KPMG

cutting through complexity

32E28100 - Markkinoiden juridinen toimintaympäristö

Tietosuojalainsäädännön soveltaminen käytännön liiketoiminnassa

16.1.2017

Mikko Viemerö (CIPP/E, CIPM, CIPT, CISA, CISM)
KPMG Cyber Security

TIETOSUOJAN LAINSÄÄDÄNTÖKENTTÄ

TIETOSUOJAN LAINSÄÄDÄNTÖ

Tietosuoja = Yksityisyyden suoja henkilötietojen käsittelyssä

- Henkilötietodirektiivi (95/46/EY)

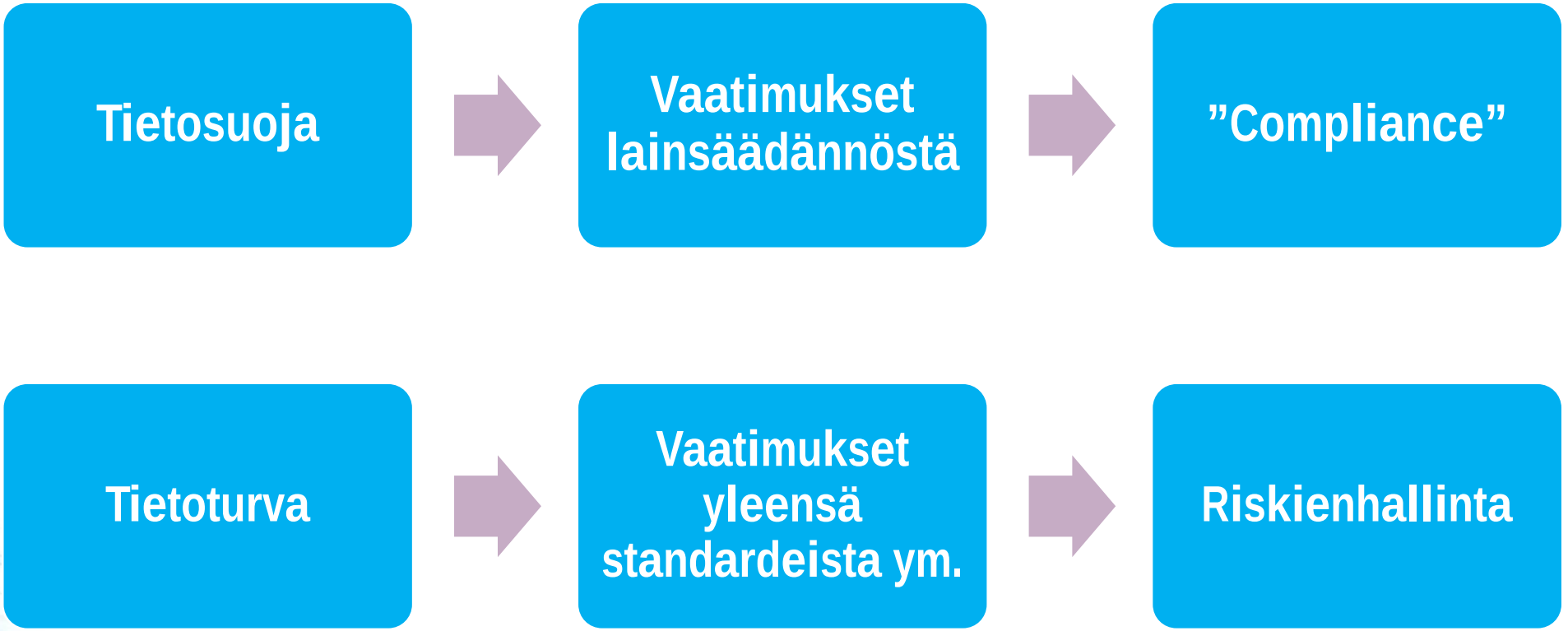
→ Henkilötietolaki (523/1999)

- Sähköisen viestinnän tietosuojadirektiivi (2002/58/EY)

→ Tietoyhteiskuntakaari (917/2014)

- Laki yksityisyydensuojasta työelämässä (759/2004)
- Tulossa: EU:n yleinen tietosuoja-asetus (”GDPR”) & ePrivacy-asetus
- Huomioitava: Julkisuuslaki (621/1999)
- Alakohtaista erityissääntelyä
- Tietoturvallisuutta säätelee mm.
  - Kansallinen tietoturva-asetus (681/2010)
  - NIS-direktiivi (2016/1148/EU)

TIETOSUOJA vs. TIETOTURVA



TIETOSUOJAN PERUSTEET

TIETOSUOJAN PERUSTEET

Määritelmiä

- **Henkilötiedolla** tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä 'rekisteröity';
  - → Kynnys henkilötiedon määritelmän täyttymiselle on matala, esim. IP-osoitteet ja pseudonymisoidut tiedot tulkitaan henkilötiedoiksi (huom. myös "toxic combinations")
  - Huom! Arkaluonteiset henkilötiedot

- **Henkilötietojen käsittely**llä tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista;

- **Henkilörekisteri**llä tarkoitetaan mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu (**"looginen rekisteri"**);

- **Rekisterinpitäjä**llä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot; jos tällaisen käsittelyn tarkoitukset ja keinot määritellään unionin tai jäsenvaltioiden lainsäädännössä, rekisterinpitäjä tai tämän nimittämistä koskevat erityiset kriteerit voidaan vahvistaa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti (vrt. **henkilötietojen käsittelijä**).

TIETOSUOJAN PERUSTEET

Henkilötietojen käsittelyn perusteet, mm.

- Rekisteröidyn suostumus
- Asiakkuussuhteen hoito
- Sopimuksen täytäntöönpano
- Työsuhde
- Muu laista johtuva velvoite

Henkilötietojen käsittelyn periaatteet

- Lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- Käyttötarkoitussidonnaisuus
- Tietojen minimointi
- Täsmällisyys
- Säilytyksen rajoittaminen

TIETOSUOJAN PERUSTEET

Rekisteröidyn oikeudet

- Tiedonsaantioikeus (→ rekisteriseloste / tietosuojaseloste)
- Rekisteröidyn oikeus saada pääsy tietoihin
- Oikeus tietojen oikaisemiseen
- Oikeus tietojen poistamiseen (”oikeus tulla unohdetuksi”)
- Oikeus käsittelyn rajoittamiseen
- Oikeus siirtää tiedot järjestelmästä toiseen
- Vastustamisoikeus

EU:N YLEINEN TIETOSUOJA-ASETUS

EU:N YLEINEN TIETOSUOJA-ASETUS

- EU:n yleinen tietosuoja-asetus korvaa henkilötietolain
- Asetus hyväksyttiin 14.4.2016
- Kahden vuoden siirtymäaika → velvoittava 25.5.2018
- Vaatimuksia tehostetaan tuntuvilla sanktioilla (jopa 20 MEUR / 4% globaalista liikevaihdosta)
- Asetuksen tarkoitus on
  - yhtenäistää henkilötietojen käsittelyn sääntely EU:n alueella
  - selkeyttää toimivaltakysymyksiä
  - tehostaa viranomaisyhteistyötä
  - selkeyttää sääntelyn käsitteitä
  - ottaa kantaa uusiin ilmiöihin ja teknologioihin
  - vahvistaa rekisteröityjen asemaa ja oikeuksia
  - velvoittaa rekisterinpitäjät toimimaan suunnitelmallisesti ja osoittamaan toimiensa vaatimustenmukaisuus

TIETOSUOJA-ASETUKSEN VAATIMUKSET

Uudet säännökset, mm.	Tiukennukset entisiin vaatimuksiin, mm.
Osoitusvelvollisuuden periaate	Säännösten sovellettavuus (henkilötiedon määritelmä/anonyymidata/pseudonyymidata)
Tietosuoja vaikutustenarvioinnit ("PIA")	Vaatimukset tehokkaalle suostumukselle
"Privacy by Design" ja "Privacy by Default"	Tuntuvat sanktiot asetuksen vaatimusten vastaisista toimista ja velvollisuuksien laiminlyönnistä
Tietovuotoilmoitukset	Kv. tiedonsiirrot
Tietosuojavastaava	Rekisterinpitäjän ja tietojenkäsittelijän välinen suhde (→ sopimusten uudelleenarviointi)
"Right to erasure"	Henkilötietojen käsittelyn oikeusperusteet
Henkilötietojen siirrettävyys	Korotetut toimeenpanovaltuudet viranomaisille
Yhden luukun periaate (viranomaisten yhteistyö)	EU:n ulkopuolisten rekisterinpitäjien velvollisuus nimetä edustaja EU:n sisällä
	Tietojenkäsittelytoimien dokumentointivelvollisuus

OSOITUSVELVOLLISUUDEN PERIAATE (”ACCOUNTABILITY”)

EU:n tietosuoja-asetus 24 artikla

Ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä yksilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit **rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että henkilötietojen käsittelyssä noudatetaan tätä asetusta.** Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa.

REKISTERINPITÄJÄN OSOITUSVELVOLLISUUS, mm.

Sanktiot!

OSOITUSVELVOLLISUUDEN PERIAATE JA RISKILÄHTÖISYYS

Asetuksen yleisluontoiset vaatimukset, esim. 32 art. (tiedon suojaaminen)

- Osa asetuksen vaatimuksista jää mm. tietoturvan luonteesta johtuen melko yleiselle tasolle, jättäen tulkinnanvaraa esimerkiksi tietoturvan tason määrittelemisessä
- Rekisterinpitäjän vastuulle jää viime kädessä päättää esim. tiedon suojaamiseen käytettävien kontrollien järeydestä ja arvioida niiden riittävyys
- Valittavien kontrollien sekä resurssien käytön tulee perustua riskiarvioon, käsiteltävien henkilötietojen luonteeseen ja teknologian tasoon
- Tilivelvollisuuden periaate täydentää asetuksen vaatimuksia, mitoittaa kontrolleja ja ohjaa toimimaan **riskilähtöisesti**
- Riskianalyysit välttämätön apuväline rajallisten resurssien tehokkaaseen kohdistamiseen
- Päätösten perusteet ja dokumentointi osa tilivelvollisesta toimintaa

Urheiluseuran jäsenrekisteri vs. potilastieto-rekisteri

TIETOSUOJAN IMPLEMENTOINTI

KRIITTISIÄ TEEMOJA TIETOSUOJAN KEHITTÄMISESSÄ

Riskien arviointi

Tietosuojan hallinnointi ja politiikkojen luonti / jalkautus

Rekisterinpidon perusedellytysten varmistaminen (oikeusperusteet, käsittelytarkoitukset)

Henkilötietojen ja tietovirtojen kartoittaminen; järjestelmien identifiointi

Prosessit ja tiedon elinkaaren hallinta

Sopimukset: Alihankinta ja henkilötietojen luovutukset

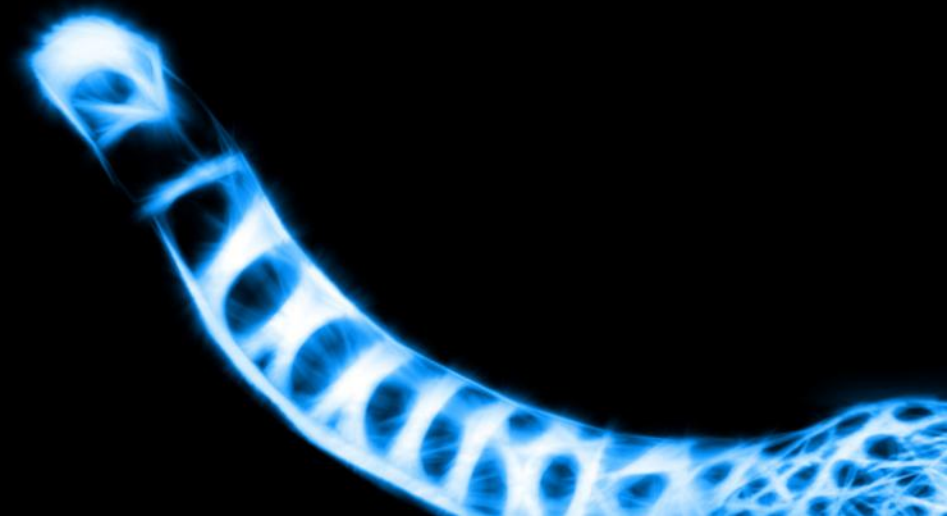
Rekisteröityjen oikeuksien toteuttaminen

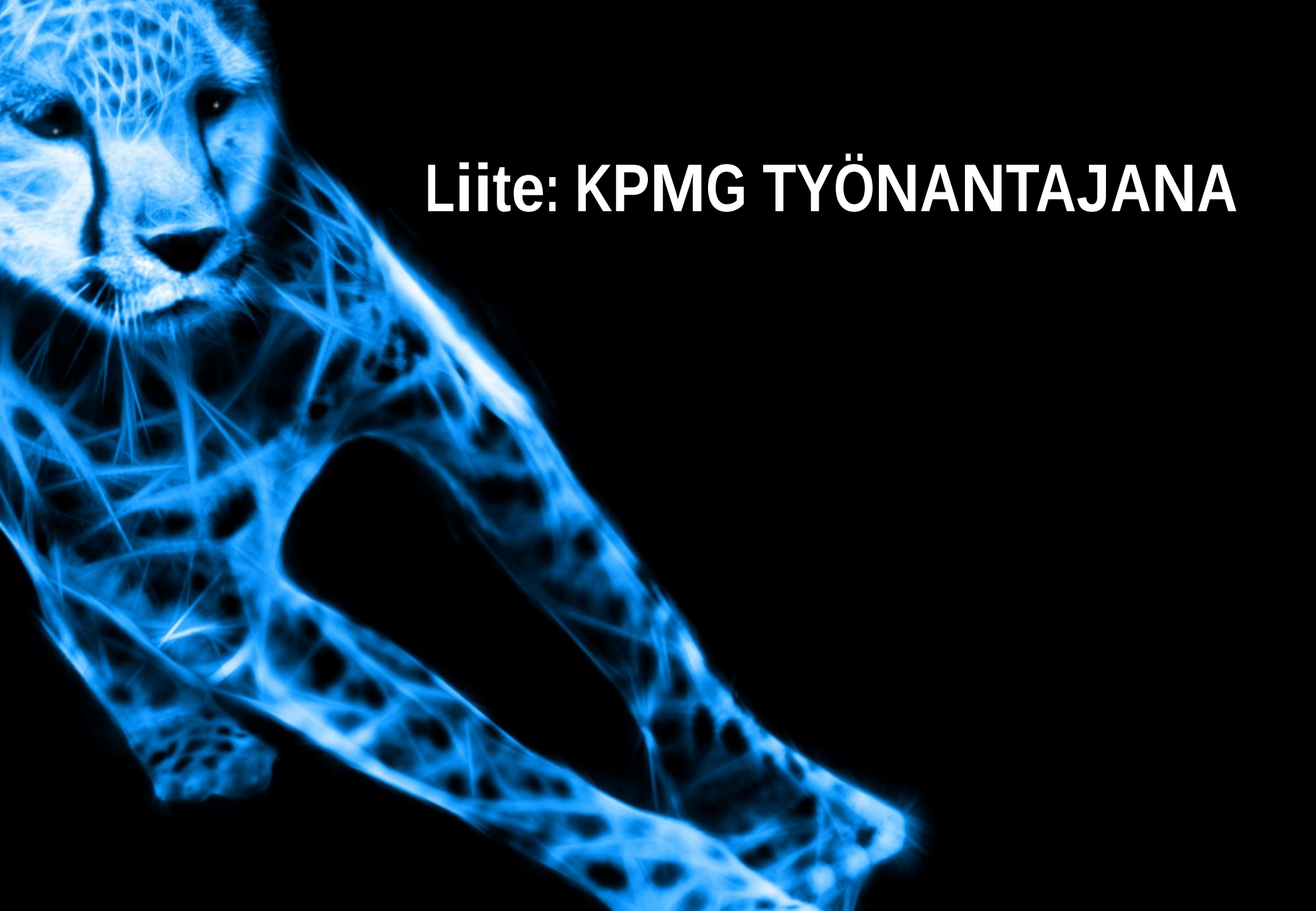
Tietosuoja-asetuksen vaatimukset ICT:lle ja sen hallinnoinnille

KPMG
cutting through complexity

KPMG Cyber Security
Mikko Viemerö
mikko.viemero@kpmg.fi
P. 020 760 3530

KPMG:n Kyberturvallisuusblogi: www.hackingthroughcomplexity.fi





Liite: KPMG TYÖNANTAJANA

KPMG Suomessa

Perustettu vuonna 1926, perustajina K.A. Widenius, Edvin Sederholm ja Juho Someri

Suomen vanhin tilintarkastustoimisto

Yksi johtavista asiantuntija-organisaatioista Suomessa

Liikevaihto
vuonna 2014:

98,7 milj. euroa

Yli **900** asiantuntijaa

23 paikkakunnalla

Liikevaihdon ja henkilöstön jakauma 2014