Digitaalisen liiketoiminnan tietosuojafoorumi – tietosuojavastaava liiketoiminnan tukena

6.10.2017, Liikenne- ja viestintäministeriö

@lvmfi

LIIKENNE- JA VIESTINTÄMINISTERIÖ

LVM 1892–2017

Suomi Finland 100

Ohjelma

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

13.10 – Ajankohtaista tietosuoja-asetuksesta
Yleinen tietosuoja-asetus ja tietosuojavastaava
Reijo Aarnio, tietosuojavaltuutettu

13.40 – Tietosuojavastaava johdon tukena
Katri Harra-Salonen, Chief Digital Officer, Finnair

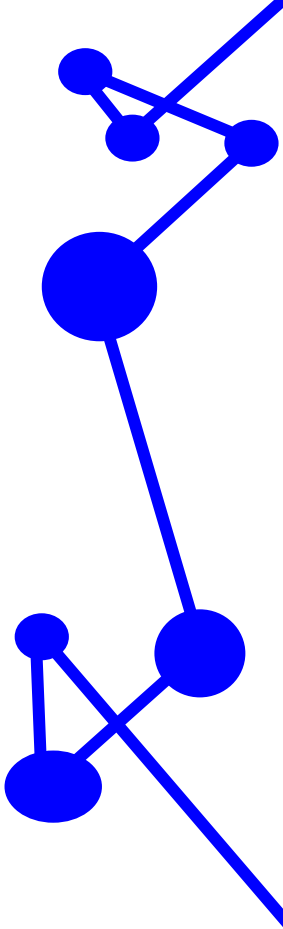
14.00 – Tietosuojatyö kansainvälisessä organisaatiossa
Minna Ääri, HR Manager, IBM

14.20 – Näkökulma käytännön työhön
Laura Tarhonen, Privacy Manager, Sanoma

14.40 – Kahvitauko

15.00 – Työpajat

15.30 – Työpajojen purku



TIETOSUOJAVALTUUTETUN PUHEENVUORO 6.10.2017

AJANKOHTAISTA TIETOSUOJASTA

Reijo Aarnio
tietosuojavaltuutettu

Tietosuojavaltuutetun toimisto

TATTI-TYÖRYHMÄ

* MIETINTÖ (I) LUOVUTETTU 21.6.2017
* LAUSUNTOKIERROS 8.9.2017 ASTI

AVOIMIA ASIOITA

- ► **LAPSEN IKÄRAJA**
- ► **HALLINNOLLISET SANKTIOT**
- ► **YHTEENSOVITTAMINEN TILKE-TYÖRYHMÄN KANSSA**

ERITYISLAINSÄÄDÄNNÖN PERKAAMINEN

DIREKTIIVITYÖRYHMÄ

- **OM ASETTANUT**

- **VALMISTELEE EHDOTUKSEN EU:N TIETOSUOJADIREKTIIVIN TÄYTÄNTÖÖNPANEMISEKSI**

- **DIREKTIIVIN SOVELTAMISALA:** Direktiivin soveltamisala ulottuu oikeus-, sisä-, puolustus- ja valtiovarainministeriön hallinnonaloille. Oikeusministeriön osalta direktiiviä sovelletaan Oikeusrekisterikeskukseen, Rikosseuraamuslaitokseen, syyttäjäviranomaisiin, yleisiin tuomioistuimiin, oikeusministeriöön sekä oikeusapu- ja ulosottoviranomaisiin.

- **MÄÄRÄAIKA 29.9.2017**
- **LAKI VOIMAAN 6.5.2018**

TIEDOTUS JA OPETUS

- **MEDIATAITOVIIKKO**
- **VIDEOT**

  www.arjentietosuoja.fi

  - Tietosuojaa meille kaikille

  - Verkkokoulutuksen on toteuttanut Julkisen hallinnon tietohallinnon neuvottelukunta (JUHTA) ja sen asettama asiantuntijaryhmä: Valtiovarainministeriö, Suomen Kuntaliitto, oikeusministeriö, tietosuojavaltuutetun toimisto, Valtori sekä Viestintävirastossa toimiva Kyberturvallisuuskeskus

- **OHJE REKISTERINPITÄJILLE**
- **KOTISIVUTIEDOTUS**
- **TIETOSUOJAVALTUUTETUN BLOGI**
- **TWITTER**

JUHTA-VAHTI-yhteishankkeen materiaalit avoimesti saatavilla

- sisältää mm. tallenteet jo pidetyistä työpajoista
- työpajojen aiheet
- seuraava pidetään pe 29.9.2017 aiheina *Rekisterinpitäjän velvollisuuksien toteuttaminen ja Riskienhallinta osa 4, tietosuojan näkökulma.*
  - ❑ suoratoistona voi seurata kuka vain

www.arjentietosuoja.fi

Koulutusvideot

Arjen tietosuojaa – tietosuojaa meille kaikille (**sisältää nettitestin**)
Kohderyhmä: organisaation kaikki työntekijät sekä kansalaiset

Johdon ja esimiesten koulutusvideo
Kohderyhmä: johto ja esimiehet

KOMISSIO

- **Commission expert group (E03461) on the Regulation (EU) 2016/679 and Directive (EU) 2016/680**

- **ASIANTUNTIJARYHMÄ**
  kts. www.tietosuoja.fi

Version: 20 September 2017

Article 29 Data Protection Working Party
DRAFT AGENDA
112th meeting
3 and 4 October 2017
ALBERT BORSCHETTE Conference Centre, Room AB-4C - Rue Froissart 36, 1040 Bruxelles

October 3, 2017

Morning

Items A: Documents for adoption without discussion

A.1 10:00 – 10:05 Draft agenda **(adoption)**
A.2 10:05 – 10:10 Draft minutes of the 111th meeting **(adoption)**

Items B: Information given by the Chair and the EU Commission (10:10 – 10:20)

B.1 Request for observer status from the Moldavian Data Protection Authority

Items C: Topics for discussion

C.1 10:20 – 12:00 **EU-U.S. Privacy Shield**
a. Joint review – **Feedback from the WP29 review team** (Rapporteur: WP29 review team)
b. Points that delegations wish to raise
Contact: Chair, B. Gencarelli (DG JUST)

C.2 12:00 – 12:30 **EDPB – Implementation of the GDPR**
a. Guidelines for controllers and processors
- Data Protection Impact Assessment – **adoption** (Rapporteur: FR DPA)

Afternoon

C.2 14:00 – 18:00 **EDPB – Implementation of the GDPR**

- Certification – **discussion** (Rapporteur: DE DPA)
- Profiling – **adoption** (Rapporteurs: EDPS, FR DPA, IT DPA, NO DPA, UK DPA)
- Consent – **discussion** (Rapporteurs: DE DPA, EDPS, FR DPA, NL DPA, UK DPA)
- Transparency – **discussion** (Rapporteurs: EDPS, IE DPA, UK DPA)
- Data breach notification – **adoption** (Rapporteur: UK DPA)
- Adequacy referential – **discussion** (Rapporteur: FR DPA)
- BCR-Controller referential – **discussion** (Rapporteur: IT DPA)
- BCR-Processor referential – **discussion** (Rapporteur: FR DPA)
- Derogations for transfers – **discussion** (Rapporteurs: DE DPA, FR DPA)

b. Internal topics for WP29/EDPB
   - Administrative fines – **adoption** (Rapporteurs: NO DPA, UK DPA)
   - Urgency procedure – **adoption** (Rapporteurs: FR DPA, NL DPA)
   - Procedure for EDPB dispute resolution system – **discussion** (Rapporteur: FR DPA)

c. Setting up the EDPB
   - MOU EDPB-EDPS – **discussion** (Rapporteur: EDPB taskforce)
   - Update on IT from EDPB IT taskforce and presentation of the IMI system – **discussion** (Rapporteur: EDPS)

d. APPA-WP29 information template on GDPR – **adoption** (Rapporteur: Chair)

e. DPA ressources - Awareness-raising activities and funding opportunities for DPAs under the Rights and Citizenship Programme (DG JUST)

f. Points that delegations wish to raise

Contact: Chair, O. Micol, K. Mojzesowicz (DG JUST)

October 4, 2017

Morning

C.3 9:30 – 10:15 **BTLE subgroup**

a. CJUE advice on PNR Canada – **discussion and request for a mandate** (Rapporteurs: BE DPA, DE DPA, EDPS, FR DPA)
b. Directive Police & Justice – **discussion** (Rapporteurs: DE DPA, IT DPA, UK DPA)
c. E-evidence – **discussion** (Rapporteur: DE DPA, EDPS, FR DPA, UK DPA)
d. Points that delegations wish to raise

Contact: DE DPA, J.Sajfert (DG JUST)

C.4 10:15 – 11:00 **Financial Matters subgroup**

a. ESMA – **discussion and possible adoption** (Rapporteur: FR DPA)
b. Codes of conduct in the financial sector – **discussion** (Rapporteur: TBC)
c. Points that delegations wish to raise

Contact: IT DPA, R. Sauer, L.Rozanski (DG JUST)

C.5 11:00 – 11:45 **Enforcement subgroup**

a. WhatsApp – **adoption of a letter** (Rapporteur: UK DPA)
b. TrueCaller, Sync.me, CIA app – **adoption of letters** (Rapporteur: UK DPA)
c. Points that delegations wish to raise

Contact: ES DPA, NL DPA, A.Moscibroda, J.Sajfert (DG JUST)

C.6 11:45 – 12:30 **Technology subgroup**

a. Formal designation of the new coordinator of the subgroup
b. BEUC letter on Google privacy policy and Facebook emotional ad-targeting – **adoption of a letter**
c. C-ITS opinion – **adoption** (Rapporteur: IT DPA)
d. Request for mandate to work on sector specific FAQ on data portability
e. EASA consultation on drones – **discussion** (Rapporteur: HR DPA, UK DPA)
f. Points that delegations wish to raise

Contact: UK DPA, K. Mojzesowicz (DG JUST), Rosa Barcelo (DG CONNECT)

D. Miscellaneous (12:30-12:45)

D.1 Information that delegations wish to share

- Code of conduct for the medical profession on the ethical use of health data
- Agreement between National Authorities that are responsible for eHealth, regarding the sharing of health data between Member States in the context of eHealth Information Services
- Global Cross Border Enforcement Arrangement adopted in the framework of the ICDPPC

(hyväksytty 4.10.2017 mennessä)
Tietosuojatyöryhmä WP 29 ohjeet tietosuoja-asetuksen soveltamisesta:

- Tietosuojavastaavat
- Tietojen siirto järjestelmästä toiseen
- Johtavan valvontaviranomaisen määrittäminen
- Tietosuojaa koskeva vaikutustenarviointi

- Profilointi (pian avoimella lausuntokierroksella)
- Henkilötietojen tietoturvaloukkauksesta ilmoittaminen (pian avoimella lausuntokierroksella)
- Hallinnolliset sakot (sisäinen asiakirja)
- Kiireellinen menettely (sisäinen asiakirja)

Nostoja

Tietosuojavastaavat (Guidelines on Data Protection Officer (’DPOs’) 16/EN WP 243 rev.01 Adopted on 13 December 2016 As last Revised and Adopted on 5 April 2017)

Tietosuojavastaavat

- Tiettyjen rekisterinpitäjien ja henkilötietojen käsittelijöiden on nimitettävä tietosuojavastaava
  - Myös vapaaehtoisuuteen perustuen
- Tarkoituksena helpottaa vaatimustenmukaisuuden ja osoitusvelvollisuuden toteutumista sekä muodostaa kilpailuetu yrityksille
- Tietosuojavastaavat eivät ole henkilökohtaisesti vastuussa henkilötietojen käsittelyn lainmukaisuudesta
- Tietosuojavastaavat ovat keskeinen elementti tiedonhallintakokonaisuudessa

Milloin on nimitettävä? (37 art. (1) (a))

- Yksityinen sektori suorittaa julkisen sektorin tehtäviä. Tietosuojavastaavan nimittäminen ei pakollista a kohdan nojalla, mutta WP 29 suosittelee tietosuojavastaavan nimittämistä myös tällöin

Milloin on nimitettävä? (37 art. (1) (b) ja (c))

- **Ydintehtävät**
  - Liittyy ensisijaisiin toimintoihin, eikä oheistoimintana tapahtuvaan käsittelyyn
  - Myös toiminnot, joihin henkilötietojen käsittely liittyy erottamattomana osana
  - Sairaalat, yksityisen tahon suorittama laajamittainen kameravalvonta julkisilla paikoilla
  - Oheistoiminnoista esim. työntekijöiden palkan maksu, standardit IT-tukitoiminnot

Milloin on nimitettävä? (37 art. (1) (b) ja (c))

- **Laajamittaista**
  - Vielä ei voida antaa tarkkoja lukuja
  - Huomioida
    - Rekisteröityjen määrä
    - Datan käsittelyn laajuus/tietotyyppien määrä
    - Käsittelyn kesto tai pysyvyys
    - Käsittelyn maantieteellinen laajuus

Milloin on nimitettävä? (37 art. (1) (b))

- **Säännöllinen ja järjestelmällinen seuranta**
  - Kaiken tyyppinen seuranta ja profilointi verkossa, mukaan lukien kohdennettua markkinointia varten
  - Myös seuranta muualla kuin verkossa
- Säännöllinen
  - Jatkuva tai tapahtuu tietyn aikavälein tietyn ajanjakson ajan
  - Toistuva tai toistetaan tietyn ajanjakson ajan
  - Kokoajan tai määräajoin tapahtuvaa
- Järjestelmällinen
  - Tapahtuu tietyn järjestelmän mukaisesti
  - Järjestetty ja organisoitu
  - Tapahtuu osana yleistä datan keräyssuunnitelmaa
  - Tapahtuu osana tiettyä strategiaa

Milloin on nimitettävä? (37 art. (1) (c))

- Käsitellään erityisiin henkilötietoryhmiin kuuluvia tietoja ***tai*** 10 artiklassa tarkoitettuja rikostuomioihin tai rikkomuksiin liittyviä tietoja

Milloin on nimitettävä?

- Jos on tulkinnanvaraista, WP 29 suosittelee, että arviointiprosessi dokumentoidaan (24 art. 1 kohta)
  - Vapaaehtoisuuteen perustuen
  - Joku muu henkilö kuin tietosuojavastaava
- Henkilötietojen käsittelijä
- Konsernille yksi DPO? Edellyttäen, että voidaan helposti ottaa yhteyttä jokaisesta toimipaikasta

Kenestä tietosuojavastaava?

- Huomioon henkilön **ammattipätevyys** ja erityisesti **asiantuntemus tietosuojalainsäädännöstä ja alan käytänteistä** sekä **valmiudet suorittaa** 39 artiklassa tarkoitetut tehtävät
- Palvelussopimuksen perusteella
- Tiimi

Miten tietosuojavastaavan asema varmistetaan

- Otetaan asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn
- Riittävät resurssit
- Tietosuojavastaavan aseman keskeinen elementti on riippumattomuus
- ”Irtisanomissuoja”

Miten tietosuojavastaavan asema varmistetaan

- Muut tehtävät eivät saa aiheuttaa eturistiriitoja
  - Määritellään yhteensopimattomat tehtävät ja asemat organisaatiossa
  - Sisäiset ohjeistukset, avataan ristiriidat

KIITOS KUUNTELUSTA

Lisätietoja: www.tietosuoja.fi

Reijo Aarnio
tietosuojavaltuutettu

Tietosuojavaltuutetun toimisto

Tietosuojafoorumi 6.10.2017

Tietosuojatyö kansainvälisessä organisaatiossa

Minna Ääri

Oy IBM Finland Ab

IBM ihmiset ja liiketoiminta

400,000+ employees

170+ countries

Cloud

Analytics

Mobile

Security

Cognitive Computing

Social

IBM:n matka tietosuojatyössä

- 1970 – Privacy Policy
- 1970 → ohjeistukset laajenivat
- 2000 Chief Privacy Officer nimitys
- 2007 Corporate Privacy Office perustaminen

IBM:n tietosuojatyön raamit

Perusta, kulmakivi, organisaatio ja valvonta

Tietosuojatyön perusta

- **Globaalit politiikat sekä**
- Yhtiön ohjeet, menettelytavat ja standardit
  - IBM:n kontrolloiman henkilötiedon osalta
  - Kerääminen, käyttö, luovuttaminen, pääsyoikeudet, säilyttäminen, suojaaminen, ym.
- Ajantasaiset ohjeet
  - Markkinointi, some, maidenväliset siirrot, kolmannet osapuolet, mobiiliappien kehitys, ym.

The world is built and fuelled by data

Cristina Cabella

Chief Privacy Officer, IBM Corporation

Implementointi

- **Globaalit tietosuojaohjelmat (Programs)**
- Jalkauttavat konsernin politiikan käytännössä ja tuottavat sen lopputuloksen, että IBM täyttää lakisääteiset velvoitteensa ympäri maailmaa -> riskien hallinta
  - Global Privacy Assessment Program
  - Data Incident Reporting & Management
  - Global Access Request Process
  - Education & Awareness

Transparency and Trust in the Cognitive Era.

THINK Blog

IBM

Kulmakivi: IBM Global Privacy Assessment Program

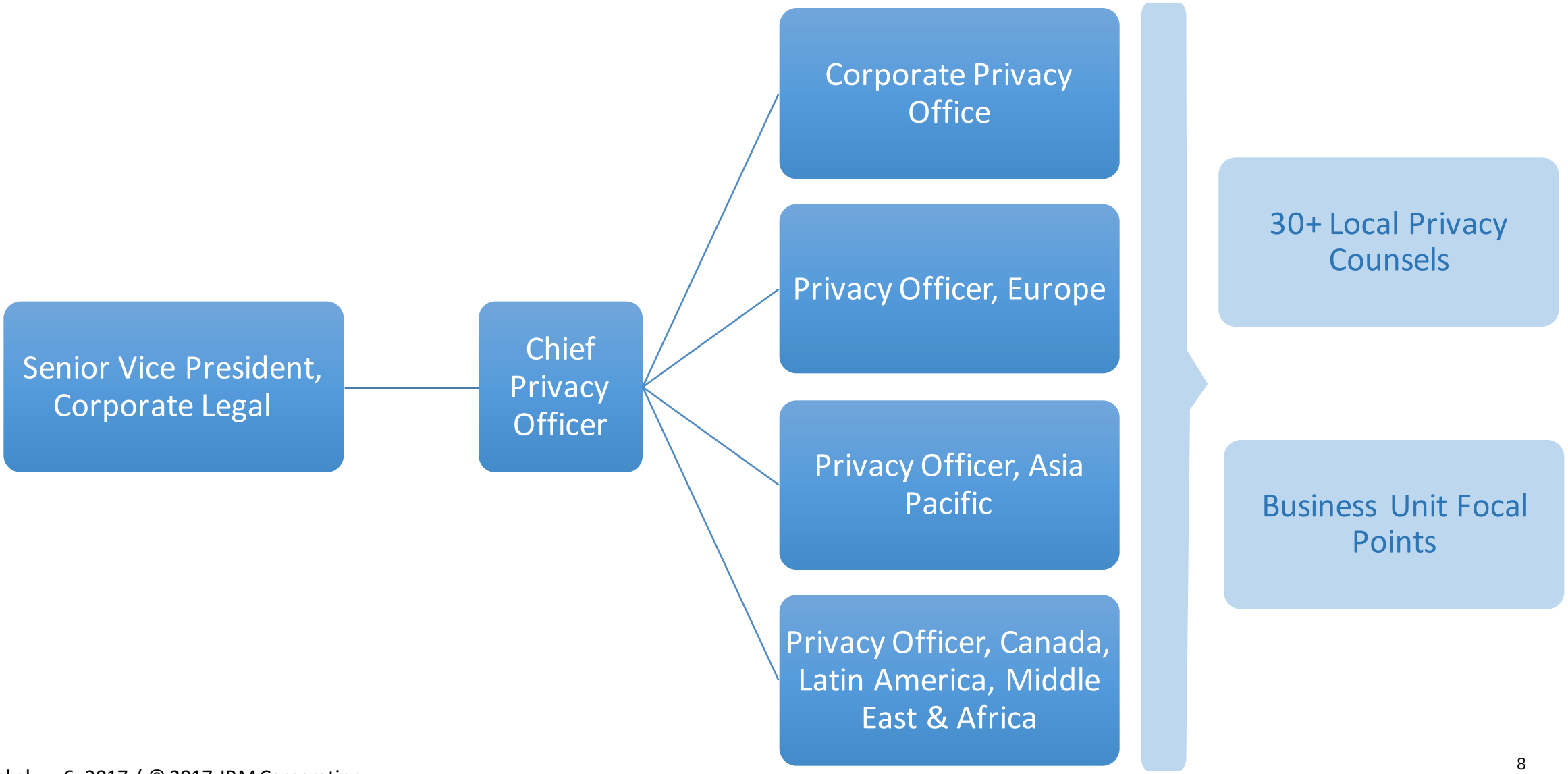
Liiketoimintaprosessit, sovellukset, hankkeet – tietosuojan ennakollinen arviointi kattavasti ja dokumentoidusti

Varmistaa lakien ja viranomaismääräysten ja sisäisten vaatimusten noudattamisen

Riskien ymmärtäminen, mitigointi ja tarvittavat toimet

Ohjaa tietosuojalakimiesten tarkistukseen ja vaadittuihin viranomaistoimiin

Sisäinen toimintaympäristö



Jalkauttaminen

Kommunikaatio

Yhteinen kieli “privacy”

Oivalluttaminen vaatii panosta
→
Sisäistäminen oman työn kautta

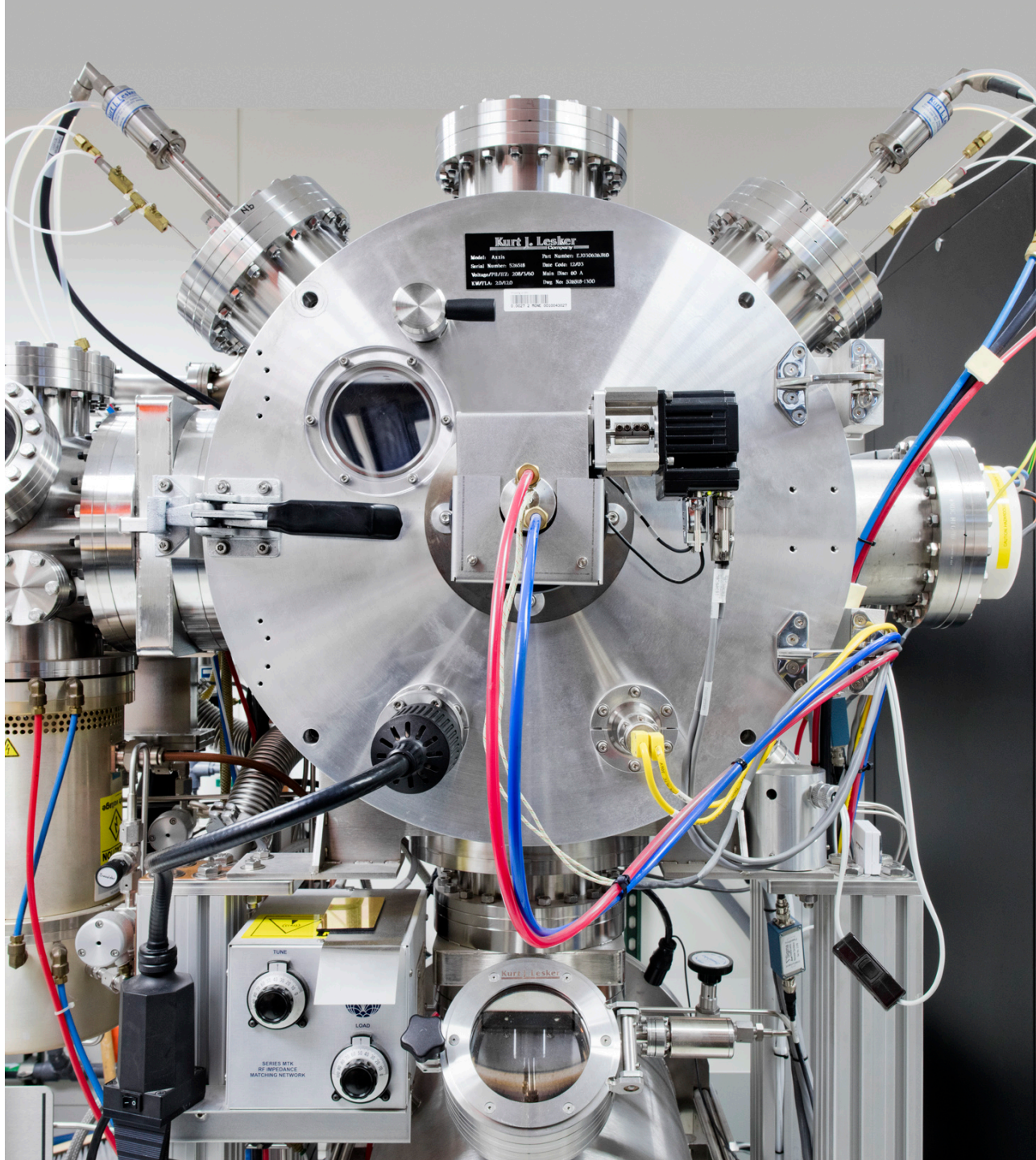
Oikein tekemisen varmistaminen

- Valvo ja testaa
- Auditointi
- Pistokokeet
- Erityisesti alueet ja toimet, joissa riski suuri tai niihin kohdistuu sertifiointi (esim. CBPR; EU/US DPS)

IBM ja Tietosuoja-asetus

IBM valmistautuminen Tietosuoja-asetukseen

- Globaali fokus
- työtä koordinoi IBM GDPR Program Management Office
- Ibm.com/GDPR
  - IBM´s Commitment to GDPR Readiness
  - How can IBM help on your journey to GDPR readiness



Kiitos !

Minna Ääri
Henkilöstöjohtaja, Oy IBM Finland Ab

minna.aari@fi.ibm.com
040 5590833
ibm.com

Twitter: Minna K Ääri @AariMinna

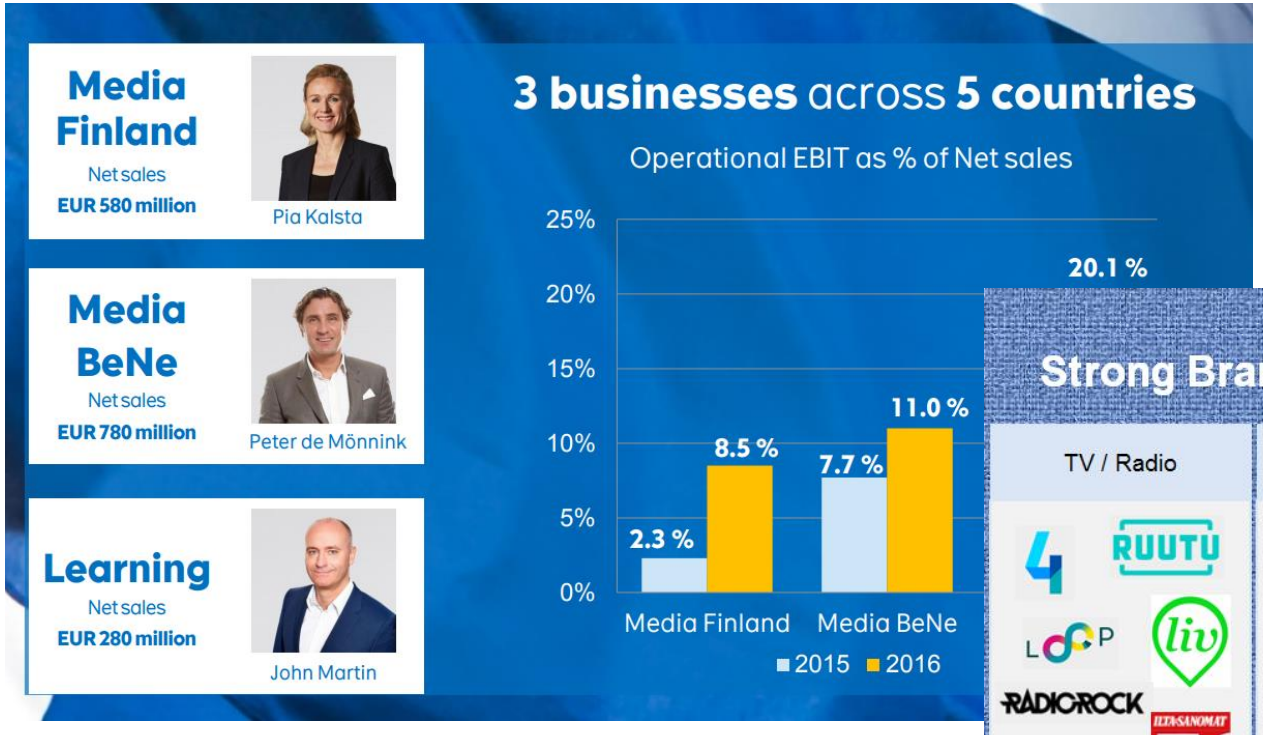
Näkökulmia käytännön työhön

6.10.2017
Laura Tarhonen
Privacy Manager Sanoma

Pictures: Sanoma; unsplash.com

sanoma get the world

Sanoman liiketoiminta keskittyy mediaan ja oppimateriaaleihin & digitaalisiin oppimisratkaisuihin



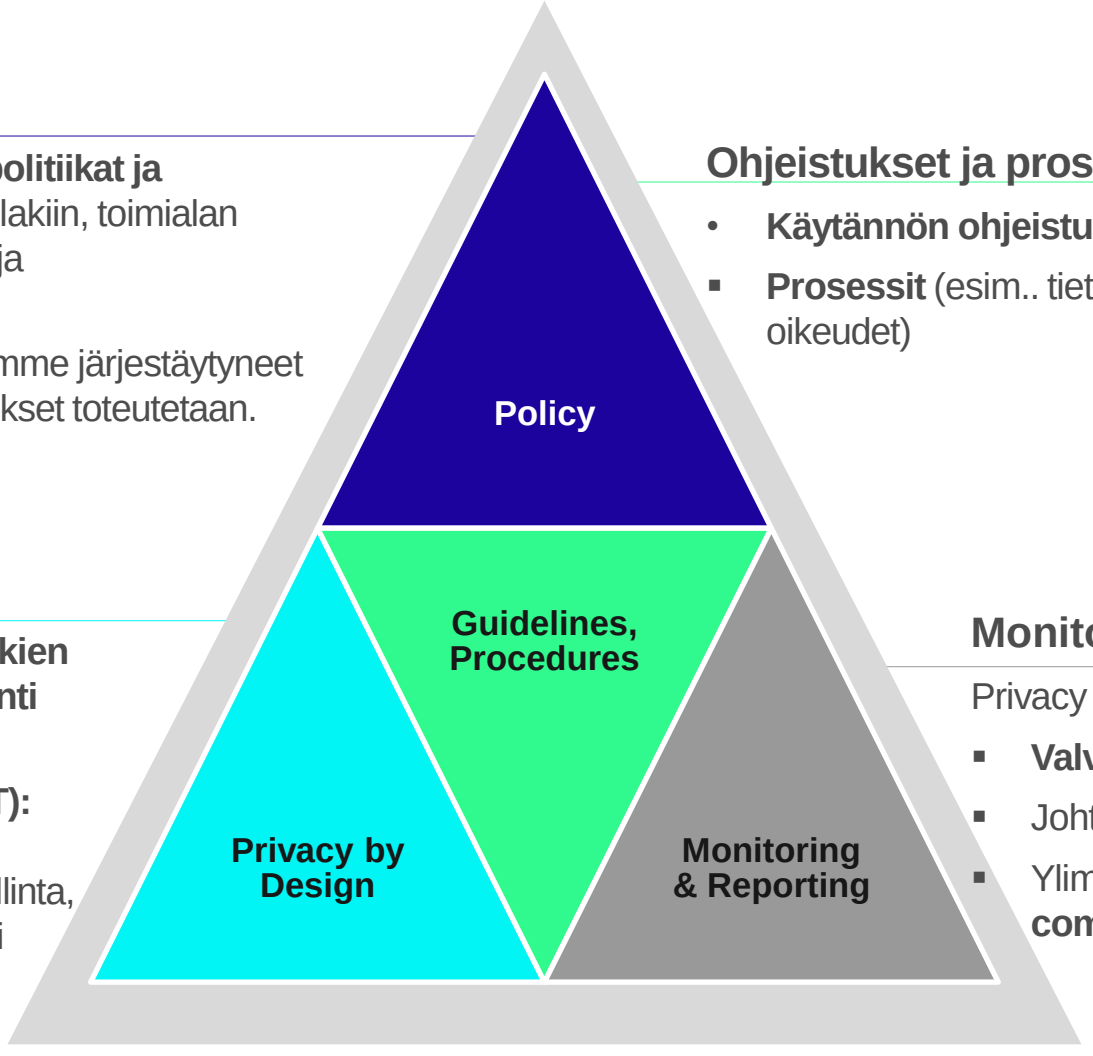
Sanoman tietosuojaohjelman osa-alueet

Politiikat

- Sanoman **tietosuojan politiikat ja periaatteet** pohjautuvat lakiin, toimialan parhaisiin käytäntöihin, ja itsesäätelyohjeistuksiin.
- **Governance**: miten olemme järjestäytyneet jotta tietosuojan vaatimukset toteutetaan.

Ohjeistukset ja prosessit

- **Käytännön ohjeistukset**
- **Prosessit** (esim.. tietoturva, laatu, kuluttajien oikeudet)



Privacy by Design

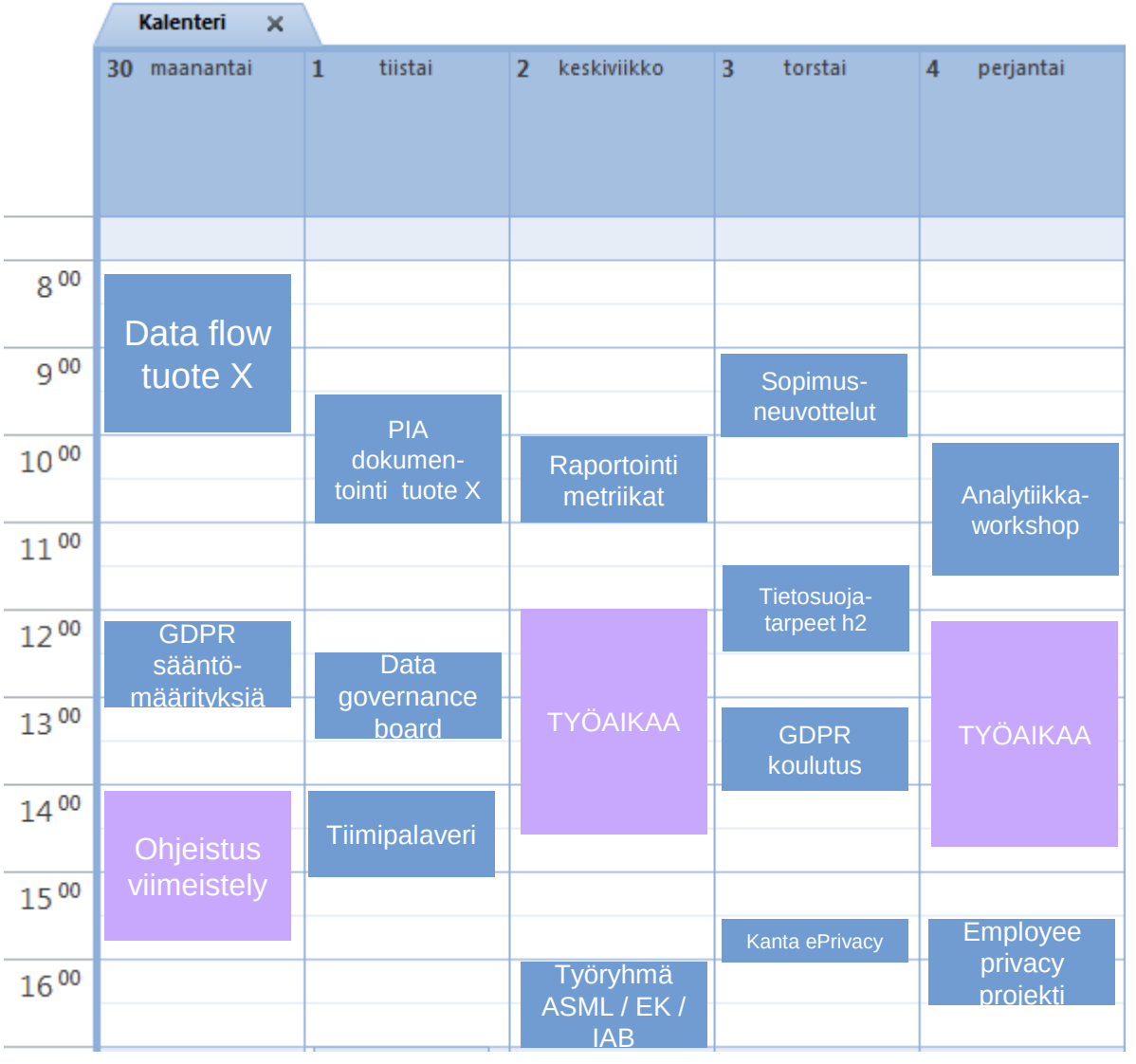
- **Proaktiivinen ja jatkuva uhkien ja mahdollisuuksien arviointi** liiketoiminnan operaatioissa.
- **Tietosuojateknologiat (PET):** Läpinäkyvyys, käyttäjäystävällisyys, lupahallinta, tiedon käsittelyn säännöt läpi tiedon elinkaaren, tietoturva

Monitorointi & raportointi

Privacy tiimi

- **Valvoo ohjeistusta ja toteutusta,**
- Johtaa **riskienhallintaa** ja
- Ylimmän johdon **informointi ja compliance raportointi**.

Mitä tietosuoja-asiantuntija tekee?



1. Tietoisuuden lisääminen
   - Koulutukset, workshopit, liiketoiminnan suunnittelukokoukset
2. Päätökset, linjaukset, ohjeet ja vaatimukset liiketoiminnalle
3. Vaikutustenarvioinnit ja vastaukset päivittäisiin kysymyksiin
4. Sopimukset
5. Toimialayhteistyö
6. Raportointi johdolle

TOP 3 vaatimukset
1. Kyky toimia sujuvasti monella abstraktiotasolla ja selittää asioita ymmärrettävästi
2. Ymmärrys teknologioista ja liiketoiminnasta
3. Uskallus antaa suosituksia ja tehdä linjauksia

Haasteita

- Yhteisen kielen löytäminen ja termien vakiinnuttaminen
- Monimutkaisten asioiden yksinkertaistaminen
- Teknologian ja lainsäädännön yhteensovittaminen
- Dokumentoinnin ja raportoinnin pitäminen ajantasalla
- Priorisointi: tietoisuuden kasvaessa kysymykset lisääntyvät eksponentiaalisesti

Hyviä käytänteitä

- Älä keksi pyörää uudelleen
- Seuraa aktiivisesti tietosuojaan liittyviä uutisia ja viranomaisten tulkintoja
- Jos joku asia tuntuu liian monimutkaiselta palastele
- Älä jää yksin, äläkä nojaa pelkkiin oletuksiin

- Oikotietä onneen ei ole… mutta yleensä tietovirtojen kuvaus ja vaikutustenarvioinnit voivat ratkaista monta ongelmaa yhdellä kertaa

- Resepti tietosuojavallankumoukseen:
  - **Vetoa tunteisiin**
  - **Kerro riskeistä ja mahdollisuuksista**
  - **Tee tietosuojavaatimusten noudattamisesta helppoa**

Kiitos!

We use data to serve customers better!

Laura Tarhonen

laura.tarhonen@sanoma.com

Työpajat

- Pöytäryhmittäin
- Sarake kerrallaan vasemmalta oikealle
- Aikaa 30-40 minuuttia yhteensä