Tietosuojamyytit ja usein kysytyt kysymykset

Tietosuojafoorumi 28.2.2018

@lvmfi
#tietosuojafoorumi

LIIKENNE- JA VIESTINTÄMINISTERIÖ

Ajankohtaista

Datatalousfoorumi

Miten dataliiketoiminnan rattaat saadaan pyörimään?

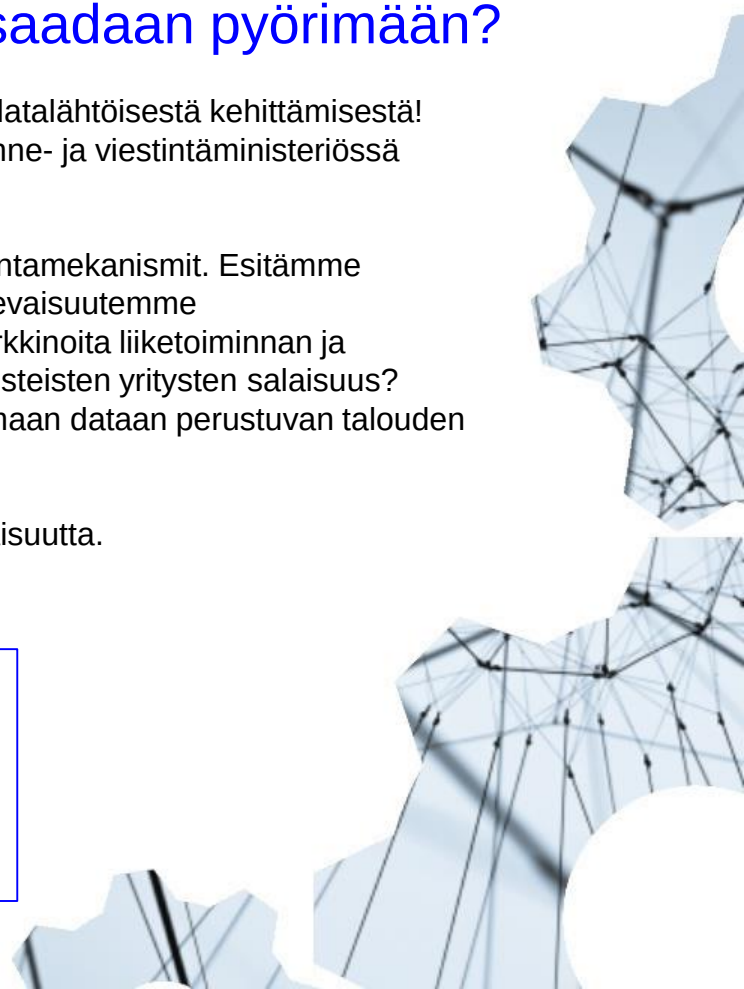
Tervetuloa kuulemaan ja keskustelemaan liiketoiminnan datalähtöisestä kehittämisestä! Datatalousfoorumi käynnistyy 14.3.2018 klo 9.30-12 liikenne- ja viestintäministeriössä (Eteläesplanadi 16).

Ensimmäisen tilaisuuden teemana on Datatalouden toimintamekanismit. Esitämme asiantuntijoiden kanssa ratkottavia haasteita: Mikä on tulevaisuutemme teknologiavetoisessa datataloudessa? Miten data luo markkinoita liiketoiminnan ja kokonaistalouden eduksi? Mikä on menestyvien dataperusteisten yritysten salaisuus? Miten toimia yhteen datataloudessa? Tervetuloa rakentamaan dataan perustuvan talouden edellytyksiä!

Kutsu ja ohjelma lähetetään noin kolme viikkoa ennen tilaisuutta.
Tilaisuuden avaa ministeri Anne Berner.

Lisätietoja: taru.rastas(a)lvm.fi, tuomas.kaivola(a)lvm.fi

Miksi datatalousfoorumi?
Dataa tuotetaan kiihtyvällä tahdilla, kun palvelut digitalisoituvat ja laitteista, prosesseista ja ihmisistä kerätään tietoa. Datataloudessa tehokkaat ja käyttäjälähtöiset palvelut luodaan tiedolla ja sen liikkuvuudella. Samalla datan taloudellinen merkitys kasvaa. Foorumin tarkoituksena on tehdä näkyväksi datatalouden kehitystoimia, oppia esimerkeistä ja edistää dataperusteisen liiketoiminnan edellytyksiä. Foorumi liittyy *Digitaalisen liiketoiminnan käasvuympäristö* -kärkihankkeeseen.



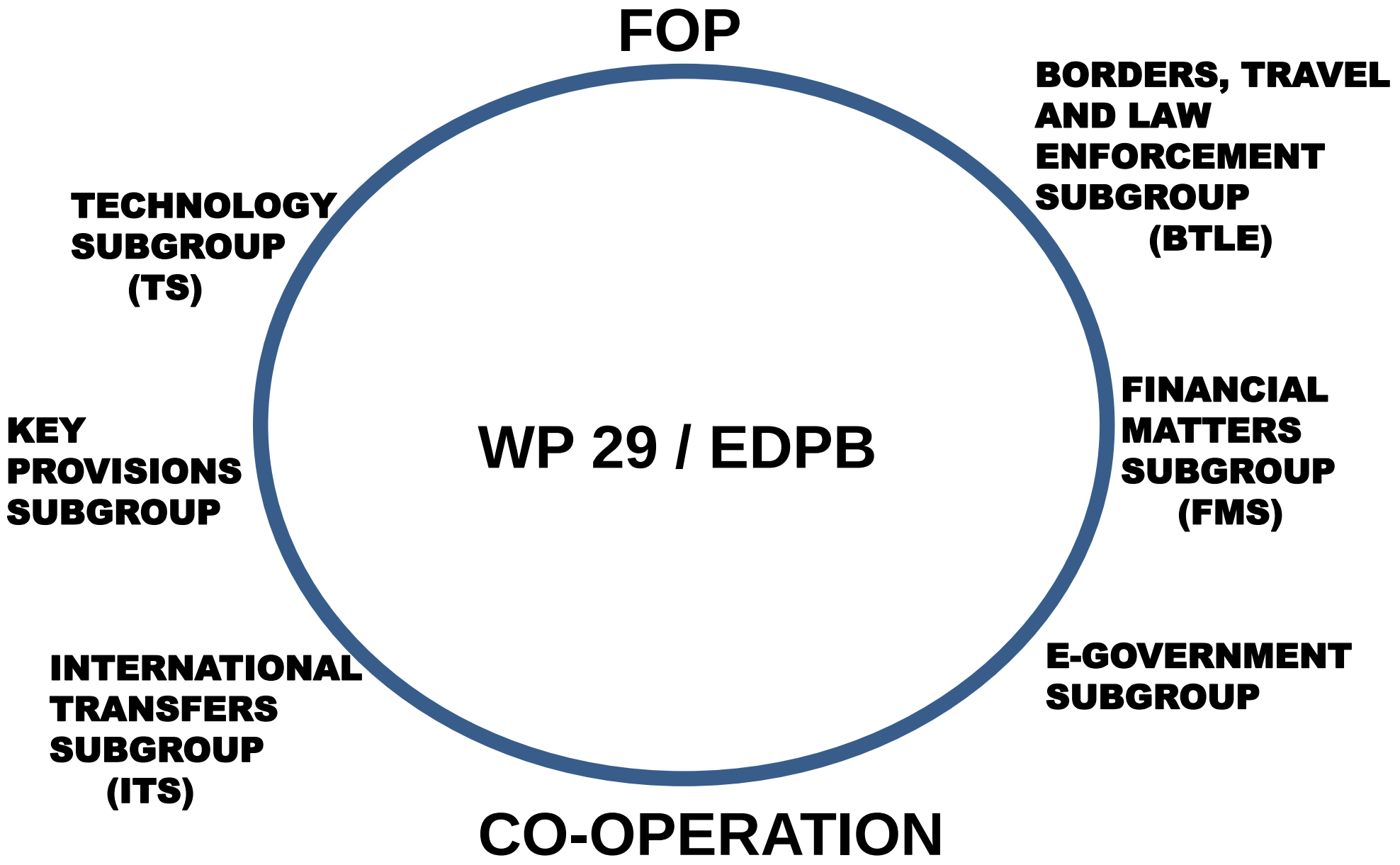
LIIKENNE- JA VIESTINTÄMINISTERIÖ

Tietosuojaforum
28.2.2018

Tietosuojavaltuutetun ajankohtaiskatsaus

Reijo Aarnio
tietosuojavaltuutettu

Tietosuojavaltuutetun toimisto


FOP
BORDERS, TRAVEL AND LAW ENFORCEMENT SUBGROUP (BTLE)
TECHNOLOGY SUBGROUP (TS)
KEY PROVISIONS SUBGROUP
WP 29 / EDPB
FINANCIAL MATTERS SUBGROUP (FMS)
INTERNATIONAL TRANSFERS SUBGROUP (ITS)
E-GOVERNMENT SUBGROUP
CO-OPERATION

BTLE: 1) **TIETOSUOJADIREKTIIVI (2016/680)**

TS: 2) **FAQ TIETOJEN SIIRRETTÄVYYDESTÄ (DATA PORTABILITY)**

3) **SALAUS (ENCRYPTION)**

4) **SERTIFIKAATIT**

KEY PROVISIONS: 5) **GDPR:N ALUEELLINEN SOVELTAMISALA**

6) **ARTIKLA 30 (5) TULKINTA**

FMS: 7) **PSD2**

MIKSI WP 29:N LISTALLA?

► havainto, että implementoitu eri tavoin MS:ssa

MITÄ OTTAA HUOMIOON?

► luku 4 TIETOSUOJA PSU (Payment Service User)

► Resital 89 refers to Directive 95/46/EU

Maksupalveluntarjoajien suorittama maksupalvelujen tarjoaminen voi sisältää henkilötietojen käsittelyä. Tämän direktiivin mukaisessa henkilötietojen käsittelyssä olisi noudatettava Euroopan parlamentin ja neuvoston direktiiviä 95/46/EY (22) sekä direktiivin 95/46/EY ja Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 45/2001 (23) saattamiseksi osaksi kansallista lainsäädäntöä annettuja kansallisia sääntöjä. Kun henkilötietoja käsitellään tämän direktiivin soveltamiseksi, olisi erityisesti mainittava täsmällinen tarkoitus, viitattava asiaankuuluvaan oikeusperustaan ja noudatettava asiaankuuluvia direktiivissä 95/46/EY säädettyjä turvallisuusvaatimuksia, sekä kunnioitettava tarpeellisuuden, oikeasuhteisuuden, käyttötarkoituksen rajoittamisen ja tietojen säilyttämisen oikeasuhteisen enimmäisajan periaatteita. Kaikkiin tämän direktiivin puitteissa kehitettäviin ja sovellettaviin tietojenkäsittelyjärjestelmiin olisi myös sisällyttävä sisäänrakennettu tietosuoja tai oletusarvoinen tietosuoja.

EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI (EU) 2015/2366, annettu 25 päivänä marraskuuta 2015, maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/110/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta

94 artikla

Tietosuoja

1. **Jäsenvaltioiden on sallittava, että maksujärjestelmät ja maksupalveluntarjoajat käsittelevät henkilötietoja, kun se on välttämätöntä maksupetoksiin liittyvien rikosten torjunnan, tutkinnan ja selvittämisen turvaamiseksi. Henkilötietojen käsittelyä koskevien tietojen antamisessa yksityishenkilöille ja tällaisten henkilötietojen käsittelyssä ja muussa tätä direktiiviä sovellettaessa toteutettavassa henkilötietojen käsittelyssä on noudatettava direktiiviä 95/46/EY, direktiivin 95/46/EY saattamista osaksi kansallista lainsäädäntöä koskevia kansallisia sääntöjä ja asetusta (EY) N:o 45/2001.**

2. **Maksupalveluntarjoajat voivat vain maksupalvelunkäyttäjän nimenomaisella hyväksynnällä saada, käsitellä ja säilyttää sellaisia henkilötietoja, jotka ovat tarpeen niiden maksupalvelujen tarjoamiseksi.**

”explicit consent”

TIETOTURVASTA

EBA → kehittää ja tarkastelee ”regulatory technical standards” (RTS)

Esim. ”strong authentication” (SCA)

Res 94 → art. 97

(94): Tunnistamista ja yhteydenpitoa koskevia teknisiä sääntelystandardeja laatiessaan pankkiviranomaisen olisi järjestelmällisesti arvioitava yksityisyysnäkökohta ja otettava se huomioon määrittääkseen kuhunkin saatavilla olevaan tekniseen vaihtoehtoon liittyvät riskit sekä korjaavat toimenpiteet, jotka voitaisiin toteuttaa tietosuojaan kohdistuvien uhkien minimoimiseksi.

KUKA VALVOO 4. LUKUA

- DPA
- FIVA
- YHDESSÄ

Jos tämä olisi epäselvä, seuraisi;

► **OSS ylikansallisissa caseissa?**
► **harmonisointi vaarantuu**

► **HUOM! WP29 EI OLE KUULTU RTS:STÄ ENNEN KUIN KOMISSIO SEN JULISTI SITOVAKSI**

→ **MANDAATTI FMS:lle**

WP 29 6.-7.2.2018

(FMS)
Financial Matters Subgroup 17.1.2018

- **arvioi onko PSD2 GDPR:n mukainen;**

  1) suostumus (94.2 art.)
  2) Ovatko RTS SCA:sta ok
  3) Miten rekisteröidyn informointi on hoidettu suhteessa GDPR:ään
  4) ”Screenscraping” siirtymäaikana

MUUTA:

8) **SANKTIO-ALATYÖRYHMÄ**

9) **NOPEUTETUN KÄSITTELYN TESTAUS**

10) **RTBF-OHJEEN PÄIVITYS**

11) **ÜBER**

EDPB:

12) **KOTISIVUT**
   * **Staattinen osa → kielet ← PROOF READING**
   * **Tiedotteet → englanniksi**

13) **IMI-JÄRJESTELMÄN KOULUTUS**
   4-5 / 2018

► ANDREA JELINEK PUHEENJOHTAJAKSI

KOMISSION KIRJE WP29: KOMISSIO OTTAA ADEKVAATTISUUS VAATIMUKSEN HUOMIOON KANSAINVÄLISESSÄ KAUPASSA

WP 29 KOKOUS 6.2.2018 /Lopullisesti hyväksytyt ohjeet/lomakkeet:

1) Henkilötietojen tietoturvaloukkauksia koskeva ohje

- WP 29 muutti kantaansa sen suhteen, milloin rekisterinpitäjä tulee tietoiseksi (having become aware of it) henkilötietojen käsittelijälle tapahtuneesta henkilötietojen tietoturvaloukkauksesta. Rekisterinpitäjä tulee uuden kannan mukaan tietoiseksi silloin, kun henkilötietojen käsittelijä ilmoittaa loukkauksesta rekisterinpitäjälle. Henkilötietojen käsittelijän on tehtävä ilmoitus ilman aiheetonta viivytystä saatuaan sen tietoonsa.
- Silloin, kun on kyse henkilötietoihin kohdistuneesta saatavuusloukkauksesta, todettiin, että tämä voi olla 33 artiklan mukaisesti ilmoitettava henkilötietojen tietoturvaloukkaus riippuen olosuhteista ja aiheutuvista riskeistä (tämä vastaa aiempaa kantaa, sitä terävöitettiin saadun palautteen perusteella).

2) Profilointia ja automatisoituja yksittäispäätöksiä koskeva ohje

- Hyväksyttiin tietyin stilistisin muutoksin.

3) Kansainvälisiä tietojen siirtoja koskevat asiat: Tietosuojan tason riittävyyttä, BCR rekisterinpitäjä ja BCR henkilötietojen käsittelijä koskevien ohjeiden päivitys ilman muutoksia.

4) Akkreditointiohje ja tämän lisäksi lähetetään ISOlle kirje, jossa pyydetään saattamaan ISO 17065 standardi kaikkien saataville.
Akkreditointia koskeva liite hyväksytään myöhemmin.

5) Sisäinen ohje/malli henkilötietojen tietoturvaloukkauksista ilmoittamisesta valvontaviranomaisten välillä.

WP 29 KOKOUS 6.2.2018

Lausuntokierrokselle lähteneet ohjeet

1) Deregation for transfers (erityistilanteita koskevat poikkeukset 49 artikla)

Valmistelussa olevat ohjeet/lomakkeet

1) Käytännesäännöt
2) Johtavan valvontaviranomaisen määrittämistä koskeva lomake
3) Puhtaasti kansalliset asiat eli 56.2 artiklan tulkintaa koskeva ohje
4) BCR approval procedure
5) Euroopan tietosuojaneuvoston kiistanratkaisumenettelyä koskeva ohje (65 artikla)
6) 3 artiklan alueellista soveltamisalaa koskeva ohje
7) 30 artiklan 5 kohdan tulkintaa koskeva ohje (poikkeukset velvollisuuteen laatia seloste käsittely toimista) tullaan hyväksymään kirjallisessa menettelyssä

Tietosuoja-asetuksen vaikutukset kansalliseen lainsäädäntöön: OM:n työryhmä

Työryhmän tehtävänä on

1) selvittää Euroopan unionin yleisen tietosuoja-asetuksen edellyttämien kansallisten lainsäädäntötoimenpiteiden tarve sekä erityisesti se, onko voimassa olevan henkilötietolain kaltaiselle yleiselle kansalliselle tietosuojalainsäädännölle tarvetta ja valmistella ehdotus asiasta mahdollisesti tarvittavaksi yleiseksi lainsäädännöksi;
2) selvittää, onko kansallista tietosuojaviranomaista koskevaa kansallista lainsäädäntöä tarpeen tarkistaa ja valmistella ehdotus tarvittavaksi lainsäädännöksi kansallisesta tietosuojaviranomaisesta, sen organisaatiosta, tehtävistä ja toimivaltuuksista;
3) selvittää tietosuoja-asetuksen jäsenvaltion lainsäädännölle jättämän kansallisen liikkumavaran antamat mahdollisuudet sekä esittää periaatteet liikkumavaran tarkoituksenmukaisesta käytöstä;
4) koordinoida ja avustaa henkilötietojen käsittelystä annetun erityislainsäädännön tarkistamiseksi tehtävää lainvalmistelutyötä.

TIETOSUOJALAKI

HE ANNETAAN VKOLLA 9

TATTI II ANNETAAN VKOLLA 9

ASETUS JA DIREKTIIVI

* Tarkistuspisteissä:
- Tilanne
- Päivitystarve
- Toteutumat
- Riskianalyysi
- kirjanpito, arvioidut kulut
- sisäinen tiedotus / hlöstö
- Miten asetuksen vaikutukset on huomioitu kansallisesti ja EU-tasolla

ALOI-TUS 18.11. 2015

Projektille annettiin nimi "TSAU"

Projekti-suunni-telman hyväk-syntä

- Esittely
- Nimitykset
- Tehtäväjako

Riskianalyysi ****

Sisäinen tiedotus

A. Osaamisen hallinta
- A.1.a Sisäinen
- A.1.b - Henkilöstösuunnitelma 2016-2019 - Koulutussuunnitelma 2016-2019 - Help desk -toiminta
- A.1.c Asianhallinta-järjestelmän laatu
- A.1.d Toteutus ja raportointi
- A.1.e Tarkistus-piste
- A.2.a Ulkoinen
- A.2.b Yhteistyö-kumppanin valinta
- A.2.c - Kotisivut - SOME - Koulutus
- A.2.d Tietosuoja-vastaavat
- A.2.e Tarkistus-piste

B. Organisaatio
- B.1.a Resurssit
- B.1.b Tarkistus-piste
- B.1.c Organisaatio-suunnitelma
- B.1.d - Toimen-kuvat - Palkat
- B.1.e - Nimitykset
- B.1.f Tarkistus-piste

C. Vaikuttavuus
- C.1.a Projekti-suunnitelma
- C.1.b Tarkistus-piste

Pohjoismainen kokous,Islanti

* Maalis 2016 Tarkistus-piste 1
* Touko 2016 Tarkistus-piste 2 (kans.väl.)
* Syys 2016 Tarkistus-piste 3
* Joulu 2016 Tarkistus-piste 4
* Kesä 2017 Tarkistus-piste 5

SEURANTA

PÄÄT TYY 2018

D. Uudet prosessit
- D.1.a Lain-säädäntö-kehikko
- D.1.a.a Nykyprosessien päivitystarve **
- D.1.a.b Työmetodit (8 uutta prosessia ***)
- D.1.b.1 Testaus
- D.1.b.2 Käyttöön-otto
- D.1.b.3 Tarkistus-piste

E. Muut projektit
- E.1.a Oikeusministeriö - toimikunta
- E.1.b Alatyöryhmät
- E.1.c Tarkistus-piste

F. Kansain-välinen yhteistyö
- F.1.a. Euroopan tietosuojaneuvosto
- F.1.b Tarkistuspiste
- F.2.a. Substanssiasiat
- F.2.b. WP 29 ohjeistus
- F.2.c Tarkistuspiste
- F.3.a. Hallinnolliset asiat
- F.3.b. WP 29 ohjeistus
- F.3.c Tarkistuspiste

G. IT-alusta
- G.1.a. Kansainväliset valitusasiat
- G.1.b. Yhteiset operaatiot
- G.1.c. Yhdenmukaisuusmekanismi
- G.1.d Tarkistus-piste
- G.2.a. Kansalliset konvertiot
- G.2.b. - Vaikuttavuus - Osaamisen hallinta - Laadun tarkkailu
- G.2.c Tarkistus-piste

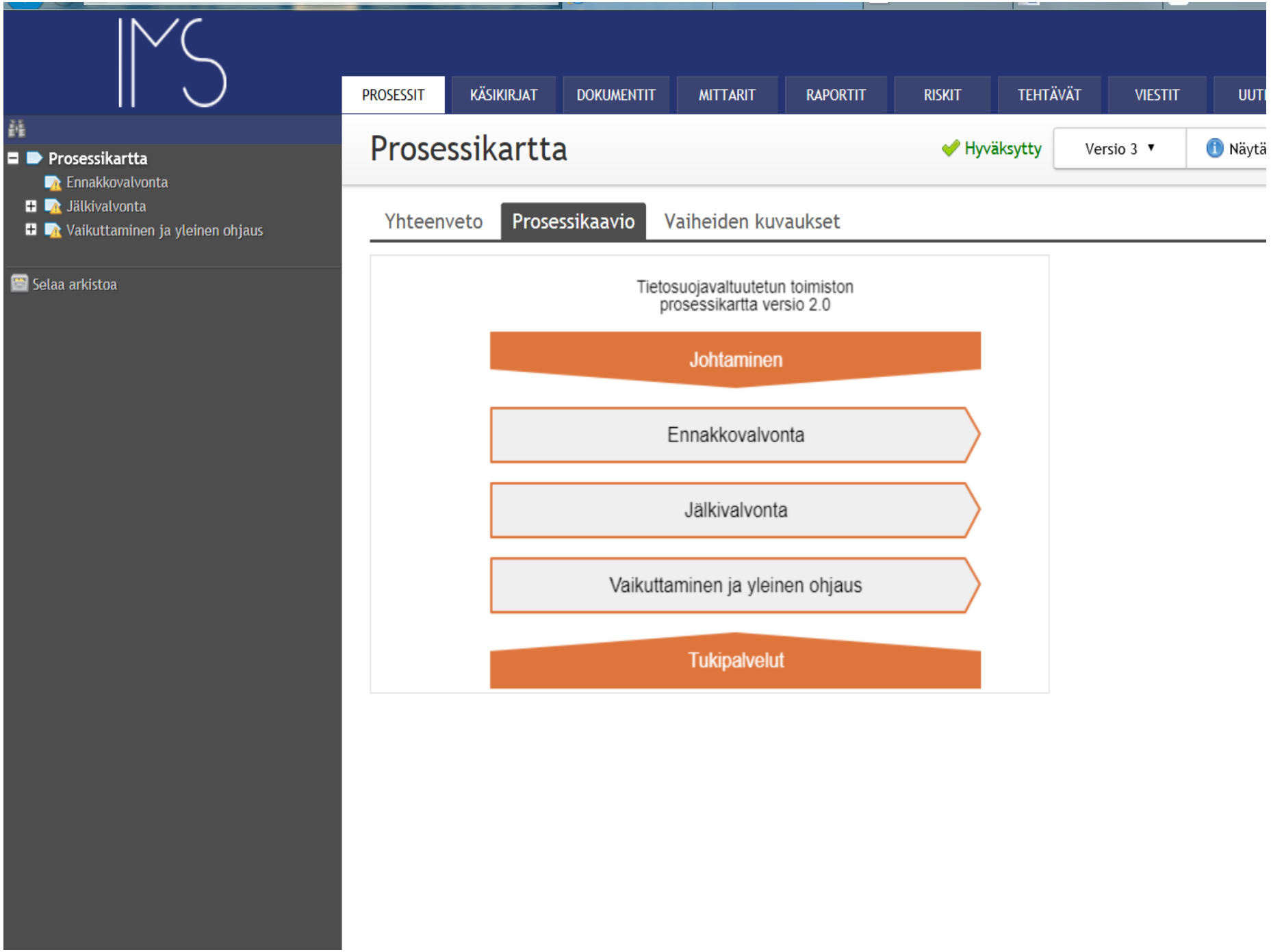
H. Yleis-tarkistus piste

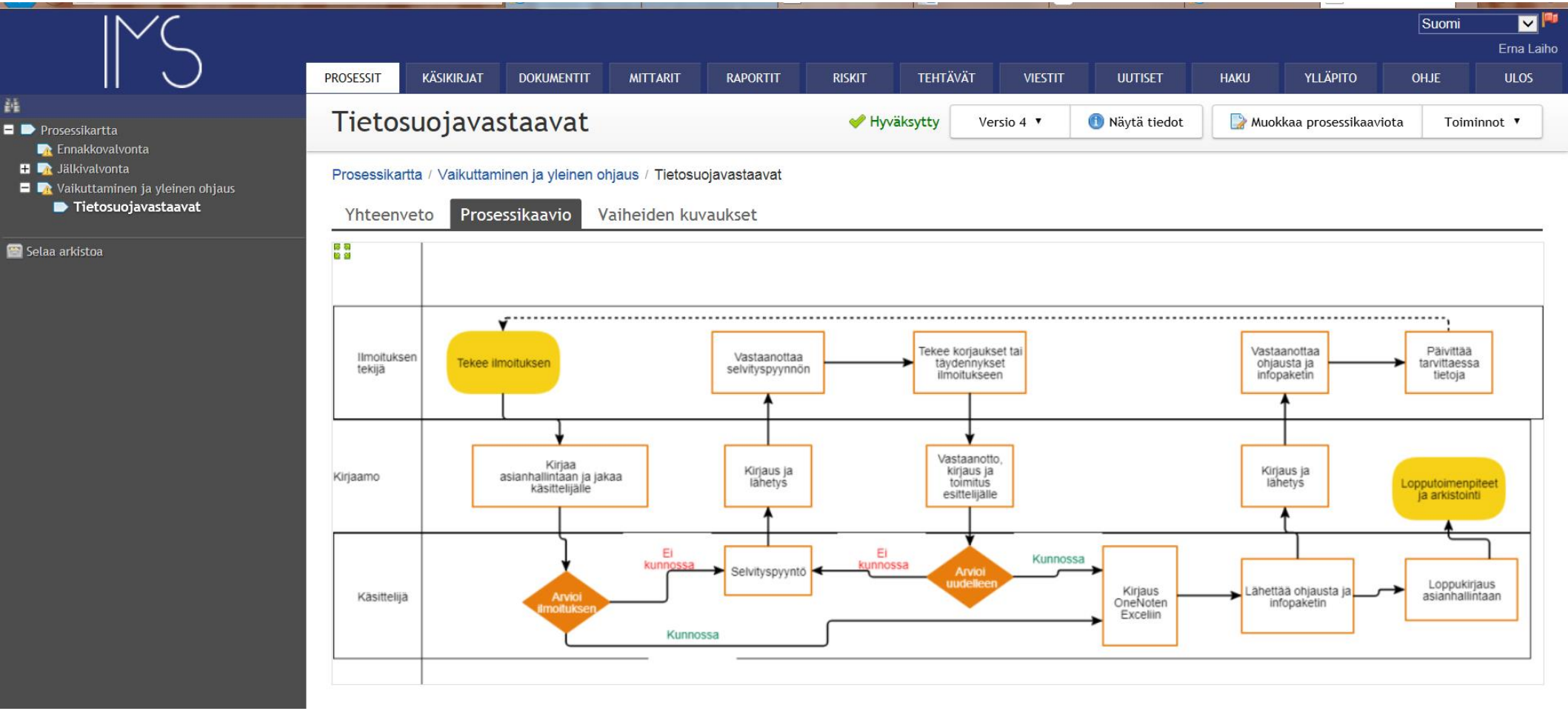
I. SAUNA-ILTA

J. KÄYTTÖÖN-OTTO

** NYKYISET PERUSPROSESSIT:
1) Asiamies/valtuutettu
2) Tarkastaja
3) Konsultti
4) Valistaja
5) Poliittinen neuvonantaja
6) Neuvottelija
7) Täytäntöön panija
8) Kansainvälinen lähettiläs.

*** UUDET PROSESSIT:
1. Yhdenmukaisuusmekanismi
2. Hallinnolliset sanktiot
3. Ennakkohyväksymistehtävät (Auditointi)
4. Ulkomaille siirrot
5. Data Breach Notifications – ilmoitusprosessi
6. Tarkastukset
7. Sähköinen asiointialusta
8. Kansallinen lainsäädäntö


IMS
PROSESSIT
KÄSIKIRJAT
DOKUMENTIT
MITTARIT
RAPORTIT
RISKIT
TEHTÄVÄT
VIESTIT
Prosessikartta
Ennakkovalvonta
Jälkivalvonta
Vaikuttaminen ja yleinen ohjaus
Selaa arkistoa
Prosessikartta
Hyväksytty
Versio 3
Näytä
Yhteenveto
Prosessikaavio
Vaiheiden kuvaukset
Tietosuojavaltuutetun toimiston
prosessikartta versio 2.0
Johtaminen
Ennakkovalvonta
Jälkivalvonta
Vaikuttaminen ja yleinen ohjaus
Tukipalvelut


IMS
Suomi
Erna Laiho
PROSESSIT
KÄSIKIRJAT
DOKUMENTIT
MITTARIT
RAPORTIT
RISKIT
TEHTÄVÄT
VIESTIT
UUTISET
HAKU
YLLÄPITO
OHJE
ULOS
Prosessikartta
Ennakkovalvonta
Jälkivalvonta
Vaikuttaminen ja yleinen ohjaus
Tietosuojavastaavat
Selaa arkistoa
Tietosuojavastaavat
Hyväksytty
Versio 4
Näytä tiedot
Muokkaa prosessikaaviota
Toiminnot
Prosessikartta / Vaikuttaminen ja yleinen ohjaus / Tietosuojavastaavat
Yhteenveto
Prosessikaavio
Vaiheiden kuvaukset
Ilmoituksen tekijä
Kirjaamo
Käsittelijä
Tekee ilmoituksen
Kirjaa asianhallintaan ja jakaa käsittelijälle
Arvioi ilmoituksen
Ei kunnossa
Selvityspyyntö
Kirjaus ja lähetys
Vastaanottaa selvityspyynnön
Ei kunnossa
Arvioi uudelleen
Vastaanotto, kirjaus ja toimitus esittelijälle
Tekee korjaukset tai täydennykset ilmoitukseen
Kunnossa
Kirjaus OneNoten Exceliin
Kunnossa
Kirjaus ja lähetys
Vastaanottaa ohjausta ja infopaketin
Lähettää ohjausta ja infopaketin
Päivittää tarvittaessa tietoja
Lopputoimenpiteet ja arkistointi
Loppukirjaus asianhallintaan

Tietosuojavaltuutetun toimisto

Sivukartta

Hae

Etusivu | Ajankohtaista | Päätökset | Materiaalia | Rekisteröidylle | Rekisterinpitäjälle | Tietosuojavaltuutetun toimisto | Yhteystiedot

Oikopolut

- Usein kysyttyä
- Oppaat
- Lomakkeet
- Näin kysyt neuvoa
- Mitä tehtäviimme ei kuulu
- EU:n tietosuojauudistus
- Sanastoa
- Tietosuojavaltuutetun ratkaisuja
- Kansainvälinen yhteistyö
- Lait

EU:n tietosuojauudistus

Uudistamme verkkosivujamme

Huomioithan, että nykyisten verkkosivujemme sisältö perustuu pääosin henkilötietolakiin (523/1999). Toukokuun 25. päivästä alkaen henkilötietojen käsittelyyn sovelletaan EU:n yleistä tietosuoja-asetusta. Kokoamme asetukseen liittyvää tietoa osioon EU:n tietosuojauudistus.

Uudistunut sivustomme julkaistaan toukokuussa 2018.

Tiedotteet ja uutiset

Ilmoitusvelvollisuus tietosuojavaltuutetun toimistolle muuttuu 25. toukokuuta

20.02.2018 Tietosuojavaltuutetun toimistolle on lähetetty paljon tarpeettomia ilmoituksia henkilötietojen käsittelystä. Jos henkilötietojen käsittely perustuu esimerkiksi suostumukseen, asiakkuuteen tai jäsenyyteen, käsittelystä ei tarvitse ilmoittaa tietosuojavaltuutetulle. Tietosuojavaltuutetun toimisto ei vastaa tarpeettomiin ilmoituksiin. Rekisterinpitäjän ilmoitusvelvollisuus muuttuu 25. toukokuuta 2018, kun EU:n yleistä tietosuoja-asetusta ryhdytään soveltamaan.

Puhelinneuvonta

ma–to klo 9–11 ja 13–15

pe klo 9–11

puh. 029 56 16670

Tietosuoja-asetusta koskevat kysymykset

Näin kysyt neuvoa

Luentopyynnöt

Yhteystiedot

Käyntiosoite:

Ratapihantie 9, 6. krs

00520 Helsinki

Postiosoite:

PL 800

Tietosuojavaltuutetun toimisto

Sivukartta

Etusivu | Ajankohtaista | Päätökset | Materiaalia | Rekisteröidylle | Rekisterinpitäjälle | Tietosuojavaltuutetun toimisto

Ajankohtaista

- Uutiset
  - 2018
  - 2017
  - 2016
  - 2015
  - 2014
  - 2013
  - 2012
  - 2011
- Avoimet työpaikat
- Blogi

Etusivu » Ajankohtaista » Uutiset » 2018 » Tietosuojavaltuutetun toimisto uudistaa verkkosivustoaan – ilmoittaudu asiakastyöpajaan ja vaikuta tuleviin verkkopalveluihin

Tietosuojavaltuutetun toimisto uudistaa verkkosivustoaan – ilmoittaudu asiakastyöpajaan ja vaikuta tuleviin verkkopalveluihin

Julkaistu 31.1.2018 Päivitetty 7.2.2018

Tietosuojavaltuutetun toimisto on uudistamassa verkkosivustoaan toukokuussa 2018. Jotta tuleva sivusto palvelisi asiakkaitamme nykyistä paremmin, toivomme kuulevamme asiakkaittemme näkemyksiä.

Kuulemista varten järjestämme asiakastyöpajan 7.2.2018 klo 9–11 Pasilassa, Helsingissä.

Työpajaan mahtuu noin 8 henkilöä. Jos kiinnostuneita on enemmän, valitsemme työpajan osallistujat eri asiakasryhmistä. Ilmoittautuminen päättyy tiistaina 6.2.2018 klo 15. Olemme yhteydessä ilmoittautuneihin sähköpostitse ja kerromme lisätietoja työpajasta.

Työpajan ohjaa palvelumuotoilija **Laura Järveläinen** D9-digitiimistä.

Olitpa sitten kansalainen, henkilötietojen käsittelijä tai tietosuojavastaava, olet tervetullut työpajaan! Toivomme saavamme näkemyksiä eri asiakasryhmistä ja aloilta.

Tarjoamme osallistujille kahvia ja pientä suolaista.

Käsitellessämme henkilötietoja noudatamme tietosuojavaltuutetun toimiston tietosuojaperiaatteita (sidosryhmärekisterin tietosuojaseloste).

Valvontaviranomaisen toimivaltuudet 58 art.

TUTKINTAVALTUUDET
Määrätä rekisterinpitäjä ja henkilötietojen käsittelijä antamaan kaikki **tehtävien suorittamiseksi tarvittavat tiedot**
Tarkastukset
Sertifiointien uudelleen tarkastelu
Ilmoitus asetuksen **väitetystä rikkomisesta**
Oikeus saada pääsy kaikkiin henkilötietoihin, jotka ovat tarpeen tehtävien suorittamiseksi
Oikeus saada pääsy rekisterinpitäjän ja henkilötietojen käsittelijän **tiloihin** kansallisen lain mukaisesti

Valvontaviranomaisen toimivaltuudet 58 art.

KORJAAVAT TOIMIVALTUUDET
Varoittaa – käsittely todennäköisesti asetuksen vastaista (ennen kuin käsittely on alkanut)
Huomauttaa – käsittely toimet ovat olleet asetuksen vastaisia (kun käsittely on jo alkanut)
Määrätä – noudattamaan rekisteröityjen pyyntöjä, jotka koskevat asetukseen perustuvien rekisteröidyn oikeuksien käyttöä
Määrätä – saattamaan käsittelytoimet asetuksen mukaisiksi, tarvittaessa tietyllä tavalla ja tietyn määräajan kuluessa
Määrätä rekisterinpitäjää ilmoittamaan henkilötietojen tietoturvaloukkauksesta rekisteröidylle
Asettaa pysyvä tai väliaikainen rajoitus käsittelylle, mukaan lukien käsittelykielto

Valvontaviranomaisen toimivaltuudet 58 art.

KORJAAVAT TOIMIVALTUUDET
Antaa määräyksiä koskien 16,17,18 ja 19 artikloiden mukaisten oikeuksien toteuttamista sekä määräyksiä näistä toimenpiteistä ilmoittamisesta 17.2 ja 19 artikloiden mukaisesti
Peruuttaa tai määrätä sertifiointielin peruuttamaan sertifiointi tai kieltää sertifiointielintä myöntämästä sertifiointia
Määrätä hallinnollisen sakon muiden toimenpiteiden lisäksi tai niiden sijaan
Määrätä tiedon siirron keskeyttämisestä kolmanteen maahaan

Korjaavien toimivaltuuksien käyttämistä koskevat periaatteet

1. Tietosuoja-asetuksen rikkomisen tulisi johtaa saman tasoisiin seuraamukseen jokaisessa jäsenvaltiossa (johdanto-osan kappale 11)

- Luonnollisten henkilöiden oikeuksien ja vapauksien suojelun tason näiden tietojen käsittelyssä olisi oltava vastaava kaikissa jäsenvaltioissa (johdanto-osan kappale 10)
- Jotta voidaan estää eroavuudet, jotka haittaavat henkilötietojen vapaata liikkuvuutta sisämarkkinoilla (johdanto-osan kappale 13)
- Valvontaviranomaisten tehtävänä on varmistaa asetuksen johdonmukainen soveltaminen ja täytäntöönpano (57.1 art. g alakohta)
- Valvontaviranomaisilla saman tasoiset valtuudet valvoa asetuksen säännösten noudattamista (johdanto-osan kappale 11)
- Rajat ylittävissä tilanteissa yhdenmukaisuus saavutetaan yhdenmukaisuusmekanismin kautta
- Ei- rajat ylittävissä tilanteissa EDPB suuntaviivat ja ohjeet

Korjaavien toimivaltuuksien käyttämistä koskevat periaatteet

2. Korjaavien toimivaltuuksien käytön on oltava yksittäisessä tapauksessa tehokasta, oikeasuhtaista ja varoittavaa

- Toimivaltuuden on oltava oikeassa suhteessa rikkomisen luonteeseen, vakavuuteen ja muihin seurauksiin
- Yksittäisiä tapauksia on arvioitava kokonaisvaltaisesti ja objektiivisesti
- Arvioinnissa huomioitava, onko tarkoituksena määrätä rangaistusluonteinen seuraamus vai saattaa asetuksen vastainen henkilötietojen käsittely asetuksen mukaiseksi (voi olla molemmat)
- Luonnollisesti valvontaviranomaisten tekemät tulkinnat ja oikeuskäytäntö tulevat tulevaisuudessa määrittämään näitä reunaehtoja tarkemmin

Korjaavien toimivaltuuksien käyttämistä koskevat periaatteet

3. Toimivaltainen valvontaviranomainen tekee arvion ”yksittäistapauksessa”

- Erityisesti hallinnollisen sakon määräämistä koskeva 83.2 art.: ”hallinnolliset sakot määrätään kunkin yksittäisen tapauksen olosuhteiden mukaisesti 58 art. 2 kohdan a-h ja j alakohdassa tarkoitettujen toimenpiteiden lisäksi tai niiden sijaan”
- Valvontaviranomaisen vastuulla on päättää, mikä on tarkoituksenmukaisin toimenpide (harkinta kaikkien korjaavien toimivaltuuksien väliltä)

Korjaavien toimivaltuuksien käyttämistä koskevat periaatteet

4. Harmonisoidun lähestymistavan omaksuminen edellyttää valvontaviranomaisten välistä aktiivista yhteistyötä

- Tietosuoja-asetuksen yhteistyömekanismit VII luku
- Proaktiivinen tietojen vaihto

Hallinnollisten sakkojen määräämisen yleiset edellytykset (art. 83)

- Sakkojen määräämisen tulee olla kussakin yksittäistapauksessa **tehokasta, oikeasuhteista ja varoittavaa**
- Voidaan määrätä muiden korjaavien toimivaltuuksien **lisäksi tai sijaan**
- Sakon enimmäismäärä riippuu rikkomuksesta (1. enint. 10 milj.€ tai 2 % vuotuinen maailmanlaajuisesta liikev. 2. enint. 20 milj.€ tai 4 % maailmanlaajuisesta liikev.)
- Kansallinen liikkumavara sen suhteen, voidaanko viranomaisille määrätä hallinnollista sakkoa
- Valvontaviranomaisen valtuuksien käyttöön sovelletaan asianmukaisia menettelytakeita
- Tietosuoja-asetuksen 84 artikla edellyttää oikeasuhtaisia, varoittavia ja tehokkaita seuraamuksia (erityisesti, kun 83 art. ei sovelleta)

Päätettäessä hallinnollisen sakon määräämisestä ja sen määrästä, kussakin yksittäistapauksessa on otettava huomioon 11 kriteeriä
a) Rikkomisen **luonne, vakavuus ja kesto**, kyseisen tietojen käsittelyn **luonne, laajuus ja tarkoitus huomioon ottaen** sekä niiden rekisteröityjen **lukumäärä**, joihin rikkominen vaikuttaa ja heille aiheutuneen **vahingon suuruus**
b) Rikkomisen **tahallisuus tai tuottamuksellisuus**
c) Toimet rekisteröidylle aiheutuneen **haitan lieventämiseksi**
d) **Vastuun aste**, ottaen huomioon 25 ja 32 artiklan nojalla **toteutetut tekniset ja organisatoriset toimenpiteet**
e) Aiemmat **vastaavat rikkomiset**
f) **Yhteistyö valvontaviranomaisen kanssa** rikkomisen korjaamiseksi ja haittavaikutusten lieventämiseksi
g) **Henkilötietoryhmät,** johon rikkominen vaikuttaa

Päätettäessä hallinnollisen sakon määräämisestä ja sen määrästä, kussakin yksittäistapauksessa on otettava huomioon 11 kriteeriä

h) Tapa, jolla rikkominen **tuli valvontaviranomaisen tietoon**. Ilmoittiko rekisterinpitäjä ja käsittelijä ja missä laajuudessa?

i) Onko **määrätty aiemmin** muita 58.2 artiklassa tarkoitettuja toimenpiteitä? Onko määräyksiä noudatettu?

j) Käytännesääntöjen ja sertifikaattien **noudattaminen**

k) Mahdolliset **muut** tapaukseen sovellettavat **raskauttavat tai lieventävät tekijät,** kuten rikkomisesta suoraan tai välillisesti saadut mahdolliset taloudelliset edut tai rikkomisella vältetyt tappiot

Hallinnollisten sakkojen määrääminen kansallisessa prosessissa (ehdotus)

- Laajennetaan koskemaan 10 artiklaa
- Koskee myös käsittelykiellon asettamista
- Tietosuojavaltuutettu esittelee asian seuraamuslautakunnalle
- Seuraamuslautakunta on päätösvaltainen pj/vpj + 2 jäsentä/varajäsent. Päätökseksi tulee esitys, jota enemmistö on kannattanut
- Hallinnollisen sakon täytäntöönpanoon sovelletaan sakon täytäntöönpanosta annettua lakia
- Muutoksenhaku hallinto-oikeuteen

Valvontaviranomaisen toimivaltuudet 58 art.

Hyväksymis- ja neuvontavaltuudet
Antaa rekisterinpitäjälle **neuvoja** 36 artiklan mukaisesti
Antaa omasta aloitteesta tai pyynnöstä **lausuntoja** eduskunnalle, valtioneuvostolle tai **jäsenvaltionlain säädännön mukaisesti** muille toimielimille tai elimme sekä yleisölle **kaikista henkilötietojen suojaa koskevista kysymyksistä**
Hyväksyä 36.5 art. tarkoitettu käsittely, jos kansallinen lainsäädäntö edellyttää ennakkohyväksyntää
Antaa lausuntoja käytännesääntöluonnoksista ja **hyväksyy** ne 40.5 art. mukaisesti
Akkreditoi sertifiointielimet 43 art. Mukaisesti
Myöntää sertifiointeja ja hyväksyy sertifiointikriteerejä 42.5 art. mukaisesti

Valvontaviranomaisen toimivaltuudet 58 art.

Hyväksymis- ja neuvontavaltuudet
Hyväksyy 28.8 art. (henkilötietojen käsittelijä) ja 46.2 art. d alakohdassa (henkilötietojen siirto asianmukaisia suojatoimia soveltaen kolmanteen maahan) tarkoitetut tietosuojaa koskevat vakiolausekkeet
Hyväksyy 46.3 art. a alakohdassa tarkoitetut sopimuslausekkeet (henkilötietojen siirto asianmukaisia suojatoimia soveltaen kolmanteen maahan)
Hyväksyy 46.3 art. b alakohdassa tarkoitettuja hallinnollisia järjestelyitä (henkilötietojen siirto asianmukaisia suojatoimia soveltaen kolmanteen maahan)
Hyväksyy yritystä koskevat sitovat säännöt 47 art. mukaisesti (BCR Binding Corporate Rules) **Huom!** 63 artiklassa tarkoitetun yhdenmukaisuusmekanismin mukaisesti

Euroopan tietosuojaneuvosto (68 art.)

WP29 -> EDPB

toimielin, oikeushenkilö
Unionin toimielin, oikeushenkilö

Varmistaa, että asetusta sovelletaan yhdenmukaisesti

- Toimii oma-aloitteisesti tai komission pyynnöstä
- Seuraa. Antaa lausuntoja, suosituksia ja suuntaviivoja

Monissa suhteissa kansallisia viranomaisia ylempi taho

- Esim. kiistanratkaisumenettely: antaa oikeudellisesti sitovia päätöksiä asioihin, joista kansallisilla viranomaisilla on eriävät näkemykset

Yhden luukun periaate (One Stop Shop)

- **Periaate:** rekisterinpitäjät ja henkilötietojen käsittelijät, joilla on liiketoimintaa useammassa EU-maassa, voivat asioida vain yhden tietosuojaviranomaisen kanssa

- Johtava valvontaviranomainen on viranomainen, jolla on ensisijainen vastuu **rajatylittävän käsittelytoiminnan** osalta

- Johtava valvontaviranomainen **koordinoi toimia**, joihin muut valvontaviranomaiset (osallistuvat valvontaviranomaiset) osallistuvat asetuksen 60-62 art. (yhdenluukunmekanismi, keskinäinen avunanto ja yhteiset operaatiot) mukaisesti

- Johtava valvontaviranomainen **toimittaa päätösehdotuksen** niille valvontaviranomaisille, joilla on intressejä asiassa

Yhden luukun periaate (One Stop Shop)

- Rajatylittävä käsittely on määritelty asetuksen 4 artiklan 23 kohdassa:
  - henkilötietojen käsittelyä, joka suoritetaan unionissa rekisterinpitäjän tai henkilötietojen käsittelijän **useammassa kuin yhdessä jäsenvaltiossa sijaitsevassa toimipaikassa toteutettavan toiminnan yhteydessä**, ja rekisterinpitäjä tai henkilötietojen käsittelijä on **sijoittautunut** useampaan kuin yhteen jäsenvaltioon; tai

  - henkilötietojen käsittelyä, joka suoritetaan unionissa rekisterinpitäjän tai henkilötietojen käsittelijän **ainoassa toimipaikassa toteutettavan toiminnan yhteydessä** mutta joka **vaikuttaa merkittävästi tai on omiaan vaikuttamaan merkittävästi useammassa kuin yhdessä jäsenvaltiossa oleviin rekisteröityihin**

Yhden luukun periaate (One Stop Shop)

- **Poikkeukset:**
  - Jos kohde liittyy ainoastaan sen jäsenvaltiossa olevaan toimipaikkaan tai vaikuttaa merkittävästi vain sen jäsenvaltiossa oleviin rekisteröityihin
  - Kun käsittelyn suorittaa viranomainen tai sen lukuun toimiva julkishallinnon elin silloin kuin käsittely perustuu art. 6 (1) c ja e kohtiin.

Miten rekisterinpitäjän johtava valvontaviranomainen määritetään?

- Sen maan valvontaviranomainen, jossa organisaation päätoimipaikka/ ainoa toimipaikka sijaitsee
  - Organisaation keskushallinnon toimipaikka
  - **PAITSI,** jos toinen toimipaikka kuitekin tekee päätökset käsittelyn tarkoituksista ja keinoista
- Johtavia valvontaviranoamisia voi olla useampi kuin yksi
  - Jos päätökset käsittelyn tarkoituksista ja keinoista tehdään eri toimipaikoissa
  - Henkilötietojen käsittelytoimintaa koskevien päätöksentekovaltuuksien keskittäminen?

Miten henkilötietojen käsittelijän johtava valvontaviranomainen määritetään?

- Henkilötietojen käsittelijän päätoimipaikka on sen keskushallinnon sijaintipaikka unionissa, ja jos sillä ei ole keskushallintoa unionissa, se henkilötietojen käsittelijän unionissa sijaitseva toimipaikka, jossa pääasiallinen käsittelytoiminta tapahtuu

- Tapauksissa, joihin liittyy sekä rekisterinpitäjä että henkilötietojen käsittelijä, toimivaltainen johtava valvontaviranomainen on rekisterinpitäjän johtava

Jos valvontaviranomaiset eivät saavuta konsensusta: Yhdenmukaisuusmekanismi

”Tiekartta”

1) tuomioistuinten ratkaisukäytännöt Privacy International vs UK

2) Verkkovalvontalaki I ja II

3) verkkovalvontalain valvonnan järjestäminen

4) Perustuslaki

5) ehdotus sähköisen viestinnän tietosuoja-asetukseksi (COM (2017) 10 final)
- ePrivacy

6) oikeusministeriön TATTI-työryhmä (yleinen tietosuoja-asetus, EU 2016/679 GDPR)

7) TATTI- työryhmän toimeksiannon (OM 1/41/2016) kohta
”normienpurkutalkoot/erityislainsäädäntö”

8) tiedonhallinnan sääntelyn kehittämistä selvittävä työryhmä
(VM/1709/00.01.00.01/2016)

”Tiekartta”

9) EU:n tietosuojadirektiivin (EU 2016/680) täytäntöönpano (OM 21/41/2016)

→ 10) mm. poliisin henkilötietolain kokonaisuudistus

11) komission ehdotus toimielinten tietosuoja-asetukseksi

12) TATTI-työryhmän toimeksiannon kohta 2, kansallinen tietosuojaviranomainen, muoto ym. MURRE-ryhmä

13) digitaalisen sisämarkkinastrategian mukaisesti annettu komission esitys (COM(2015)634) digitaalista sisältöä koskevaksi sääntelyksi

14) komission esitys (COM(2015)635) "digitaalista kauppaa koskevaksi laiksi”

15) Privacy Shield (C(2016) 4176 final

16) asetusehdotus Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelimen perustamisesta (BEREC-asetus) COM(2016) 591 Final
kts. U 68/2016 vp

KIITOS KUUNTELUSTA

Lisätietoja: www.tietosuoja.fi

Reijo Aarnio
tietosuojavaltuutettu

Näin vastaat

Jokaiseen kysymykseen on noin minuutti aikaa vastata

Pöydissä ryhmä päättää yhden vastauksen, ja nostaa lapun esiin

Muut osallistujat vastaavat äänestämällä osoitteessa: screen.io/lvm

20 kysymystä, 5 kokonaisuutta

- Soveltamisala
- Suostumus
- Informointi
- Rekisteröidyn oikeudet
- Käytännön toimet

Vastaus-vaihtoehdot

Myytti!

Myyteissä on totuuden siemen…

Näin on!

Screen.io/lvm

A. Soveltamisala

Nopea

1

Tietosuoja-asetusta ei sovelleta, jos henkilötiedoista ei muodostu henkilörekisteriä

A. Soveltamisala

Nopea

2

Yhdellä rekisterinpitäjällä on vain yksi rekisteri

A. Soveltamisala

Nopea

3

IP-osoite on henkilötieto

A. Soveltamisala

4

Kaikkea henkilötietoa ei tarvitse käsitellä samoin menettelyin

A. Soveltamisala

5

Meillä on vain yrityksiä asiakkaina – GDPR koskee silti myös meidän toimintaamme

A. Soveltamisala

Nopea

6

Pseudonymisoitu data on henkilötietoa, joten siihen sovelletaan GDPR:ää

A. Soveltamisala

7

Biometrinen data on aina arkaluonteista henkilötietoa

B. Suostumus käsittelyperusteena

Nopea

8

Henkilötietoja saa käsitellä vain suostumuksella

B. Suostumus käsittelyperusteena

9

Suostumus on pyydettävä uudestaan vanhoilta rekisteröidyltä

B. Suostumus käsittelyperusteena

10

Lasten henkilötietojen käsittelyyn tulee saada huoltajan suostumus

C. Rekisteröidyn informoiminen

Nopea

11

Rekisteriselostetta ei saa enää käyttää, koska sitä ei mainita GDPR:ssä

C. Rekisteröidyn oikeudet

12

Rekisteröidyllä on aina oikeus saada tietonsa poistetuksi

C. Rekisteröidyn oikeudet

13

Tarkastusoikeutta ei tarvitse toteuttaa, jos rekisteröity ei ole tunnistettavissa

C. Rekisteröidyn oikeudet

14

Profilointi vaatii aina rekisteröidyn suostumuksen

D. Käytännön toimet

Nopea

15

Tietosuoja tarkoittaa
käytännössä tietoturvaa

16

Tietosuojavastaava vastaa henkilötietojen käsittelyn lainmukaisuudesta

D. Käytännön toimet

Nopea

17

GDPR:n rikkominen johtaa aina huomattaviin sakkoihin

D. Käytännön toimet

18

Tilaaja on vastuussa toimittajan suorittamasta käsittelystä

19

Henkilötunnusta ei saa käyttää asiakkaan tunnistamiseen

D. Käytännön toimet

Nopea

20

Jokaisesta henkilötietojen tietoturvaloukkauksesta on ilmoitettava

Kysymyksiä?

@lvmfi
#tietosuojafoorumi

LIIKENNE- JA VIESTINTÄMINISTERIÖ

Kiitos!