miten pyydetään suostumus evästeiden käyttöön?

iab finland
Muutoksen tekijöille.

Roolit henkilötietojen käsittelyssä

Roolit henkilötietojen käsittelyssä

- Rekisterinpitäjä on se taho, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot
  - Esimerkiksi mainostaja tai julkaisija
- Ne tahot, jotka käsittelevät henkilötietoja ainoastaan rekisterinpitäjän lukuun toimeksiannon perusteella ovat henkilötietojen käsittelijöitä
  - Esimerkiksi mainostoimisto tai mediatoimisto
  - Entä tilanne, jossa mainostaja antaa budjetin ja mainostoimisto saa ”vapaat kädet” kampanjan suunnitteluun?
- Sama taho voi olla sekä rekisterinpitäjän että käsittelijän rooleissa samassa sopimussuhteessa

iab finland
Muutoksen tekijöille.

Käsittelysopimukset

Käsittelysopimus (DPA) vai sopimus tietojen luovutuksesta (data sharing agreement)?

- Roolit ymmärrettävä ja kuvattava sopimuksessa
  - Rekisterinpitäjä määrittelee miten ja miksi henkilötietoja käsitellään
  - Rekisterinpitäjä voi kuitenkin delegoida käsittelijälle päätöksen ja toimenpiteet siitä miten tietoja teknisesti käsitellään
  - Arvioinnissa otetaan huomioon mm. osapuolten todellinen toiminta, vaikutusvallan laajuus, sopimuksen kirjaukset, käsittelijäksi nimetyn liikkumavara
  - Samalla toimijalla voi samassa suhteessa olla useita rooleja
- Jos sopimusosapuolilla on useita rooleja, on kuvattava mitä käsittelytoimenpiteitä tehdään missäkin roolissa
  - Kahden rekisterinpitäjän välisen tietojen luovutussopimuksen sisältöä ei ole määritelty GDPR:ssä
  - Mahdollista laatia ”hybridisopimus”

iab finland
Muutoksen tekijöille.

Käsittelysopimukset

- Rekisterinpitäjän ja käsittelijän on laadittava GDPR:n mukainen kirjallinen sopimus henkilötietojen käsittelystä
  - ”Pakko sopia”
  - Esimerkiksi sopimukset mainostajan ja mediatoimiston välillä
- Käsittelysopimuksissa huomioitava esimerkiksi:
  - Käsittelyn kohde, käsittelyn kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi, rekisteröityjen ryhmät, rekisterinpitäjän velvollisuudet ja oikeudet
  - Henkilötietojen käsittelijä saa käsitellä henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti
  - Alihankkijoiden (alikäsittelijöiden) käyttö
  - Vaaditut toimenpiteet käsittelyn turvallisuuden varmistamiseksi
  - Rekisterinpitäjän tarkastusoikeus
- Suositeltavaa huomioida myös esimerkiksi vastuunrajoitukset, käsittelijän oikeus veloittaa rekisterinpitäjän avustamisesta sekä käsittelyn päättymiseen liittyvät toimenpiteet

iab finland
Muutoksen tekijöille.