Digitaalisen liiketoiminnan tietosuojafoorumi 22.3.2017 – rekisteröidyn oikeudet

Päivi Antikainen, yksikönjohtaja

www.lvm.fi/tietosuojafoorumi
@lvmfi

LIIKENNE- JA VIESTINTÄMINISTERIÖ

LVM 1892–2017

Suomi Finland 100

Digitaalinen liiketoiminta edellyttää vahvaa tietosuojaa

Tilanne 16.3.2017

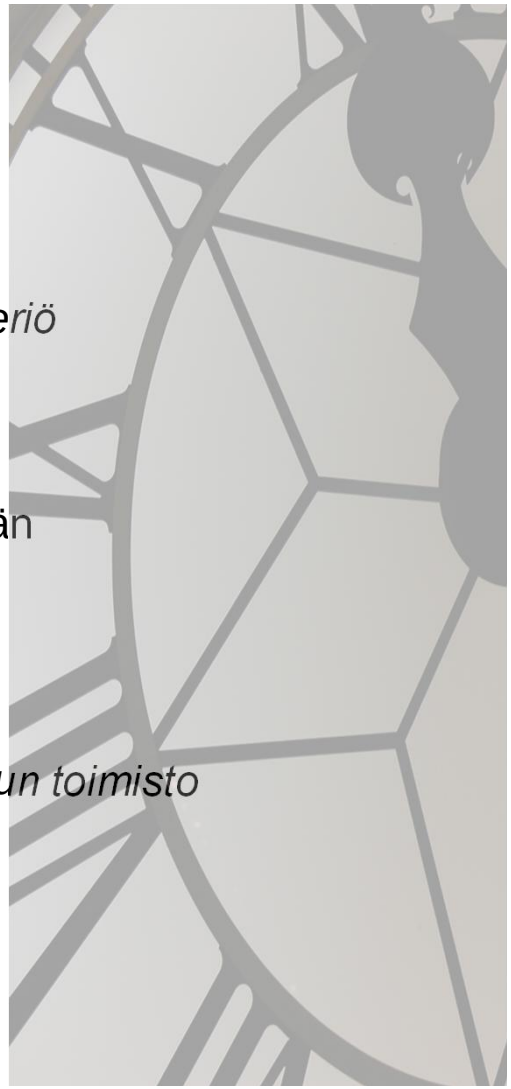
LIIKENNE- JA VIESTINTÄMINISTERIÖ

Ohjelma

13.00 Tilaisuuden avaus
Päivi Antikainen, yksikönjohtaja, liikenne- ja viestintäministeriö

13.10 Rekisteröidyn oikeudet: säännöistä käytännön toteutukseen
Jari Perko, toimitusjohtaja, Asiakkuusmarkkinointiliitto
13.30 Rekisteröityjen oikeuksien toteuttaminen henkilötietojen käsittelijän näkökulmasta
Jussi Tokola, General Counsel, Tieto
13.50 Ajankohtaista tietosuoja-asiaa
Miten toteutan rekisteröidyn oikeudet?
Heljä-Tuulia Pihamaa, toimistopäällikkö, tietosuojavaltuutetun toimisto

14.20 Työpajakeskustelut
14.50 Työpajakeskusteluiden purku



LIIKENNE- JA VIESTINTÄMINISTERIÖ

Rekisteröidyn oikeudet: säännöistä käytännön toteutukseen

Jari Perko, ASML
@asiakkuus –www.asml.fi

LVM / Digitaalisen liiketoiminnan tietosuojafoorumi 22.3.2017

YKSILÖ VS. RYHMÄ/YLEISÖ

Yrityksen asiakastiedon käsittelyssä ei pääosin ole seurata yksittäistä henkilöä vrt. ”intrusion of privacy”-ajattelu.

➔ Kehitetään asiakkuuksien arvoa ja elinkaarta.

➔ Aiemmin massana käsitellyn ryhmän jakamisesta pienempiin ryhmiin raja-arvojen ja ryhmäparametrien perusteella. Paremmat palvelut, paremmat sisällöt.

GDPR:n henki enemmän kallellaan ”intrusion of privacy”-suuntaan?

ASML

”Paljollako myyt selainhistoriasi?”

➔ **UK:ssa kansa vastasi:** Hinta 934£

➔ Mainostajat maksavat UK:ssa selainhistoriasta osana selainyleisöä 0,00014£/kpl (TotallyMoney Study, UK)

Tietosuoja on hyvin mielipide-, kulttuuri- ja tietoriippuvaista – pultattuja elementtejä on vähän. Hyviä tapoja tehdä oikein voi olla lukuisia.

ASML

KARKEISTAEN:

Milloin on kyse hiekanjyvän asemasta kauhaisussa?

Milloin on kyse ainutlaatuisen jalokiven suojaamisesta?

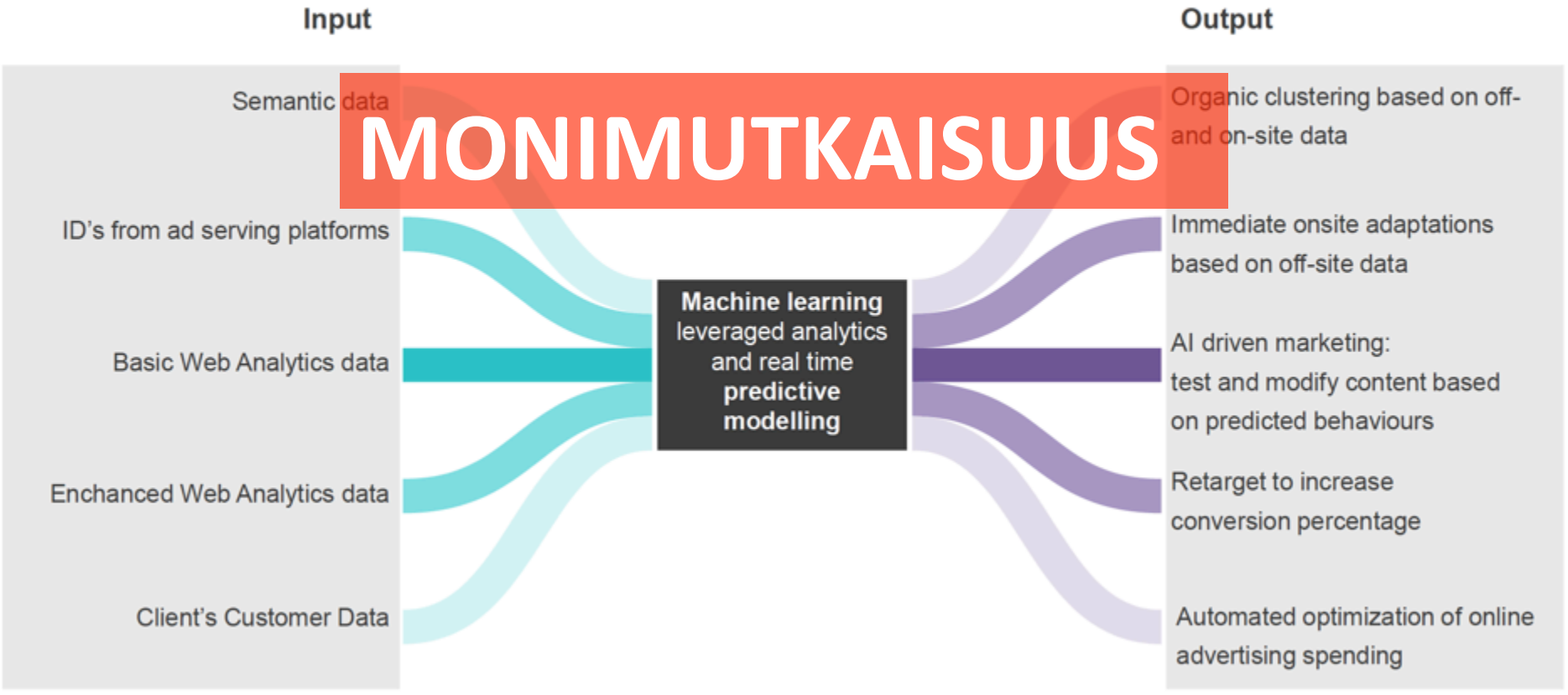
A. Henkilötieto ➔ Massadata ➔ Parempi palvelu/sisältö

B. Henkilötieto ➔ Henkilötieto ➔ Parempi palvelu/sisältö

Henkilötiedon turvallinen ”raaka-ainekäyttö” mahdollistaa huikeita hyötyjä koko yhteiskunnassa.

uber.movement.com

Future Development Streams



MONIMUTKAISUUS

annalect

Bugeja?

Yrityksen ei tietosuojainformoinnissaan (13 art) tarvitse informoida rekisteröidyltä keräämiään tietoja!
”*Kyseessä olevat henkilötietoryhmät*” täytyy informoida jos tiedot kerätään muualta kuin rekisteröidyltä (14 art)

➔ Totta kai yritys kertoo mitä tietoja kerää asiakkaistaan mutta miten erottaa ”bugit ominaisuuksista” GDPR:n eri artikloissa?

ASML

Offline-ajan rakenteita?

Right of Access - 15.3. artikla
”Rekisterinpitäjän on toimitettava jäljennös käsiteltävistä henkilötiedoista. Jos rekisteröity pyytää useampia jäljennöksiä, rekisterinpitäjä voi periä niistä hallinnollisiin kustannuksiin perustuvan kohtuullisen maksun. Jos rekisteröity esittää pyynnön sähköisesti, tiedot on toimitettava yleisesti käytetyssä sähköisessä muodossa, paitsi jos rekisteröity toisin pyytää.”

➔ Jäljennösten toimittaminen ”datajoen” virtauksesta on vanhan liiton rakenne ja ratkaisu. Pitää päästä tarkoituksenmukaiseen käytäntöön.

ASML

Skaalautuvuus - Siirrettävyys?

1 Yrityksessä on vain suostumuksen perustuva asiakaspaneeli.
➔ Mikä tolkku on implementoida Data Portability paneelin osalta?

2 Viestintäpalveluissa on taustadataa saapuvista yhteyksistä kuluttajalle ➔ Siirrettävyys: Raskas, kallis, kukaan ei tarvitse…

Siirrettävyys ”huutaa” järkeviä tulkintoja.

ASML

Back Up

GDPR sopii huonosti back up'eihin (49% käyttää nauhoja) ➔
Pitäisi löytää ”täyspäinen” tulkinta-ratkaisu – ei pidä johtaa kalliiseen ”pakkovaihtoon”.

- Back upit ovat usein monoliittinen ”media” joissa ei ole haku- ja käsittelytoimintoja.
- Turvallinen ja hyvin suunniteltu back up-toiminto suojaa rekisteröityjen kokonaisuutta ja rekisterinpitäjää.

➔ Back up-säilytys voisi jatkua ”sopivasti tulkitun” pseudonymisointiartiklan (11 art) pohjalta?

ASML

Mustavalkoiset tulkinnat sopivat huonosti Privacy by Design –ajatteluun.

- Yritysten kyettävä perustelemaan paremmin ratkaisunsa.
- Viranomaisten vältettävä liian kategorisia Sallittu/Kielletty-tulkintarakenteita.


ASML
Parturiketju
Parturi
Vuokratuoli-yrittäjä
CRM/viestintäinfra
Asiakastiedot
GDPR?

Ihminen, luonnollinen ”profiloija”

Vastasyntynyt alkaa heti kerätä valtavasti dataa erotellakseen riittävällä tavalla ympäristönsä eri asioita toisistaan.

Datan käsittely ja johtopäätökset ovat
paljolti likiarvoista, ennusteluonteista ja iteroivaa.

Ihmisen ja yrityksen elämä on pääosin ”likiarvoista analytiikkaa”.
Ethics by Design needed.
Täydellinen accountability mahdotonta…

Clip: pbs.org/program/human-face-big-data/

Henkilötietojen käsittelijä ja rekisteröityjen oikeudet

Digitaalisen liiketoiminnan tietosuojafoorumi 22.3.2017
– miten toteutan rekisteröidyn oikeudet?

Jussi Tokola

General Counsel
Tieto, Legal
jussi.tokola@tieto.com

Public

tieto

Tieto is the leading Nordic software and services company

3000 Projects annually

Serving Nordic clients since **1968**

Around **1500** clients

Turnover of approximately **€1.5 billion**

Employing **13000** experts globally, in close to **20** countries

Serving customers in over **85** countries worldwide

Investments in technology and services more than **€100 millio n*** per year

*incl. capital expenditure and operational costs

Asetuksen roolit



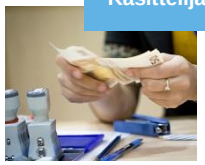
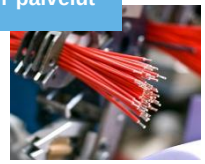
Rekisteröidyt
- Käsittelyä koskevat tiedot
- Käsittelyn lainmukaisuus
- Oikeuksia koskevat pyynnöt
- Tietomurrosta ilmoittaminen
- Vahingonkorvausoikeus

Rekisterinpitäjä
- Käsittelyn periaatteet
- Tilivelvollisuus
- Sisäänrakennettu oletusarvoinen tietosuoja
- Tietoturva
- Rekisteröityjen oikeuksien toteuttaminen
- Käsittelijöiden hallinta
- Henkilötietojen siirrot

Tietosuojaviranomainen
- Valvonta
- Tietomurrosta ilmoittaminen
- Ennakkokuuleminen
- Määräysvalta
- Hallinnolliset sakot

Henkilötietojen käsittelijä
- Takeet käsittelystä
- Tietosuojalausekkeet
- Käsittelyn ohjeet
- Avustaminen oikeuksissa
- Tietoturva
- Henkilötietojen siirrot

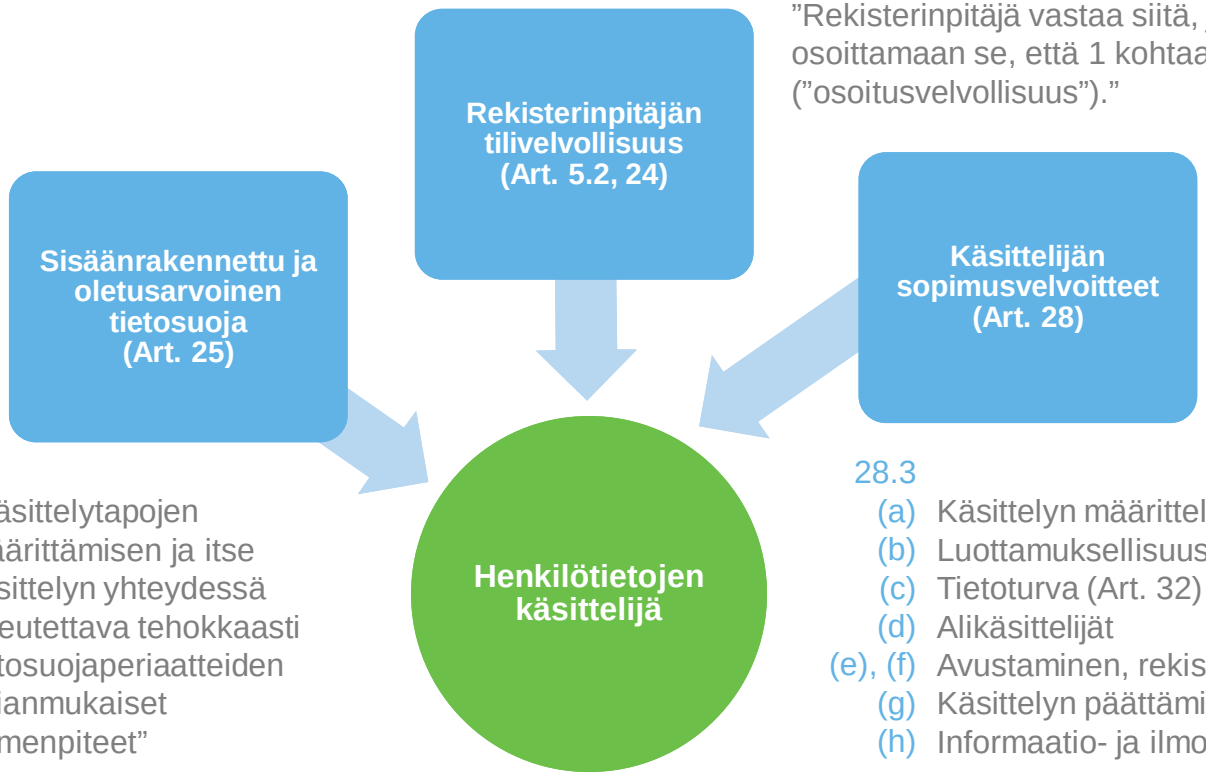
Käsittelijän palvelut

Henkilötietojen käsittelijän alihankkijat

Public

Käsittelijän asema



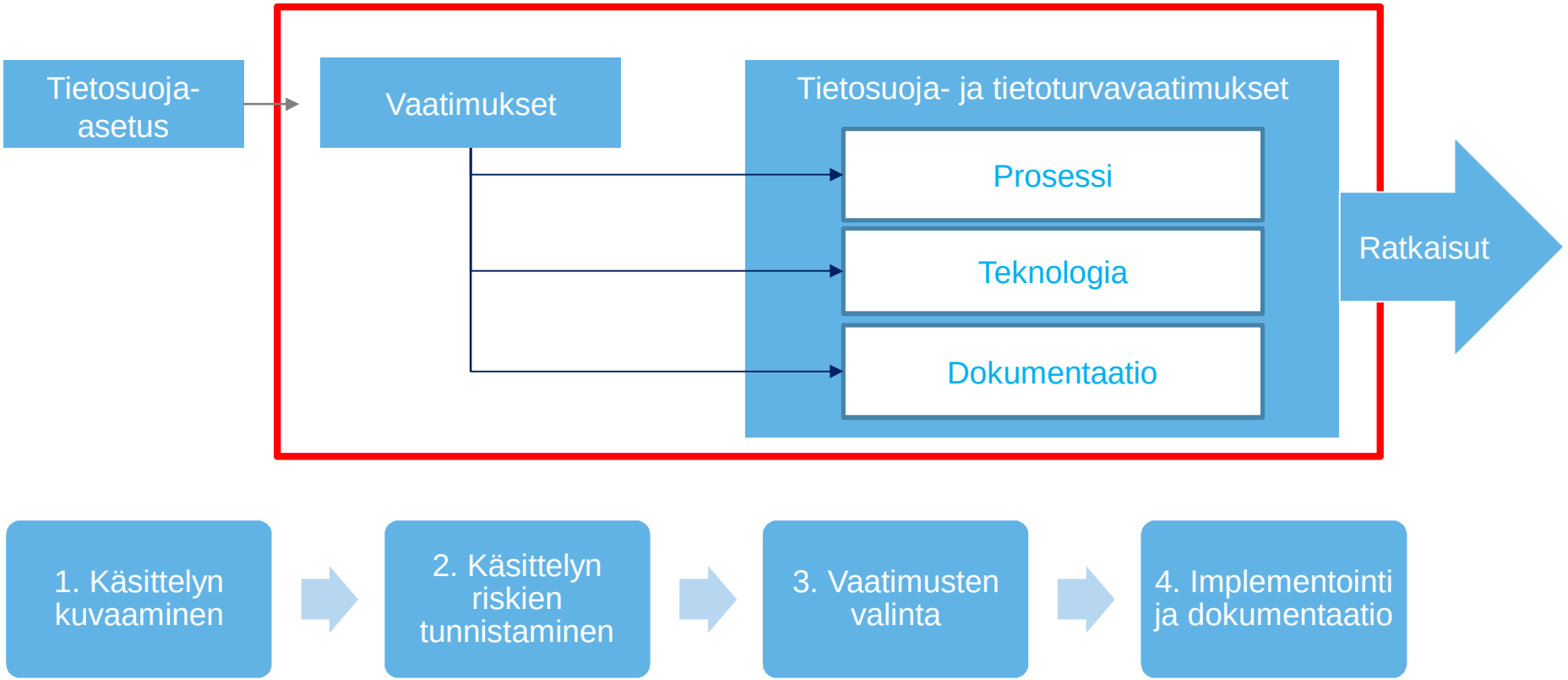
”Rekisterinpitäjä vastaa siitä, ja sen on pystyttävä osoittamaan se, että 1 kohtaa on noudatettu (”osoitusvelvollisuus”).”

”Käsittelytapojen määrittämisen ja itse käsittelyn yhteydessä toteutettava tehokkaasti tietosuojaperiaatteiden asianmukaiset toimenpiteet”

28.3

(a) Käsittelyn määrittely, ohjeet ja henkilötietojen siirrot
(b) Luottamuksellisuus
(c) Tietoturva (Art. 32)
(d) Alikäsittelijät
(e), (f) Avustaminen, rekisteröityjen oikeudet (luku III) ja Art. 32-36
(g) Käsittelyn päättäminen
(h) Informaatio- ja ilmoitusvelvoitteet, auditointi

Vaatimusten tunnistaminen ja ratkaisujen suunnittelu



Hankinta ja sopiminen

Esimerkkejä tarjouspyynnön vaatimuksista

Vaatimus	Peruste
Toimittakaa kuvaukset tietosuojasäännöistä ja prosesseista	Tilivelvollisuus (Art. 24)
Toteuttaako palvelu rekisteröidyn oikeuden saada pääsy tietoihin? Kuvatkaa prosessit ja tekninen toteutus.	Rekisteröityjen oikeudet (Art. 15)
Toteuttaako palvelu oikeuden siirtää tiedot järjestelmästä toiseen? Kuvatkaa prosessit ja tekninen toteutus.	Rekisteröityjen oikeudet (Art. 20)
Toimittakaa kuvaukset järjestelmän tietoturvasta	Käsittelyn turvallisuus (Art. 32)
Toimittakaa kuvaukset tietojen käsittely- ja säilytysajoista	Säilytyksen rajoittaminen (Art. 5.1 (e))

Suositus

- Kartoita olennaiset tietosuoja-asetuksen vaatimukset hankinnoissa tilivelvollisuuden täyttämiseksi ja osapuolten velvoitteiden täsmentämiseksi

Rekisteröityjen oikeudet

3 (e) ottaen huomioon käsittelytoimen luonteen auttaa rekisterinpitäjää asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä mahdollisuuksien mukaan täyttämään rekisterinpitäjän velvollisuuden vastata pyyntöihin, jotka koskevat III luvussa säädettyjen rekisteröidyn oikeuksien käyttämistä;

- Toimitettavat tiedot (Art. 13, 14)
- Pääsy tietoihin (Art. 15)
- Oikeus tietojen oikaisemiseen (Art. 16)
- Oikeus tulla unohdetuksi (Art. 17)
- Oikeus käsittelyn rajoittamiseen (Art.18)
- Oikaisua tai poistoa koskeva ilmoitusvelvollisuus (Art. 19)
- Oikeus siirtää tiedot (Art. 20)
- Vastustamisoikeus (Art. 21)
- Profilointi (Art. 22)

Rekisteröityjen oikeudet

”Ottaen huomioon käsittelytoimen luonteen auttaa rekisterinpitäjää asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä mahdollisuuksien mukaan” Miten avustaminen toteutetaan: • Automaatio, manuaalisuus • Huomioi myös aikarajat rekisteröityjen pyynnöille
Monimutkaiset ympäristöt: • Kartoita, mikä taho pystyy toteuttamaan tietyn oikeuden tai toiminnallisuuden (sovellustukipalvelu vs. hosting-palvelu)
Yksityiskohtainen sopiminen perusteltua suhteuttaa myös käsittelypalvelun luonteeseen
Avustusvelvoitteen hinnoittelua ei mainittu asetuksessa → sovi erikseen, jos osa kiinteää hintaa → arviot oikeuksien käyttämisen laajuudesta

Kysymyksiä?

Public

tieto

Kansalaisten vahvistuvat oikeudet tietosuoja-asetuksessa

Toimistopäällikkö Heljä-Tuulia Pihamaa
LVM:n tietosuojafoorumi
22.3.2017

TIETOSUOJAVALTUUTETUN TOIMISTO

Ajankohtaista tietosuojavaltuutetun toimistosta

- Tietosuojatyöryhmä WP 29
  - Co-operation subgroup
    - Viranomaisten välisen yhteistyön prosessit ja sanktiot
  - Enforcement subgroup
    - Älykkäät lelut, Microsoft, jne.
  - Technology subgroup
    - E-privacy Regulation
  - Future of Privacy subgroup
    - Ohjeiden kommentointia, EDPB:n perustaminen
  - WP 29 seuraava kokous 4.-5.4., jonka jälkeen WP 29 Fablab (teemat: profilointi, suostumus, DBN)
  - Privacy Shield

- Kansalliset työryhmät
  - TATTI-työryhmä
  - Direktiivityöryhmä

30 vuotta rekisteröidyn oikeuksia

Tietosuoja-asetus rekisteröityjen kannalta

- Läpinäkyvyyden ja avoimuuden lisääminen
- Henkilötietojen käsittelyyn liittyvät oikeudet päivitetty digitaaliselle aikakaudelle
- Rekisteröityjen mahdollisuudet valvoa ja vaikuttaa omien henkilötietojen käsittelyyn paranevat
- Henkilötietojen suojan yhdenmukaistaminen EU:n jäsenvaltioissa
- Valvontaviranomaisten toiminnan tehostaminen toimivaltojen kautta
- Lasten erityisaseman huomioiminen

Viranomaisen rooli rekisteröityjen oikeuksien toteuttamisessa

- Rekisteröidyn oikeussuojakeino
- Viranomaisen rooli aktualisoituu silloin, kun oikeuksia ei toteuteta
- Toimivaltaa määrätä rekisterinpitäjää toteuttamaan rekisteröidyn pyyntö

TIETOSUOJA-ASETUKSEN MUKAISET REKISTERÖIDYN OIKEUDET

TIETOSUOJAVALTUUTETUN TOIMISTO

Yksityiskohtaiset säännöt rekisteröidyn oikeuksien toteuttamista varten

- Tietosuoja-asetuksen 12 artiklaa on luettava yhdessä muiden III luvun artikloiden kanssa

- Menettelysäännöt oikeuksien toteuttamiselle
  - Pääsääntö kirjallisesti, tapauksen mukaan sähköisesti
  - Määräajat (1-3 kk)
  - Pääsääntönä maksuttomuus
  - Oikeus tehdä valitus valvontaviranomaiselle
  - Rekisteröidyn henkilöllisyyden varmistaminen

”Vanhat oikeudet”

Oikeus saada läpinäkyvää informaatiota

- Kun tiedot kerätään suoraan rekisteröidyltä
- Kun tiedot kerätään muualta kuin rekisteröidyltä
- Tietosuoja-asetuksen mukainen informointivelvoite on tietosisällöllisesti henkilötietolain mukaista informointivelvoitetta laajempi ja yksityiskohtaisempi
- Ymmärrettävyys, erottuvuus ja selkeys rekisteröidyn kannalta
- Vakiomuotoiset kuvakkeet; tavoitteena antaa mielekäs yleiskuva henkilötietojen käsittelystä

Oikeus saada pääsy tietoihin

- Oikeuden ydin sama kuin nykyisin tarkastusoikeuden
    - Oikeus saada tietää, käsitelläänkö itseä koskevia henkilötietoja ja jos, mitä tietoja
- Oikeuden toteuttamista koskevat säännöt poikkeavat hieman henkilötietolaista

Oikeus tietojen oikaisemiseen ja oikeus tietojen poistamiseen

- Oikeus tietojen oikaisemiseen vastaa henkilötietolain virheen korjaamista koskevaa sääntelyä

- ”Oikeus tulla unohdetuksi” ei uusi oikeus
  - Tietosuoja-asetuksessa on säädetty edellytyksistä, milloin ko. oikeus tulee sovellettavaksi ja rajoituksista, jolloin oikeutta ei sovelleta
  - Vahvistettu EUTI:n ns. Google Spain ratkaisussa

Automatisoidut yksittäispäätökset; profilointi mukaan luettuna

- Oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automatisoituun käsittelyyn
  - Jolla on rekisteröityä koskevia oikeusvaikutuksia tai vaikuttaa häneen vastaavalla tavalla merkittävästi
- Poikkeukset
  - Tämä on välttämätöntä sopimuksen tekemistä/täytäntöönpanoa varten
  - Siitä säädetään laissa, jossa on säädetty myös asianmukaisista suojatakeista
  - Perustuu rekisteröidyn nimenomaiseen suostumukseen
- Oikeus vaatia, että tiedot käsittelee rekisterinpitäjän puolesta luonnollinen henkilö sekä oikeus esittää kantansa ja riitauttaa päätös
- Ei voi pääsääntöisesti perustua arkaluonteisiin tietoihin

Vastustamisoikeus

- Rekisteröidyllä on oikeus vastustaa itseään koskevien tietojen käsittelyä JOS
  - Käsittelyn oikeusperusteena on yleistä etua koskevan tehtävän suorittamiseksi/rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi tai rekisterinpitäjän tai kolmannen oikeutetun etujen toteuttaminen
- Jos rekisteröity käyttää oikeuttaan, rekisterinpitäjä ei saa enää käsitellä henkilötietoja, PAITSI jos rekisterinpitäjä voi osoittaa, että tähän on huomattavan tärkeä ja perusteltu syy

- Suoramarkkinoinnin osalta absoluuttinen vastustamisoikeus

”Uudet oikeudet”

Oikeus käsittelyn rajoittamiseen

- Rekisterinpitäjä voi pääsääntöisesti ainoastaan säilyttää tietoja

- Sovelletaan tietyissä tilanteissa
  - Esim. jos rekisteröity kiistää henkilötietojen paikkansapitävyyden tai käsittely on lainvastaista

- Ilmoitettava rekisteröidylle, jos käsittelyä koskeva rajoitus poistetaan

Oikeus siirtää tiedot järjestelmästä toiseen

- Tarkastusoikeuden luonnollinen evoluutio
- Sovelletaan,
  - jos käsittely perustuu suostumukseen tai sopimukseen; ja
  - käsittely suoritetaan automaattisesti
- Rekisteröidyn oikeus saada henkilötiedot, jotka hän ”on toimittanut” rekisterinpitäjälle, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa
- Rekisteröidyllä on oikeus siirtää tiedot toiselle rekisterinpitäjälle. Tiedot on oikeus saada siirrettyä suoraan, jos se on teknisesti mahdollista
- Oikeuden toteuttaminen ei saa vaikuttaa haitallisesti muiden oikeuksiin ja vapauksiin

Rekisteröidyn oikeus tulla informoiduksi henkilötietojen tietoturvaloukkauksista

- Pääsääntöisesti, jos henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin
- Ilmoitettava ilman aiheetonta viivytystä
- Ilmoitusta ei tarvitse tehdä:
  - Toteutetaan asianmukaiset suojatoimet (salaus); tai
  - Toteutetaan jatkotoimenpiteet, joilla voidaan varmistaa, ettei riski todennäköisesti toteudu; tai
  - Vaatisi kohtuutonta vaivaa → julkinen tiedonanto tai vastaava toimenpide
- Valvontaviranomainen voi edellyttää ilmoituksen tekemistä

Rajoitukset

- Jos rekisterinpitäjä ei pysty tunnistamaan rekisteröityä
  - Paitsi jos rekisteröity antaa oikeuksia käyttääkseen lisätietoja, joiden avulla hänet pystytään tunnistamaan
- Artiklakohtaiset ja 9 luku
- Tietosuoja-asetuksen 23 artiklan perusteella kansallisen lainsäädännön nojalla?
  - TATTI -työryhmä

Rekisteröityjen oikeudet rekisterinpitäjän näkökulmasta

- Rekisterinpitäjän velvollisuus on toteuttaa rekisteröityjen oikeuksia
  - Osoitusvelvollisuus
- Tietojen minimoinnin periaate ja säilytysaikojen määrittely
- Mitkä oikeudet tulevat sovellettavaksi omaan toimintaan?
  - Mm. käsittelyn oikeusperusteen määrittely
- Valmiudet toteuttaa oikeuksia?
- Tietosuojavastaavan rooli?
- Henkilötietojen käsittelijän rooli?

Huoneentaulu rekisteröityjen oikeuksista

- Oikeus saada läpinäkyvää informaatiota
  - Silloin, kun henkilötiedot kerätään suoraan rekisteröidyltä
  - Silloin, kun henkilötiedot kerätään muualta kuin rekisteröidyltä
- Oikeus saada pääsy tietoihin (*tarkastusoikeus*)
- Oikeus tietojen oikaisemiseen (*virheen oikaisu*)
- Oikeus tietojen poistamiseen (”oikeus tulla unohdetuksi”)
- Oikeus käsittelyn rajoittamiseen
- Oikeus siirtää tiedot järjestelmästä toiseen
- Vastustamisoikeus
- Automatisoidut yksittäispäätökset; profilointi mukaan luettuna
- Oikeus tulla informoiduksi henkilötietojen tietoturvaloukkauksista
- Lasten erityisasema
- Oikeus saada valvontaviranomaiselta apua
- Oikeus luottaa tietoturvaan

Tietosuojavaltuutetun kotisivut:

www.tietosuoja.fi

Tietosuoja-asetus teksti:

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil:ST_5419_2016_INIT