KPMG

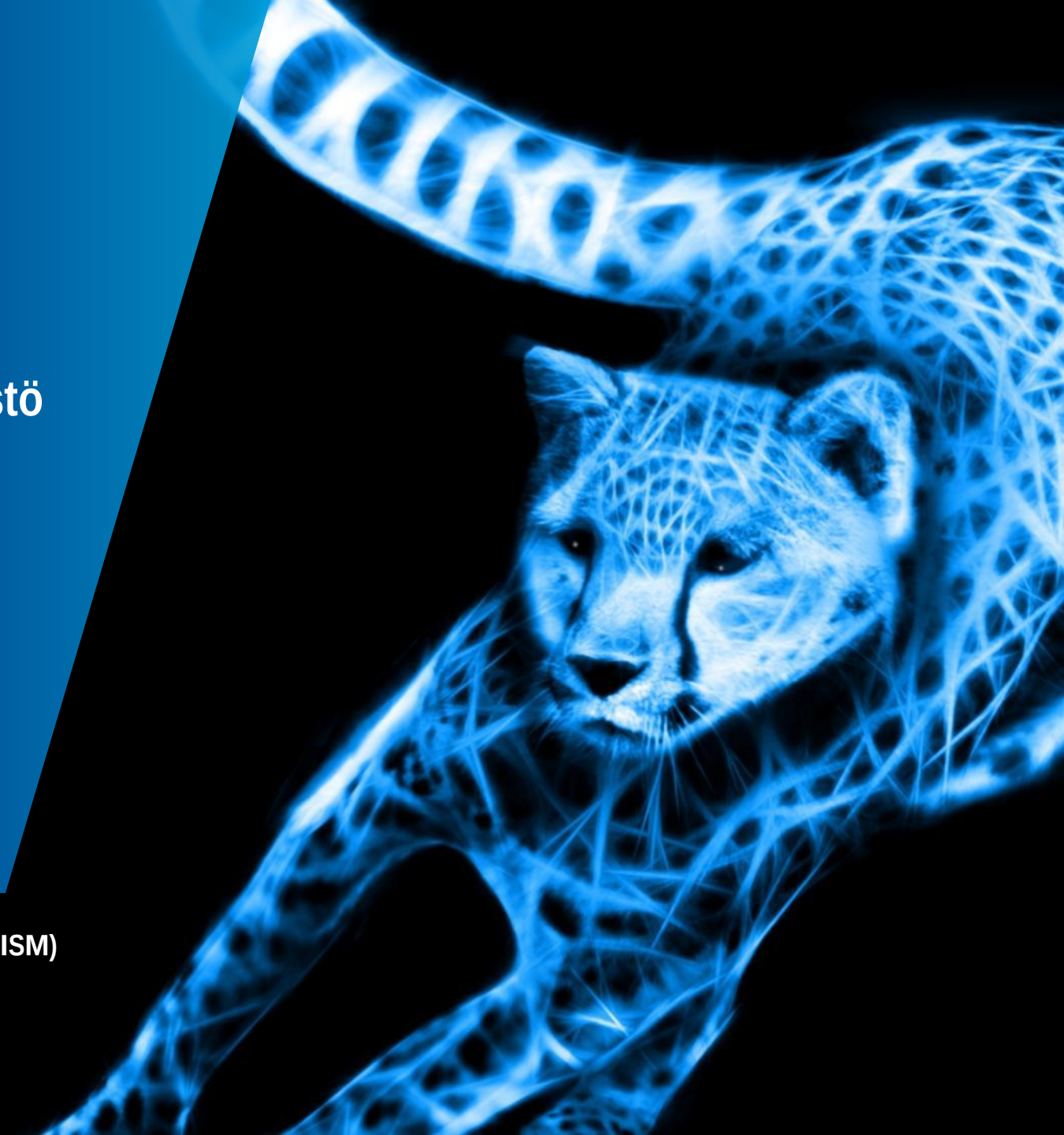
cutting through complexity

32E28100 - Markkinoiden juridinen toimintaympäristö

Luento 2 Case 2: Tietosuojalainsäädännön soveltaminen käytännön liiketoiminnassa

18.1.2016

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



TIETOSUOJAN LAINSÄÄDÄNTÖKENTTÄ

TIETOSUOJAN LAINSÄÄDÄNTÖ

Tietosuoja = Yksityisyyden suoja henkilötietojen käsittelyssä

- **Henkilötietodirektiivi (95/46/EY)**

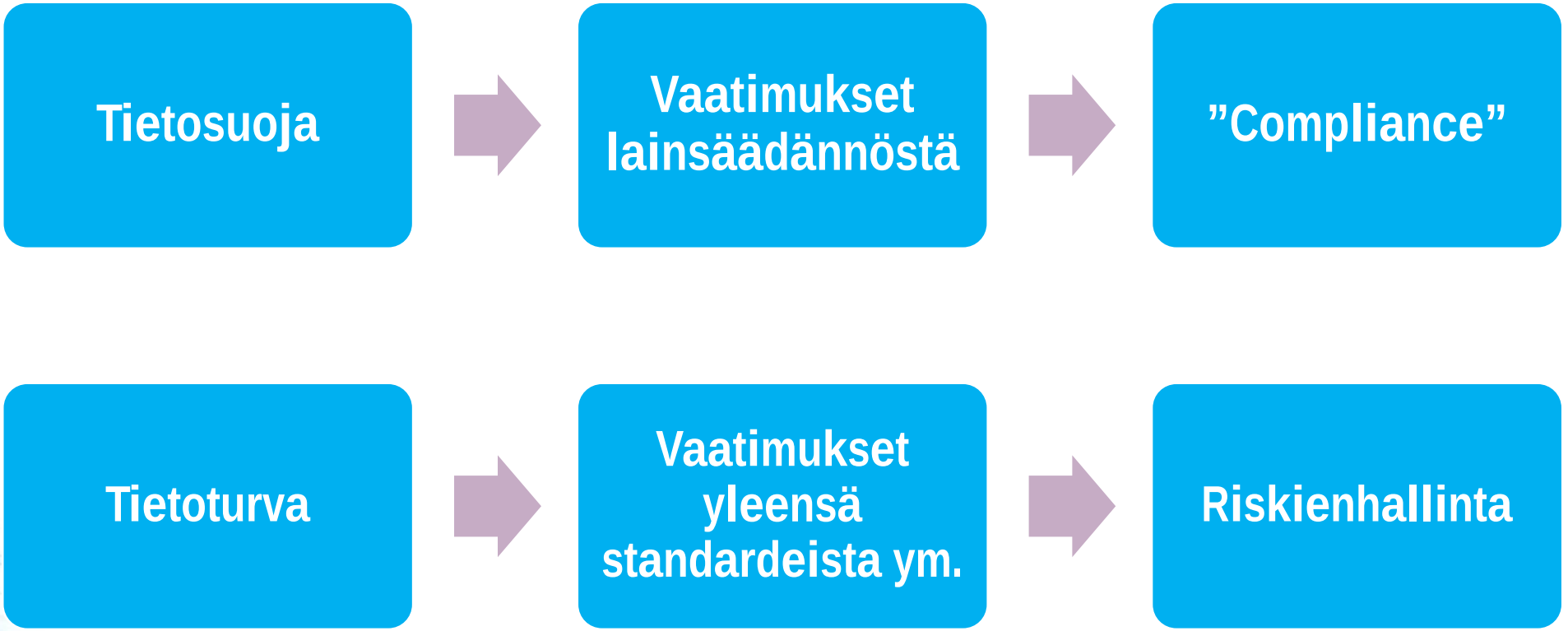
→ **Henkilötietolaki (523/1999)**

- **Sähköisen viestinnän tietosuojadirektiivi (2002/58/EY)**

→ **Tietoyhteiskuntakaari (917/2014)**

- **Laki yksityisyydensuojasta työelämässä (759/2004)**
- **Tulossa: EU:n yleinen tietosuoja-asetus (”GDPR”)**
- **Huomioitava: Julkisuuslaki (621/1999)**
- **Alakohtaista erityissääntelyä**
- **Tietoturvallisuutta säätelee mm. Tietoturva-asetus (681/2010)**

TIETOSUOJA vs. TIETOTURVA



TIETOSUOJAN PERUSTEET

HENKILÖTIETOLAKI

Määritelmiä

- **Henkilötiedolla** tarkoitetaan kaikenlaisia luonnollista henkilöä (→ **rekisteröity**) taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi;
  - → 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 henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä;

- **Henkilörekisteri**llä tarkoitetaan käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa (nk. **loogisen rekisterin käsite**), jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta;

- **Rekisterinpitäjä**llä tarkoitetaan yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty (vrt. **henkilötietojen käsittelijä**).

HENKILÖTIETOLAKI

Henkilötietojen käsittelyn perusteet, mm.

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

Henkilötietojen käsittelyn periaatteet

- Huolellisuusvelvoite
- Suunnitteluvelvoite
- Käyttötarkoitussidonnaisuus
- Tarpeellisuusvaatimus
- Virheettömyysvaatimus

HENKILÖTIETOLAKI

Rekisteröidyn oikeudet

- Tiedonsaantioikeus (→ rekisteriseloste / tietosuojaseloste)
- Tarkastusoikeus
- Oikeus saada tieto korjatuksi
- Kielto-oikeus (suoramarkkinointiin)

HENKILÖTIETOJEN KÄSITTELY JA VALVONTA

Salassapito

- ”Need to know”-periaate: Luottamuksellisia tietoja saa käsitellä vain ne, joiden työtehtäviin käsittely kuuluu – tällöinkin vain perustellusta tarpeesta
- Arkaluonteiset tiedot ja henkilötunnus vaativat erityistä suojaa (rajatumpi käsittely, erillään pito, tuhoaminen, erityisalat)
- Käsittely rajattava minimiin
- Käsittelijäpiirillä vaitiolovelvollisuus
- Käsittelijäpiiri rajataan mm. käyttöoikeuksien avulla

Käyttöoikeudet

- Käyttäjätunnukset ja salasanat ovat aina henkilökohtaisia
- Salasanojen oltava riittävän vahvoja
- Pidettävä ajan tasalla

Lokitus

- Käyttäjien toimia valvotaan kriittisissä järjestelmissä nk. lokituksen avulla
- Lokit keräävät järjestelmistä tietoa, esim. kuka on käsitellyt mitä henkilötietoaineistoa ja milloin
- Mahdollistavat tietosuojaloukkausten jälkikäteisen selvittelyn

TIETOSUOJA – VASTUUNJAKO, esim.

	Suunnittelu	Toteutus	Valvonta
Johto	Business case Tietosuojastrategia Tietosuojapolitiikka	Budjetointi Vastuutus	Raporttien vaatiminen Kurinpitotoimista päättäminen
Riskienhallinta / compliance / tietosuojavastaava	Riskianalyysit Auditoinnit Nykytilan arviointi Standardien ja ohjeistusten tuottaminen Kontrolliympäristö ja valvonta Henkilöstön koulutus	Riskianalyysit Auditoinnit Nykytilan arviointi Standardien ja ohjeistusten tuottaminen Henkilöstön koulutus	Kokonaisuuden mittaaminen ja raportointi Kontrollien toteuttamisen valvonta Projektien seuranta
Liiketoiminta-yksiköt / tiedon omistaja	Vaatimusanalyysi ja vaatimusten esittäminen Prosessien kuvaaminen Rutiinien kuvaaminen Käyttövaltuushallinta	Tietosuojakontrollien ja valvonnan vieminen osaksi työrutiineja Tiedon luokittelu Poikkeamien havainnointi ja eskalointi Käyttövaltuushallinta	Asiakaspalaute Käytännön palaute toimivuudesta Politiikkojen noudattamisen valvonta

TIETOSUOJA – VASTUUNJAKO, esim.

	Suunnittelu	Toteutus	Valvonta
Tietoturva	Tietoturvaratkaisut tukemaan tietosuojaa	Tekniset suojausratkaisut Päivitystoimet Tietojärjestelmien valvonta	Suojausten toimivuuden testaus
Tietohallinto	Tietojärjestelmien käyttösäännöt ja perehdytys	Tietojärjestelmien kehitys	Teknisen valvonnan toteutus
HR	Henkilöstön kartoittaminen Rekrytointi	Henkilöstön tietoisuusohjelma	Koulutuksen suorittamisen seuraaminen
Henkilötietojen käsittelijä		Henkilötietojen lainmukainen käsittely Politiikkojen ja ohjeistusten noudattaminen Vaitiolovelvollisuus	Tietosuoja- ja tietoturvapoikkeaminen raportointi

EU:N YLEINEN TIETOSUOJA-ASETUS

EU:N YLEINEN TIETOSUOJA-ASETUS

- EU:n yleinen tietosuoja-asetus korvaa henkilötietolain yleiset vaatimukset
- Asetuksen sisältö hyväksyttiin 15.12.2015
- Kahden vuoden siirtymäaika → velvoittava 2018
- Toistaiseksi käytössä konsolidoitu luonnos
- Vaatimuksia tehostetaan tuntuvilla sanktioilla (jopa 100 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

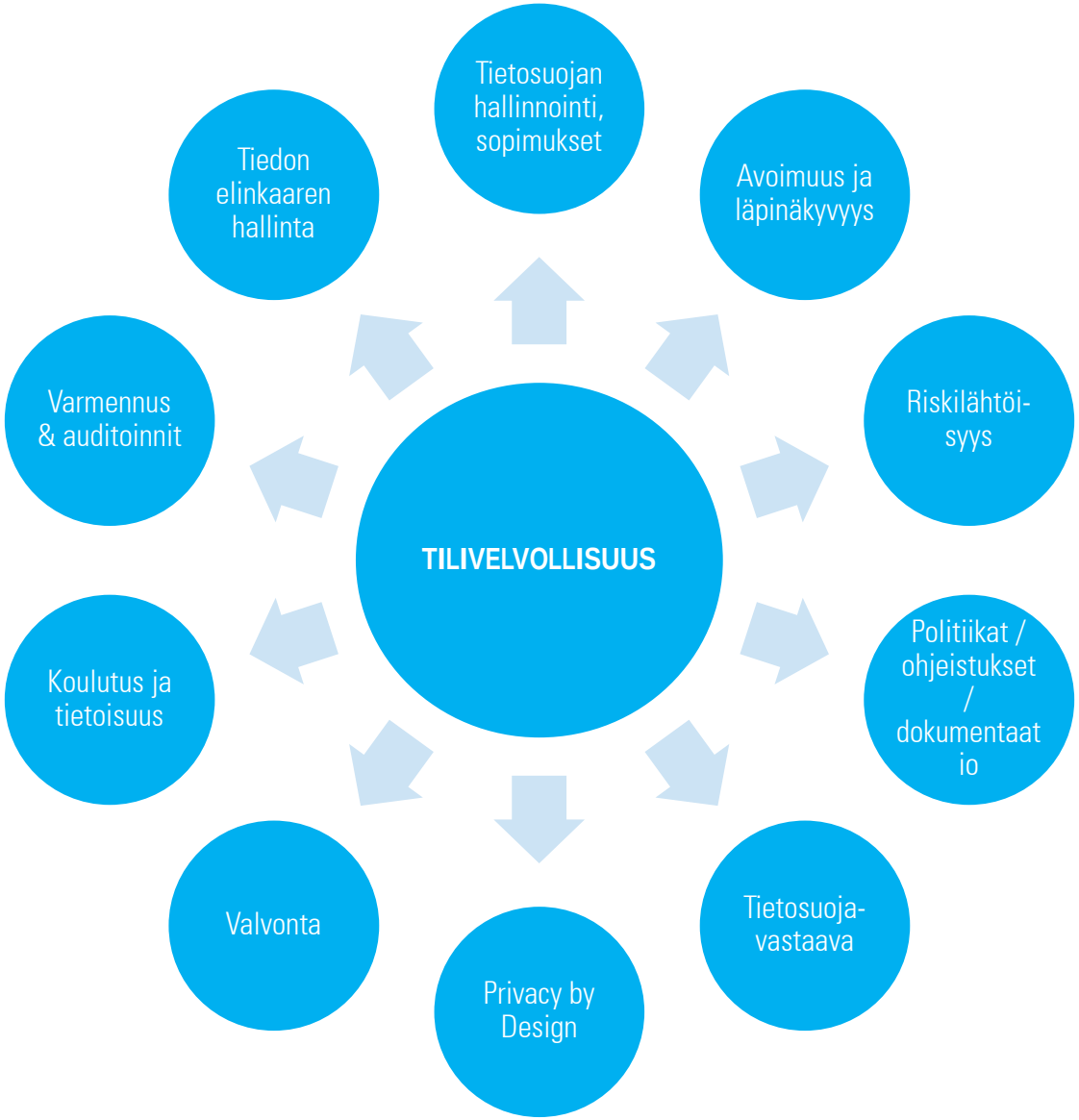
Uudet säännökset, mm.	Tiukennukset entisiin vaatimuksiin, mm.
Tilivelvollisuuden periaate	Säännösten sovellettavuus (henkilötiedon määritelmä/anonyymidata/pseudonyymidata)
Privacy „by Design“ ja „by Default“	Vaatimukset tehokkaalle suostumukselle
Tietosuojan vaikutustenarvioinnit	Merkittävät sanktiot asetuksen vaatimusten vastaisista toimista
Tietovuotoilmoitus pakolliseksi	Kv. tiedonsiirrot
Tietosuojavastaava	Rekisterinpitäjän ja tietojenkäsittelijän välinen suhde (→ sopimusten uudelleenarviointi)
Yhden luukun periaate (viranomaisten yhteistyö)	Henkilötietojen käsittelyn perusteet
“Right to erasure”	Tietojenkäsittelytoimien dokumentointivelvollisuus
Henkilötietojen siirrettävyys	Korotetut toimeenpanovaltuudet viranomaisille
	EU:n ulkopuolisten rekisterinpitäjien velvollisuus nimetä edustaja EU:n sisällä

TILIVELVOLLISUUDEN PERIAATE (”ACCOUNTABILITY”)

EU:n tietosuoja-asetus 22 artikla (konsolidoitu luonnos):

”…the controller shall implement appropriate **technical and organisational measures to ensure and be able to demonstrate** that the processing of personal data is performed in compliance with this Regulation. These measures shall be reviewed and updated where necessary.”

REKISTERINPITÄJÄN TILIVELVOLLISUUS, mm.



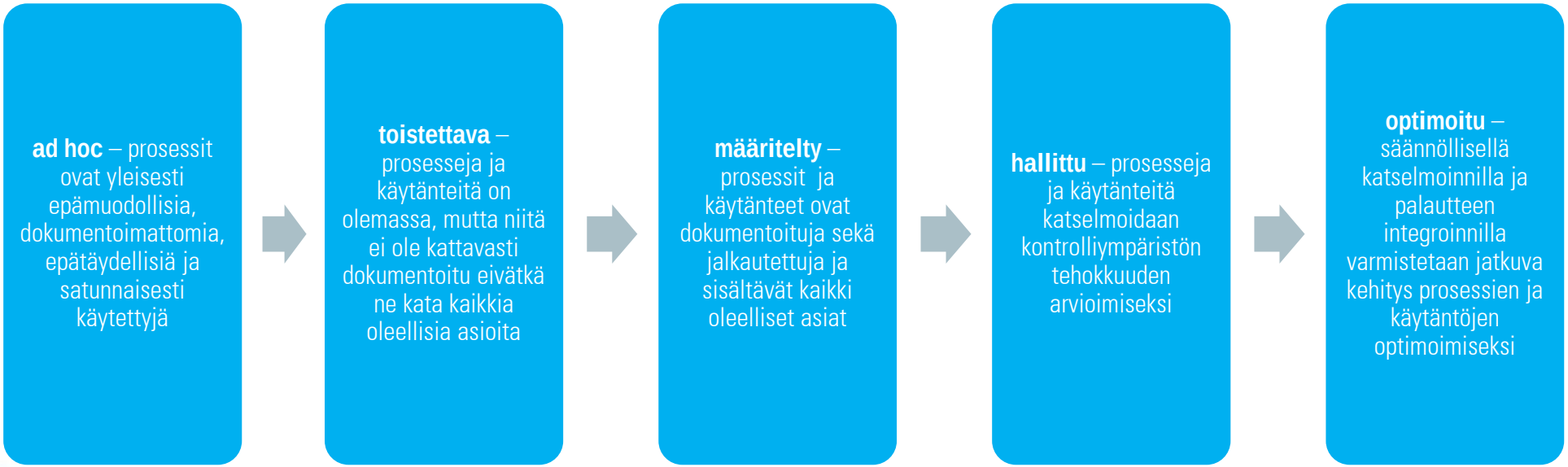
Sanktiot!

TIETOSUOJA-ASETUS: RISK-BASED APPROACH!

- Riskilähtöisyys: Valittujen riskienhallintatoimenpiteiden, kontrollien ja resurssien käytön tulee perustua riskiarvioon, käsiteltävien henkilötietojen luonteeseen, teknologian tasoon sekä organisaation riskinottohalukkuuteen
- Riskianalyysin tarkoitus on kartoittaa riskinäkökulmasta mm.
  - Liiketoimintaympäristö ja sidosryhmät
  - Liiketoiminnan substanssi
  - Organisaation resurssit
  - Henkilötietojen käsittelyn prosessit ja käytänteet
  - Teknologia
  - Alihankintasopimukset
  - Lainsäädännön vaatimusten noudattaminen
- Riskityypit, mm.:
  - Siirretyt riskit
  - Mitigoidut riskit
  - Jäännösriskit
  - Hyväksytyt riskit
  - Vältetyt riskit

TIETOSUOJAN IMPLEMENTOINTI

KYPSYYSTASOT, esim.



TIETOSUOJA-ASETUS JA KEHITYSTYÖ

- Suomalaisten rekisterinpitäjien tietosuojan kypsyystaso ei keskimäärin vielä ole riittävällä tasolla (vrt. KPMG:n kyselytutkimus 2014)

1. Nykytilan arviointi

- Järjestelmien, palvelujen, tietovirtojen ja henkilörekisterien identifiointi
- Nykyisten prosessien, käytänteiden, kontrollien ja johtamisen läpikäynti haastattelujen ja dokumentaation avulla
- Sääntelykentän kartoittaminen ja juridiset erityiskysymykset

→ Arvio tietosuojatoimintojen kypsyystasosta

2. Gap-analyysi / riskianalyysi

- Auditointi (nykyisiä ja) tulevia tietosuojavaatimuksia vastaan

→ Puutteet nykyisessä toiminnassa

- Riskianalyysi havaituista puutteista
- Riskiluokitus ja korjaustarpeen priorisointi

3. Kehitystoimenpiteet

- Kehityssuunnitelman laatiminen henkilötietojen käsittelyn prosessien kehittämiseksi ja vaatimustenmukaisuuden saavuttamiseksi
- Avustaminen kehitystoimenpiteiden toteutuksessa
- Useampi kehityssykli
- Todentaminen (huom! riippumattomuus)

TIETOSUOJAVAATIMUSTEN IMPLEMENTOINTI

Kontrollitavoitteet	Kontrolliviite	Kontrollikuvaus	Tarvittavat dokumentit	Lakiviittaus / nykyinen lainsäädäntö
Tietosuojan hallinnointi				
Kontrollit varmistavat, että tietosuojan hallinnointi on suunnitelmallista ja johdonmukaista. Kontrollit varmistavat, että tietoturvaan ja tietosuojaan liittyvät politiikat on hyväksytty johdon toimesta ja kommunikoitu henkilöstölle. Kontrollit varmistavat, että henkilöstöllä on riittävä tietosuojaosaaminen. Kontrollit varmistavat, että tietosuojatyöhön osallistuvien vastuut on määritelty ja kommunikoitu.	Tietoturvapolitiikka	1.2 Organisaatiolle on laadittu johdon hyväksymä tietoturvapolitiikka. Tietoturvapolitiikka on yleisesti saatavilla ja se pidetään ajantasaisena.	Ajantasainen, johdon hyväksymä tietoturvapolitiikka, joka on helposti henkilöstön saatavilla	Vahti 2/2010 Tietoturvallisuuden hallinta 1.1.1.3.
	Tietosuojapolitiikka	1.3 Organisaatiolle on laadittu johdon hyväksymä tietosuojapolitiikka. Tietosuojapolitiikka on yleisesti saatavilla ja se pidetään ajantasaisena.	Ajantasainen, johdon hyväksymä tietosuojapolitiikka, joka on helposti henkilöstön saatavilla, sis. mm.: - tietosuojatyön tavoitteet - tietosuojatyön vastuut ja tehtävät - henkilötietojen käsittelyn määritelmät ja periaatteet - mitä tietoja käsitellään ja mihin tarkoituksiin - henkilöstön vaitiolovelvollisuus - toimintaohjeet tietosuojapoikkeamien varalle	HetiL 5 § Huolellisuusvelvoite HetiL 6 § Henkilötietojen käsittelyn suunnittelu HetiL 32 § Tietojen suojaaminen
	Tietoturva- ja tietosuojaohjeistus	1.4 Henkilöille, joiden työtehtäviin kuuluu henkilötietojen käsittely, on laadittu sisäinen henkilötietojen käsittelyn ohjeistus.	Henkilötietojen käsittelyn ohjeistus	HetiL 5 § Huolellisuusvelvoite HetiL 6 § Henkilötietojen käsittelyn suunnittelu HetiL 32 § Tietojen suojaaminen
	Rekisteriseloste	1.5 Kaikista henkilörekistereistä on laadittu HetiL 10 § mukainen rekisteriseloste	Rekisteriselosteet	HetiL 10 § Rekisteriseloste
	Tietosuojaperehdytys	1.6 Henkilöille, joiden työtehtäviin kuuluu henkilötietojen käsittely, järjestetään tietosuojaperehdytys.	Perehdytysmateriaali	HetiL 5 § Huolellisuusvelvoite HetiL 6 § Henkilötietojen käsittelyn suunnittelu HetiL 32 § Tietojen suojaaminen
	Säännöllinen tietosuojakoulutus	1.7 Henkilöille, joiden työtehtäviin kuuluu henkilötietojen käsittely, järjestetään säännöllistä tietosuojakoulutusta. Koulutusten suorittamista seurataan.	Koulutusmateriaali	HetiL 5 § Huolellisuusvelvoite HetiL 6 § Henkilötietojen käsittelyn suunnittelu HetiL 32 § Tietojen suojaaminen

TIETOSUOJAVAATIMUSTEN IMPLEMENTOINTI – harjoitus

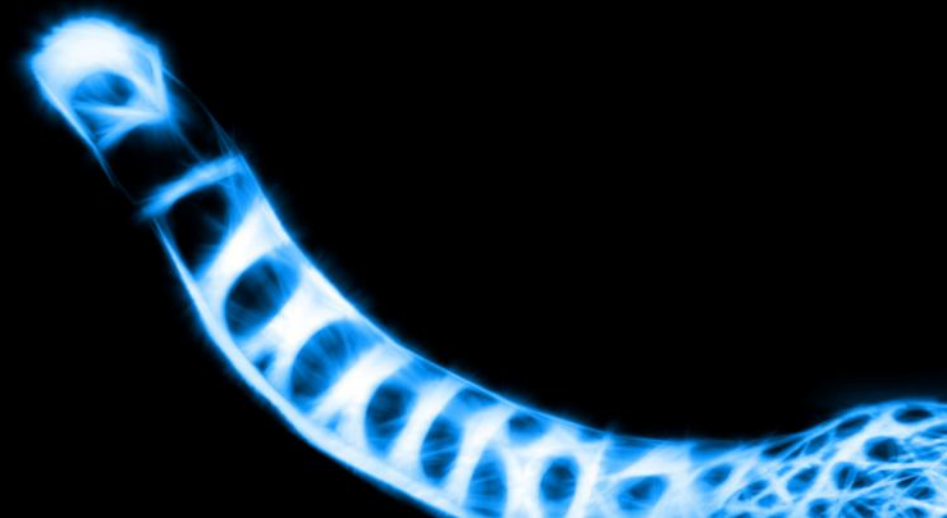
Tietosuojavastaava avustaa organisaatiota	Tietosuojavastaava on organisaation erityisasiantuntija
■ Hoitamaan lakisääteiset velvoitteet ■ Henkilötietojen käsittelyn suunnittelussa ja dokumentoinnissa ■ Riskiarviointien tekemisessä ■ Arvioimaan tietosuojan ja tietoturvan tilaa ja kehitystarpeita mahdollisimman riippumattomasti	■ Tuki sekä johdolle että henkilöstölle ■ Mahdollisimman riippumaton asema ■ Raportointi suoraan johdolle ■ Tavoitteena hyvä henkilötietojen käsittelytapa sekä korkea tietosuojan taso

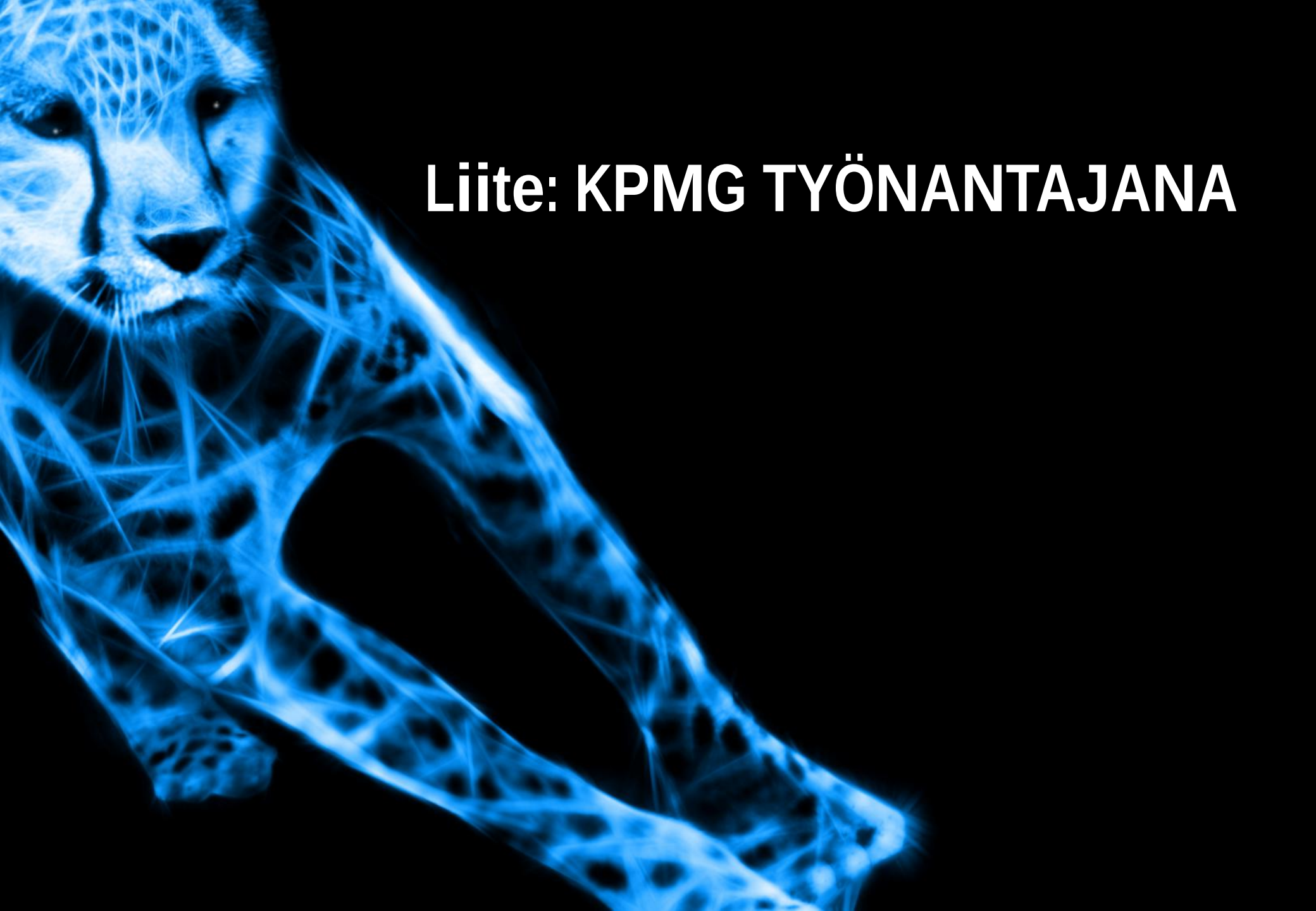
Kysymys: Mitä toimenpiteitä organisaation johdon tulee suorittaa, jotta vaatimus tietosuojavastaavan nimittämisestä ja toimintaedellytysten luomisesta pystytään täyttämään tilivelvollisuuden periaatteen mukaisesti?

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 **850** asiantuntijaa

22 paikkakunnalla

Liikevaihdon ja henkilöstön jakauma 2014