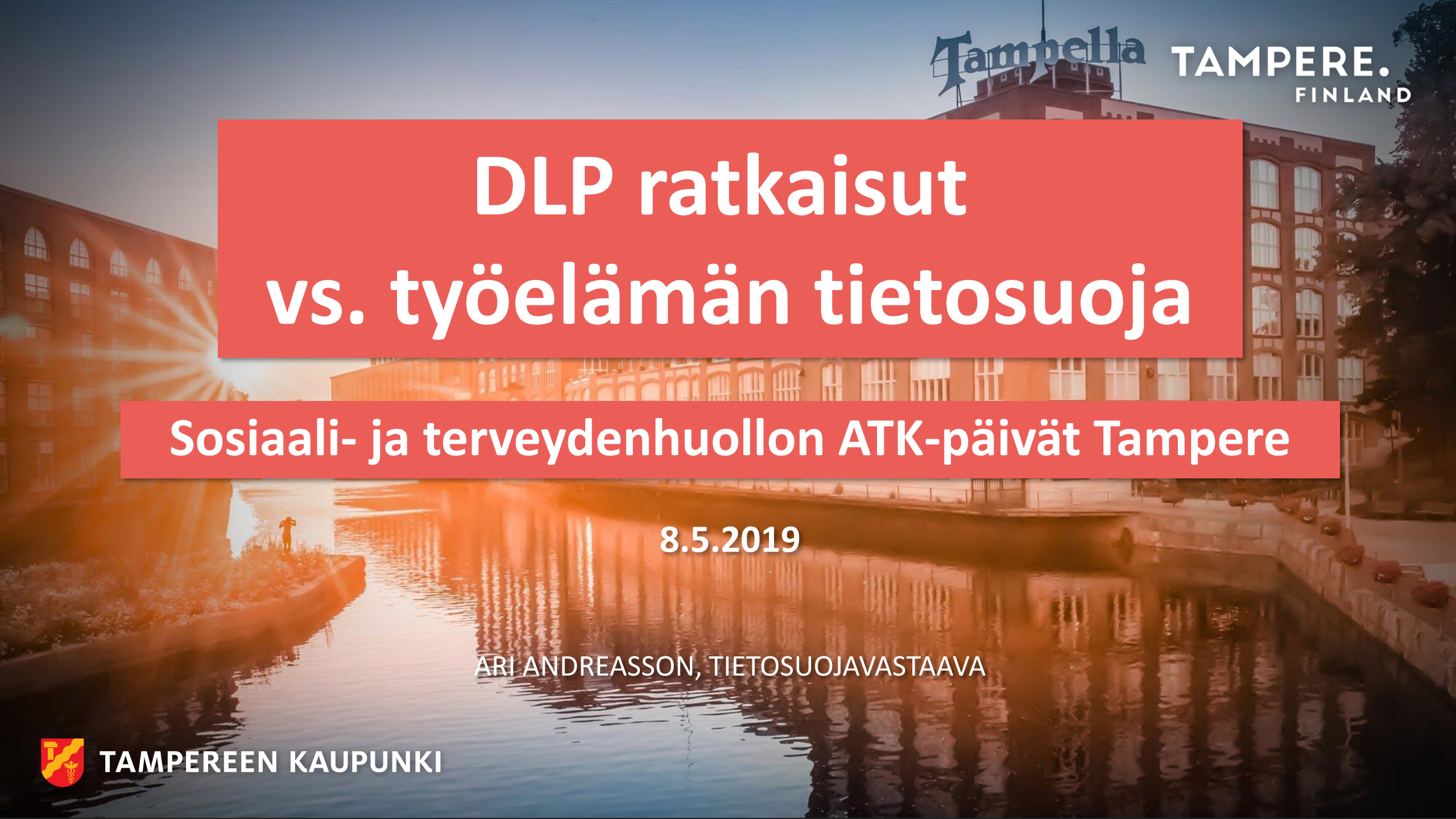


DLP ratkaisut vs. työelämän tietosuoja

Sosiaali- ja terveydenhuollon ATK-päivät Tampere

8.5.2019

ARI ANDREASSON, TIETOSUOJAVASTAAVA

TAMPEREEN KAUPUNKI

TIETOSUOJAVASTAAVA ARI ANDREASSON

TAMPERE. FINLAND

Nykyisiä rooleja:

- Tampereen kaupungin
  - työpaikkana: Tietohallintoyksikön digiturvallisuus ja riskienhallinta-tiimi
  - peruskunnan tietosuojavastaava (kunta liikelaitoksineen)
  - tietoturva- ja tietosuojaryhmän sihteeri
  - Pegasos-kehittämis- ja ylläpitoryhmän jäsen

- Tampereen kaupungin ja seudun (yhteensä 9 kuntaa)
  - Tampereen seudun tietoturvaryhmän jäsen

- Kansallisia rooleja
  - Kuntaliiton tietosuojavastaavien verkoston työvaliokunnan puheenjohtaja
  - Pirkanmaan tietosuojavastaavien verkoston jäsen
  - Terveydenhuollon tietosuojan yhteistyöryhmän jäsen

- Sivutoiminen tietokirjailija
  - uusin kirja ilmestyi 1.3.2019: Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus

DLP:n (data loss prevention, automaattiset tietosuojakeinot) etuja

- Oikein toteutettuna estää tietovuotoja ja parantaa tietoturvaa (sekä sen toteutumisen seurantaa)
- Varmistaa miten esim. erityisiin henkilötietoryhmiin tai liikesalaisuuksiin liittyviä tietoja voi liikutella tai mihin niitä ylipäätänsä saa edes tallentaa organisaatiossa
- Ehkäisee tiedon katoamista
- Auttaa työntekijöitä ymmärtämään tietojen käsittelyn ohjeet

Lainsäädäntöä, jota on syytä pohtia

- **EU:n yleinen tietosuoja-asetus (32 artikla)**
  - 1. Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet
  - 2. Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi
- **Laki yksityisyyden suojasta työelämässä**
  - mm. yhteistoiminta teknisin menetelmin toteutetun valvonnan ja tietoverkon käytön järjestämisessä (jos YT-lainsäädäntöä ei sovelleta, niin tilaisuus tulla kuulluksi)
- **Laki sähköisen viestinnän palveluista**
  - mm. välitystietojen käsittely, tiedonantovelvollisuudet, yhteisötilaajan erityissääntely ennakkoilmoitukset jne.

Mitä DLP-ratkaisut tekevät?

- DLP voi haluttaessa estää tiedon, kuten henkilötunnuksen, pankkitilin tai passin numeron tai muun vastaavan lähettämisen sähköpostilla tai tallentamisen tiedostoon tai pyytää käyttäjältä vahvistuksen toimenpiteeseen tai neuvoa käyttäjää toimimaan organisaation toimintapolitiikan mukaisesti

- DLP-tuotteet voivat automaattisesti luokitella viestejä ja tiedostoja tietosisällön mukaan, antaa käyttäjälle mahdollisuuden luokitella niitä ja automaattisesti salata tiedostot ja viestit koko niiden elinkaaren ajaksi

- Tuotteissa on usein myös erilaisia erikseen halutessa käynnistettäviä skannaustoimintoja, joilla voi etsiä haluttua dataa (esim. henkilötunnuksia). Näitä käyttäen organisaation kyvykkyys paranee arvioida sitä mitä dataa on tallennettu

Tietosuojakysymyksiä

- Miten organisaatio varmistaa työntekijän ja rekisteröidyn/asiakkaan oikeuksien yhteensovittamisen? Varsinkin kun työtekijä on usein myös rekisteröidyn roolissa esim. organisaation loki-, HR- ja taloushallinnon rekistereissä

- Tekninen valvonta ja automaattinen puuttuminen työntekijän toimiin: Riittääkö tiedottaminen ja YT-käsittely vai pitääkö olla työntekijän suostumus?
  - Käsitelläänkö sähköisiä viestintävälineitä eri tavoin lainsäädännön näkökulmasta kuin esim. verkkotyötilojen ja verkkolevyjen suojaamista? Sähköpostin tunnistetiedot ovat eri asia kuin varsinaisen viestin sisältö
  - Huomioitavaa on myös se, että organisaation tietoihin saa käyttöoikeuksia muutkin kuin vain työntekijät
  - Mihin DLP:n lokeja kerätään? Onko käytössä esim. SIEM ja mihin henkilörekisteriin kerätyt tiedot kuuluvat?

- **Joka tapauksessa ratkaisuja käyttöönotettaessa on syytä tehdä DPIA-arvio sekä pohtia miten asia informoidaan työsopimuksen teon yhteydessä ja esim. tietojen ja tietojärjestelmien käyttö- ja salassapitositoumuksissa sekä muissa politiikoissa ja ohjeissa, jotka organisaatiota ohjaavat.**

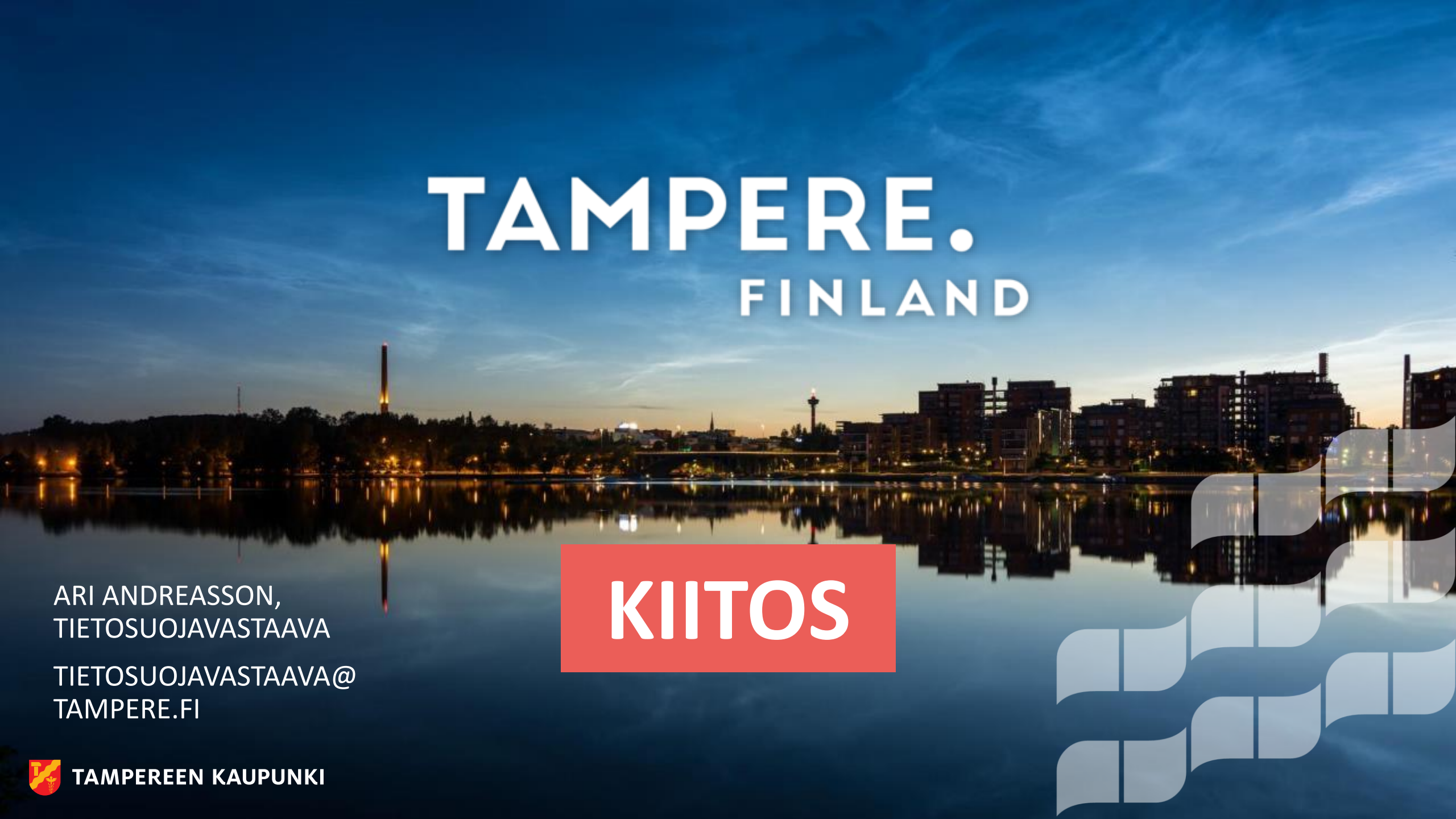
Loppusanat

Kyberhäiriöselvityksestä lainattua:

”DLP-ratkaisut

Yrityksiltä kysyttiin haastatteluissa Data Loss Prevention-ratkaisuista, joita on melko laajasti saatavilla. Palveluntarjoajayritykset pitivät Suomen markkinaa jossakin määrin epäkypsänä ja yrityksiä tarpeettoman varovaisina DLP-ratkaisujen käytössä. Näiden ratkaisujen sallittuus lainsäädännön näkökulmasta riippuu pitkälti niiden toteuttamistavasta. Tarve ratkaisuille kasvaa samalla kun pilvipalvelujen tarjonta lisääntyy. ”

- **Itse toivon kansallista ohjausta/mallia!**



KIITOS

ARI ANDREASSON,
TIETOSUOJAVASTAAVA

TIETOSUOJAVASTAAVA@
TAMPERE.FI

TAMPEREEN KAUPUNKI