EU:n uusi tietosuoja-asetus tulee, oletko valmis?

KEUKE
20.3.2018
Markus Myhrberg

LEXIA
Legal Excellence

Uudistuva tietosuojasääntely

Mistä on kyse ja mikä muuttuu?

Sääntelykehys

Keskeiset käsitteet

Rekisteröityjen oikeudet

Sopimukset

Tietoturva

Dokumentit

Tietosuoja-asetus haltuun

Tietosuoja-asetus: Mistä on kyse?

Tietovuodot 26.9. 15:42

Tuhansien ihmisten laboratoriotuloksia vuosi internetiin, kun THL:n työntekijä laati esitystä – salaiset tiedot ehtivät olla verkossa useita kuukausia

Kyseessä ei ole ollut tietomurto vaan inhimillinen virhe tietojen käsittelyssä. Ensi vuonna voimaan tulevassa tietosuoja-asetuksessa kömmähdyksistä saatettaisiin määrätä muhkea sanktio.

Debatti: EU:n uusi tietosuoja-asetus auttaa pistämään datan kunnolla töihin

20.7.2017 10:30

Home » News » Editor's Choice » Dealers urged to prepare now for 2018 GDPR

Dealers urged to prepare now for 2018 GDPR data protection rules

Posted by: Curtis Hutchinson in Editor's Choice, Latest News Friday, 26 May 2017 0

Google tallentaa osan puheestasi – EU-asetus tuo helpotusta, jos tämä tuli yllätyksenä

New EU data regulation aims to protect driver privacy

03/05/2016 in Fleet Industry News

FT: Työnhakijan Facebook-profiilin kurkkimiseen pitää olla pätevä syy, toteaa EU:n työryhmä

Arviolta 60 prosenttia työnantajista hyödyntää sosiaalista mediaa rekrytoinnissaan, mutta osuus saattaa pian pudota roimasti.

Tietosuoja 13.7.2017 klo 13:20

Tietosuoja-asetus: Mistä on kyse?

- Koskee **henkilötietojen käsittelyä**

- Asetus tullut voimaan toukokuussa 2016, mutta **sitä sovelletaan 25.5.2018 lähtien**
  - Siirtymäaika tarjonnut mahdollisuuden saada käytännöt ja järjestelmät asetuksen mukaisiksi ennen soveltamisen aloittamista.
  - Asetus korvaa nykyisen henkilötietodirektiivin ja henkilötietolain

- Asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa
  - Kansallisia poikkeuksia
    - Uusi tietosuojalaki
    - Erityislakeja, joissa tietosuoja-asioita

Keskeinen tietosuojasääntely 25.5.2018

Yleinen tietosuoja-asetus ((GDPR)
(ePrivacy Directive)

Tietosuojalaki

Tietoyhteiskuntakaari
(evästeet, sähköinen suora)

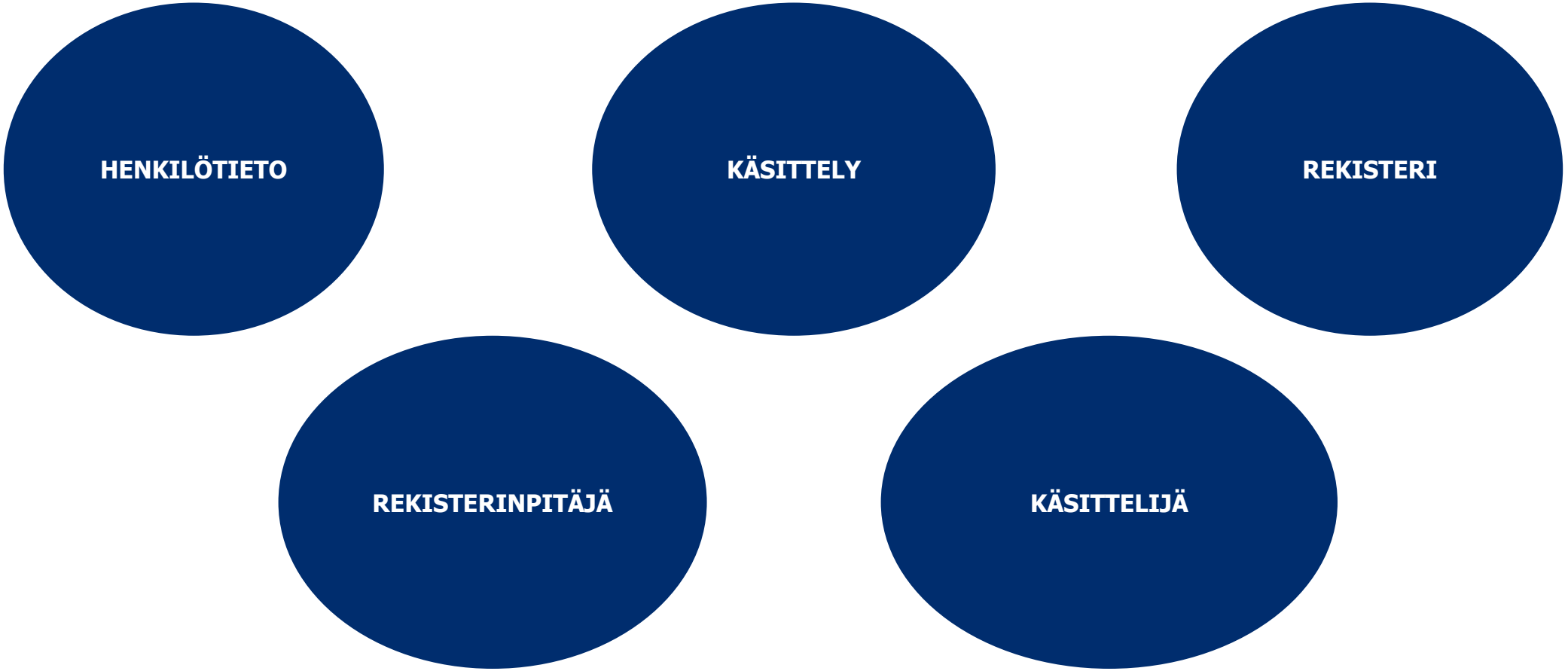
Työelämän tietosuojalaki

Erityislainsäädäntö

Mikä muuttuu?

- Annettava aiempaa enemmän informaatiota henkilötietojen käsittelystä
- Rekisteröidyllä enemmän oikeuksia, kattavampi informointi
- Laadittava uusia sisäisiä dokumentteja
  - compliance & accountability
- Käsittelijän vastuu ja velvollisuudet
- Laadittava tai päivitettävä sopimukset palveluntarjoajien kanssa
- Viranomaisvalvonta ja sanktiot

Keskeiset käsitteet



Rekisterinpitäjän velvollisuudet

Kohti **periaatekeskeisempää** sääntelyä

Kaiken toiminnan lähtökohtana **riskiperusteinen lähestymistapa**

Noudattamisvelvollisuus ja **osoittamis**velvollisuus

Oletusarvoinen ja sisäänrakennettu tietosuoja

Käsittelyssä noudatettavat periaatteet

✓**Noudatettava** henkilötietojen käsittelyssä

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

✓Pystyttävä **osoittamaan** noudattaminen

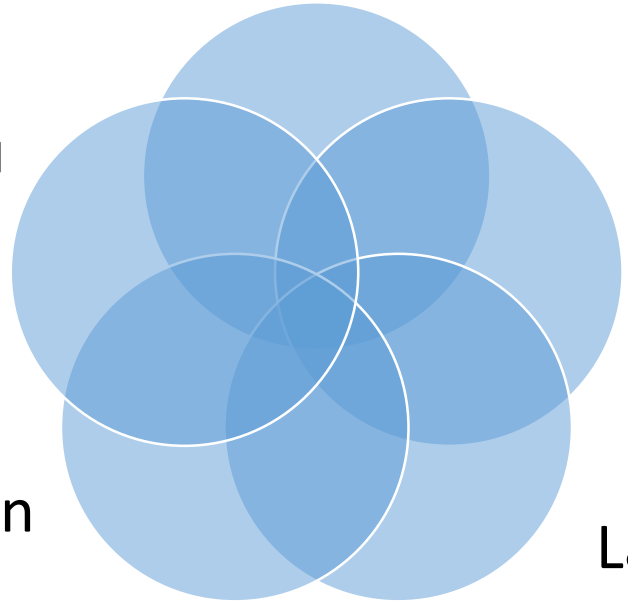
4. Täsmällisyys
5. Säilytyksen rajoittaminen
6. Eheys ja luottamuksellisuus

Käsittelyperuste

Määrittele etukäteen
Muista osoitusvelvollisuus

Suostumus

Oikeutettu etu



Sopimus

Elintärkeiden etujen suojaaminen

Lakisääteisen velvoite

Asiakastietojen käsittely

- Asiakkuutta ei määritelty asetuksessa (resitaaleissa mainittu…)

- Asiakkaista saa käsitellä tietoja, jotka **sopimuksen kannalta** tarpeellisia
  - Myös **oikeutettu etu** perusteena
    - Suostumus, jos ei muuta perustetta
  - Milloin asiakassuhde **syntyy**?
    - Ostotapahtuma, rekisteröityminen,

- Määritteltävä mm.
  - **Mitä tietoja tarpeen käsitellä** asiakassuhteen kannalta? (tietojen minimointi)
    - Asiakkaan tiedot, esim. yhteystiedot
  - Milloin **asiakassuhde päättyy**? (säilytyksen rajoittaminen)
    - Tietojen säilytysprosessin ja säilytysajan määrittäminen (tai määrittämiskriteerit)
  - Tietojen oltava **täsmällisiä ja päivitettyjä** (täsmällisyys)

Markkinointitietojen käsittely

- Asetuksessa **ei** vastaavaa jaottelua kuin henkilötietolaissa pysyvään markkinointirekisteriin, kampanjarekisteriin ja yhteystietorekisteriin (BtoB)

- Markkinointiviestintään liittyvien tietojen erottaminen
  - Mitkä tiedot tarpeen markkinointia varten (pyri minimoimaan)
  - Käsittelyperuste: **oikeutettu etu, sopimus tai suostumus**
  - **Informointivelvoitteet ja kielto-oikeus**

- Automaattinen profilointi

Tietoyhteiskuntakaari
- **Sähköinen suoramarkkinointi** (sähköposti, sms)
  - BtoC etukäteinen suostumus, BtoB kielto-oikeus
- Evästeet ja muu tekninen seuranta
- Seuraa muutoksia 2019/2020

Rekisteröityjen informointi

- **Läpinäkyvää** ja **helposti saatavilla olevaa** informointia
- Helposti ymmärrettävässä, tiiviissä muodossa ja yksinkertaisella kielellä
  - Laajempi informointivelvollisuus → **tietosuojakäytäntö**
    - Saatavilla eri kanavissa
  - Kattavalla informoinnilla voi pienentää tarvetta **tarkastusoikeuden** käyttämiseen
  - Samalla voi hoitaa **tietoyhteiskuntakaaren** edellyttämien informointivelvoitteita

Rekisteröityjen informointi

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

Rekisteröityjen oikeudet

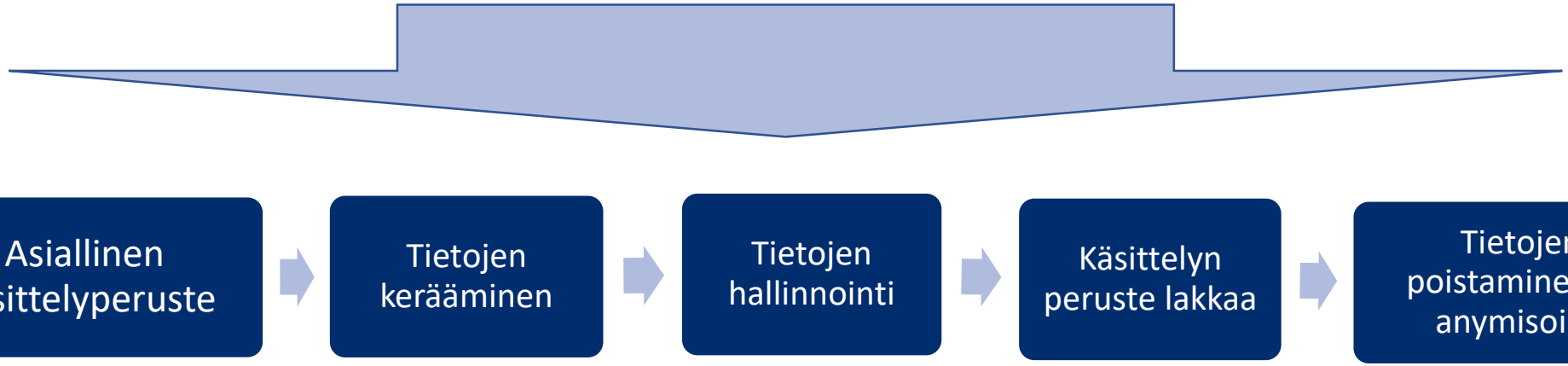
- Oikeus saada läpinäkyvää ja ajantasaista tietoa
- Oikeus päästä tietoihin
- Oikeus tietojen oikaisuun
- Oikeus siirtää tiedot järjestelmästä toiseen
- Oikeus tietojen poistamiseen (oikeus tulla unohdetuksi)
- Oikeus käsittelyn rajoittamiseen
- Vastustamisoikeus (suoramarkkinointikielto)
- Oikeus vastustaa profilointia ja käsittelyä oikeutetun edun perusteella (mm. markkinointi)
- Oikeus olla joutumatta automaattista päätöksenteon kohteeksi
- Oikeus saada ilmoitus tietoturvaloukkauksesta
- Oikeus luottaa tietoturvan korkeaan tasoon

MITEN HUOMIOIN OMASSA TOIMINNASSANI?

- Järjestelmät, toimintatavat, ohjeistukset jne.

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

Tietoturvaloukkaukset

Tietoturvaloukkaus, **josta voi aiheutua** rekisteröityjen oikeuksiin ja vapauksiin kohdistuvaa riskiä

- Ilmoitettava siitä **ilman aiheetonta** viivytystä ja **mahdollisuuksien mukaan 72 tunnin** kuluessa valvontaviranomaiselle.
- Jos todennäköisesti aiheuttaa **korkean riskin** luonnollisten henkilöiden oikeuksille ja vapauksille, rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta **rekisteröidylle** ilman aiheetonta viivytystä.
- Ilmoituksen sisällöstä tarkemmat määräykset asetuksessa
- Lisäksi rekisterinpitäjän on dokumentoitava tietoturvaloukkaus, sen vaikutukset ja korjaavat toimenpiteet (yksi tekijä arvioitaessa, onko sääntelyä noudatettu)

Toiminta tietoturvaloukkauksen sattuessa

- Arvio, **aiheutuuko riskiä rekisteröityjen oikeuksille**: ilmoitus viranomaiselle 72 tunnin kuluessa
- Arvio, aiheutuuko **korkeaa riskiä rekisteröidyille:** Ilmoitus rekisteröidyille ilman aiheetonta viivytystä. Ei tarvita ilmoitusta, jos
  - Tiedot on riittävällä tasolla salattu
  - Suoritettu jatkotoimenpiteet riskin poistamiseksi
  - Aiheuttaa kohtuutonta vaivaa
- Joka tapauksessa kaikki tietoturvaloukkaukset dokumentoitava
- Käytännössä mahdoton toteuttaa vaaditussa ajassa, ellei mietitty ennakolta!

Tietosuojavastaava

- Rekisterinpitäjän ja käsittelijän on nimitettävä tietosuojavastaava:
  - *”ydintehtävät muodostuvat käsittelytoimista, jotka **luonteensa, laajuutensa ja/tai tarkoitustensa vuoksi edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa**;”*
  - *rekisterinpitäjän tai henkilötietojen käsittelijän **ydintehtävät** muodostuvat laajamittaisesta käsittelystä, **joka kohdistuu erityisiin henkilötietoryhmiin**.*

- Yksi keino täyttää **osoitusvelvollisuutta,** usein kannattaa nimittää vaikka ei olisi suoraa velvollisuutta

Palvelu- ja alihankintasopimukset

- Rekisterinpitäjän ja käsittelijän välille henkilötietojen käsittelyä koskeva sopimus
- Asetus **velvoittaa sopimaan** kirjallisesti useista seikoista
  - Sovittava mm. käsittelyn kohteesta, kestosta, tarkoituksesta ja osapuolten velvollisuuksista & oikeuksista, ohjeistus, tietoturva, rekisteröidyn oikeudet, auditointi, salassapito, poistaminen
- Tietosuojaa koskevat sopimusehdot ja/tai tietosuojaliitteet osaksi normaaleja sopimuskäytäntöjä
  - Yksi osatekijä **osoitusvelvollisuuden täyttämisessä**
- Vastuukysymysten ja riskienhallinnan näkökulmasta myös **suositeltavaa sopia** aiempaa tarkemmin myös tietosuojaan liittyvistä seikoista
  - Vastuunrajoitusten merkitys korostuu

Tietosuojadokumentaatio

→ ARVIOI TARVE SUHTEESSA OMAAN TOIMINTAAN

- ? **TIETOVARANTOJEN JA TIETOVIRTOJEN DOKUMENTOINTI**
- ? **TIETOSUOJAKÄYTÄNNÖT JA KÄSITTELYSELOSTEET**
- ? **SOPIMUKSET KÄSITTELIJÖIDEN KANSSA (DPA)**
- ? TIETOSUOJA- JA TIETOTURVAPOLITIIKAT, SISÄISET OHJEISTUKSET
- ? PROSESSIKUVAUKSET
- ? VAIKUTUSTENARVIOINNIN JA PÄÄTÖSTEN DOKUMENTOINTI
- ? TIETOSUOJA-ORGANISAATION / TIETOSUOJAVASTAAVAN TOIMINNAN DOKUMENTOINTI

Tapoja täyttää osoitusvelvollisuutta

NYKYTILA-ANALYYSI

- Tee analyysi nykytilasta
- Mitä, missä, miksi, minne, kuinka kauan, miten dokumentoitu,
- Kartoita tietovirrat ja -varannot

DOKUMENTOI PROSESSIT

- Tunnista velvollisuutesi ja dokumentoi käsittelyyn liittyvät prosessit sekä tietosuojaperiaatteet
- Tunne myös alihankkijasi prosessit ja tee kirjallinen sopimus käsittelystä (DPA)
- Tietosuojaseuranta ja ohjeet

NIMITÄ TIETOSUOJAVASTAAVA

- Seuraa tietosuojalainsäädäntöä ja toimii yhteyspisteenä
- Mukana kaikessa tietosuojatoiminnassa – tietosuojatiimi tukena
- Voi nimittää, vaikka ei velvollisuutta

RISKIANALYYSI JA VAIKUTUSTENARVIOINTI

- Asetus perustuu riskiperusteiselle lähestymistavalle
- Tee tarvittaessa asetuksen mukainen vaikutustenarviointi
- Muista oletusarvoisen ja sisäänrakennetun tietosuojan periaate

TIETOTURVA / ORGANISATORISET TOIMET

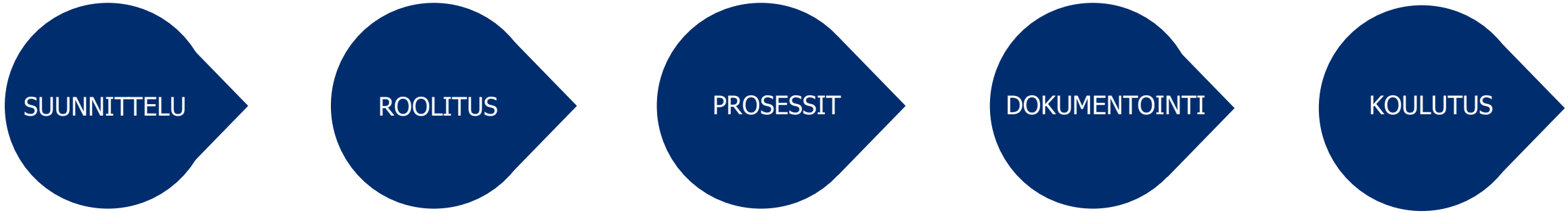
- Huolehdi tietoturvasta
- Tee toimenpidesuunnitelma tietosuojaloukkauksen varalle
- Auditointi
- Salassapito

- Koulutus ja ohjeistus

INFORMOINTI

- Huolehdi avoimuudesta ja läpinäkyvyydestä - pidä saatavilla tietosuojaselosteet
- Laadi tietosuojapolitiikka
- Huolehdi muiltakin osin rekisteröityjen oikeuksien toteutumisesta

Tietosuoja-asetus haltuun



→ Tee nykytila-analyysi ja suunnitelma muutoksista

→ Vastuuta selkeästi: kuka tekee, missä vaiheessa ja mitä

→ Mitä tehdään nykyisille käytännöille ja järjestelmille ja miten huomioidaan tuotekehityksessä

→ Dokumentoi valittujen ratkaisut ja toimenpiteet (osoitusvelvollisuus)
→ Ulkoiset ja sisäiset selosteet ja ohjeistus
→ Seuranta

→ Huolehdi ohjeistamisesta ja koulututa tarvittaessa

Lexia Attorneys Ltd

Markus Myhrberg
Partner
markus.myhberg@lexia.fi
puh. +358 40 505 5343
@markusmyhrberg

Lönnrotinkatu 11
FI - 00120 Helsinki
tel. + 358 10 4244 200
fax. + 358 10 4244 210
www.lexia.fi