EU:N TIETOSUOJA-ASETUS JA SEN VAIKUTUS REKISTERÖITYNEELLE

Tietoturvallisuusasiantuntija Pauliina Hirvonen
Citrus Solutions Oy
07.03.2017

CITRUS TYÖNANTAJANA

- 2002 ICT-konsultointi, -arkkitehtuuri ja -sovelluskehitys,
  2014 alkaen yhä enemmän omia projekteja
  2016 alkaen yhä enemmän omia palveluita, toiminnan digitalisointiin, riskienhallintaan, tietosuojan automatisointiin
- Yli 50 työntekijää
- Toimistot Helsingissä ja Turussa
- Toimintaa myös Tampereella, Jyväskylässä, Oulussa, Saigonissa
- Kumppanit ja yhteistyöverkostot

AGENDA

- Peruskäsitteet
- Taustoitus
  - Toimintaympäristön muutos
- Rekisteröidyn oikeudet
- Tietosuoja-asetuksen vaikutukset
- Yhteenveto

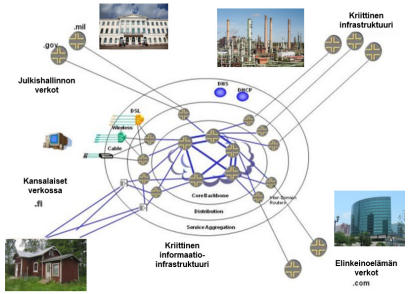
TAVOITE

- Tietosuoja-asetuksen merkityksen ja vaikutusten ymmärtäminen rekisteröityneen kannalta

PERUSKÄSITTEET

- Henkilötiedot
- Henkilötietojen käsittely
- Tilivelvollisuus – tilintekokykyisyys
- Ilmoitusvelvollisuus
- Rekisteröityjen (henkilötietojen käsittelyn kohteena olevien) oikeudet
  - *omia henkilötietoja koskeva tiedonsaantioikeus*
  - *oikeus saada tiedot oikaistua*
  - *oikeus tulla unohdetuksi*
  - *oikeus tietojen poistamiseen ja tietojenkäsittelyn vastustamiseen*
- Lasten henkilötiedot

MIKÄ ON MUUTTUNUT

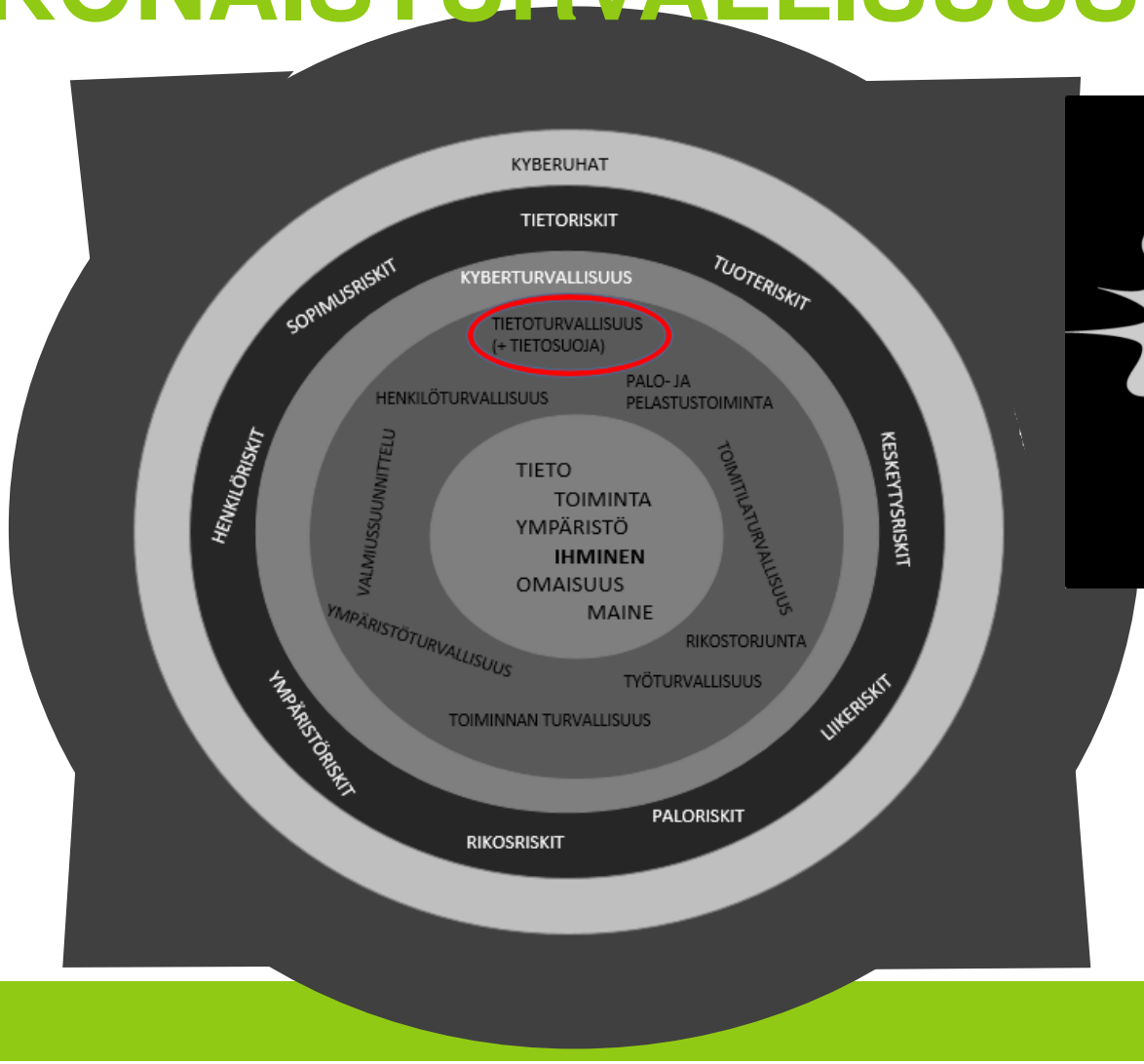


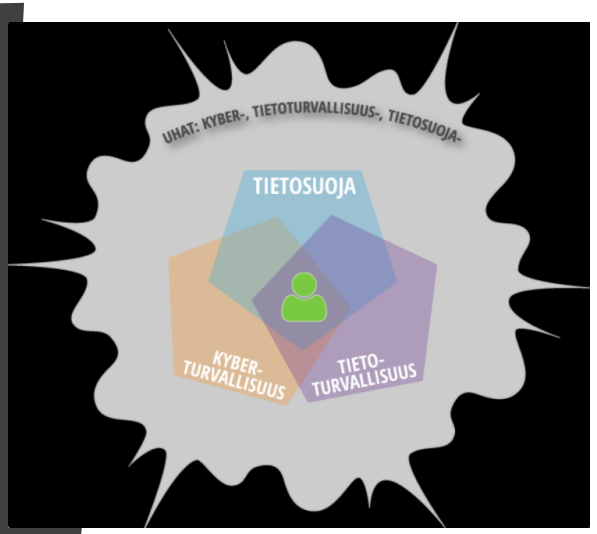
- Aika: toiminnan viive pienentynyt
- Data: syntyy nyt joka toinen päivä yhtä paljon kuin ihmiskunnan alkuajoista vuoteen 2003 mennessä
- Verkko: Kriittinen infrastruktuuri, informaatioinfrastruktuuri ja SCADA. Fyysisestä maailmasta vaikutus digitaaliseen maailmaan ja toisinpäin.
- Äly: verkostoituneiden laitteiden määrä kymmeniä miljardeja. Älyteknologia, IoE, IoT etc.

→ Luottamus, omaisuuden ja yksityisyyden hallinta

- GDPR vs. verkostoitunut maailma

KOKONAISTURVALLISUUS





MUOKATTU,
ALKUPERÄINEN
LÄHDE: SFS, 2012

REKISTERÖIDYN OIKEUDET –PERIAATTEET

- Tietosuoja on ihmisten yksityiselämän suojaamista, ja siihen kuuluu kunkin oikeus henkilötietoihinsa.
- Rekisteröityjen oikeuksien perusperiaatteena on henkilötietojen suojan takaaminen valtuudettomalta tai henkilöä vahingoittavalta tietojen käytöltä.
- Tietosuoja-asetuksen määrittelemät rekisteröityjen oikeudet ovat osin vastaavia kuin aiemmin henkilötietolaissakin määritellyt oikeudet.

REKISTERÖIDYN OIKEUDET

- **Oikeus saada pääsy omiin tietoihinsa:** rekisterinpitäjän velvollisuus toimittaa jäljennös sähköisesti kaikista käsiteltävistä rekisteröidyn henkilötiedoista on syytä ottaa huomioon henkilötietoja käsittelevien järjestelmien ja käsittelyä hoitavien kolmansien osapuolten näkökulmasta.
- **Oikeus tietojen oikaisemiseen**: oikeus vaatia, että rekisterinpitäjä oikaisee rekisteröityä koskevat virheelliset henkilötiedot tai täydentää puutteellisia henkilötietoja.
- **Oikeus poistaa tiedot** (”oikeus tulla unohdetuksi”): rekisteröidyn oikeus pyytää rekisterinpitäjää poistamaan esim. häntä koskevat vanhentuneet henkilötiedot tai oikeus peruuttaa suostumuksensa, johon käsittely on perustunut.
- **Oikeus siirtää tiedot järjestelmästä toiseen**: rekisteröidyllä oikeus saada häntä koskevat henkilötiedot yleisesti käytössä olevassa siirtomuodossa ja toimittaa ne toiselle rekisterinpitäjälle.
- **Oikeus vastustaa käsittelyä, automaattista päätöksentekoa ja profilointia**: oikeus henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä.
- **Oikeus saada ilmoitus henkilötietojen tietoturvaloukkauksesta**: oikeus astuu voimaan, jos loukkaus todennäköisesti aiheuttaa suuren riskin yksilön oikeuksille ja vapauksille, esim. identiteetinvarkauksien, maksuvälinepetosten tai muun rikollisen toiminnan muodossa.

ILMOITUSVELVOLLISUUS

Rekisteröidylle

- Ilmoitusvelvollisuus koskee henkilötietojen tietoturvaloukkaustilanteita, joissa henkilötietojen luottamuksellisuus on vaarantunut**: rekisteröidyillä oikeus saada ilmoitus, jos hänen henkilötietonsa ovat vuotaneet ulkopuolisille luvattomasti.**
- Ilmoitus tehtävä, jos tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin rekisteröityjen oikeuksille ja vapauksille (esim. identiteetinvarkaus, maksuvälinepetos tai muu rikollinen toiminta).

Viranomaiselle

- Rekisterinpitäjän ilmoitus valvontaviranomaiselle henkilötietojen tietoturvaloukkauksesta 72 tunnin kuluessa siitä, kun loukkaus on havaittu.
- Jos ilmoitusta valvontaviranomaiselle ei ole mahdollista tehdä 72 tunnin kuluessa tietoturvaloukkauksen ilmitulosta, on rekisterinpitäjän tässä ajassa liitettävä ilmoitukseensa perusteltu selvitys viivästyksen syistä valvontaviranomaiselle.
- Ilmoitusvelvollisuus on huomioitava organisaation kriisi- ja häiriötilanneviestinnässä niin prosessin kuin ohjeistuksen osalta.

REKISTERÖIDYN OIKEUDET HENKILÖTIETOJA SISÄLTÄVISSÄ JÄRJESTELMISSÄ

- Oikeus saada läpinäkyvää informaatiota henkilötietojen käsittelystä
- Rekisteröidyn oikeus saada pääsy tietoihin
- Oikeus tietojen oikaisemiseen ja oikeus tulla unohdetuksi
- Oikeus käsittelyn rajoittamiseen ja rekisterinpitäjän velvollisuus ilmoittaa rajoituksesta
- Oikeus siirtää tiedot järjestelmästä toiseen
- Vastustamisoikeus
- Automatisoidut yksittäispäätökset ja profilointi

VAIKUTUKSET

REKISTERÖITY

- Selkeät säännöt vastuista
- Tarkemmat määritelmät käsitteistä
- Mahdollisuus ”hallita” omia tietoja
  - Kriittinen aineeton omaisuus

ORGANISAATIO

- GDPR digitalisoinnin lähtölaukauksena
  - Palveluiden automatisointi
  - Mahdollistaa skaalautuvuuden
- Tietoeettisyys ja läpinäkyvyys
  - Viesti asiakkaille organisaation vastuullisuudesta
  - Kilpailuedun ja markkina-aseman pitäminen
    - GDPR:n sitominen yrityksen strategiaan ja liiketoimintaan
- GDPR osana yrityksen arkea

EPÄONNISTUMISEN VAIKUTUKSET

RAJATTUJA
LYHYTAIKAISIA
EI MERKITYKSELLISIÄ
VAIKUTUKSIA
LAAJA-ALAISIA
PITKÄ-KESTOISIA
VAKAVIA

Organisaatiotaso	Yksityinen taso
Suorat taloudelliset vahingot ja rikosoikeudelliset seuraamukset (Mikäli yrityksen todetaan rikkoneen asetuksen vaatimuksia, hallinnolliset sanktiot voivat nousta jopa 20 miljoonaan euroon tai 4 %:in globaalista liikevaihdosta, korkeamman mukaan, vankeus..)	*Yksityisyyden menetys*
Menetetyn aineettoman omaisuuden aiheuttama vahinko	*Henkilökohtaisen, perheen ja läheisten turvallisuuden vaarantuminen*
Arkaluontoisen tiedon menettämisen aiheuttamat vahingot	*Omaisuuden vaarantuminen*
Kilpailuedun ja maineen menetys	*Suorat taloudelliset vahingot*
Työsuhdeperustaiset seuraamukset	*Henkilökohtaisen identiteetin ja immuniteetin vaarantuminen*
Luottamuksen menetys	*Arjen ja toimintojen hallinnan vaarantuminen*
Asiakkuuksien ja yt-kumppaneiden menetys	*Hyvinvoinnin heikentyminen*
Toimintojen ja palveluiden pysähtyminen tai hidastuminen	*Turvattomuuden lisääntyminen*
Aiheutuvat lisä- / vaihtoehtoiskustannukset	*Aiheutuvat lisäkustannukset*
Toiminnan kannattamattomuus	*Maineen menetys*

FYYSISIÄ
TALOUDELLISIA
AINEELLISIA
AINEETTOMIA
HENKISIÄ
POLIITTISIA

RIKKOMUSTEN SEURAAMUKSIA

Toteutuneilla tietosuojaloukkauksilla voi olla vaikutuksia esimerkiksi:

- verkkoihin
- laitteisiin
- käyttöoikeuksiin
- Tietoon (CIA)
- palveluihin ja tuotteisiin
- ihmisiin

- Yrityksen täytyy perusteellisesti osoittaa, että heillä vähintään aito tarkoitus noudattaa lakia. Uusi vaatimus ulottuu tietotekniikan tasolle ja konkreettisesti todettuna tietojärjestelmien tulee jo suunnitteluvaiheessa sisältää vain asianmukaisen tiedon käsittelyä.
- Järjestelmien tulee tukea jo oletusasetuksinaan tietosuojaa. Esimerkiksi kuluttajan valmiiksi ruksitettua laatikkoa ei pidetä pätevänä suostumuksena henkilötietojen käsittelyyn.

YHTEENVETO

- Peruskäsitteet
- Taustoitus
- Henkilötietojen käsittelyn oikeusperusteet
- Rekisteröidyn oikeudet
- Tietosuoja-asetuksen vaikutukset

- Avointen kysymysten läpikäynti
  - Kokemuksia ja ajatuksia?
  - Mitä olen oppinut?

KIITOS

pauliina.hirvonen@citrus.fi

mygdpr.fi