

EU:n tietosuoja-asetus ja sen vaikutukset verkkokaupalle

eComGrowth - Teemavalmennus: Rahoitus, laki ja johtaminen

Jukka Lång, asianajaja, CIPP/E ([Twitter: @JukkaLang](#))

> 23.3.2017

DITTMAR & INDRENIUS

Sisältö

- 1) Mitä tulee tietää lainsäädäntömuutoksista?
 - EU:n tietosuoja-asetus ("GDPR")
- 2) Miten muutos vaikuttaa liiketoimintaasi?
 - Verkkokaupan ja digitaalisen liiketoiminnan näkökulma

> 23.3.2017

DITTMAR & INDRENIUS



EU ja kiristyvää tietosuojalainsäädäntö

- EU ottanut hyvin kunnianhimoisen asenteen datan säätelyyn
- Tulossa merkittäviä rajoituksia digitaaliselle liiketoiminnalle
 - esimerkkejä GDPR:n soveltamisalasta:
 - käsittelyn **ulkoistaminen** ja pilviratkaisujen käyttö
 - datan **kerääminen, käyttö ja jakaminen**
 - asiakkaiden **profilointi**
 - **Big Data -analytiikan** hyödyntäminen



MUUTOSTA OHJAAVAT VOIMAT

DITTMAR & INDRENIUS

EU:n digitaaliset sisämarkkinat

- **Säätelyn harmonisaatio**
 - Yhtäläisen lain suora sovellettavuus kaikissa EU-jäsenvaltioissa
- **Tietosuoja osa laajempaa projektia**
 - Kuluttajansuoja, tekijänoikeudet ja kilpailuoikeus harmonisoituvat
- **Lain koura ulotetaan myös EU:n ulkopuolisiin kilpailijoihin**
 - Kohteena kaikki, jotka myyvät EU-kansalaisille



> 23.3.2017

DITTMAR & INDRENIUS

Henkilötiedon käsite



Henkilötiedolla tarkoitetaan:

”kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä ’rekisteröity’, liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella” (GDPR 4 art. kohta 1)

> 23.3.2017

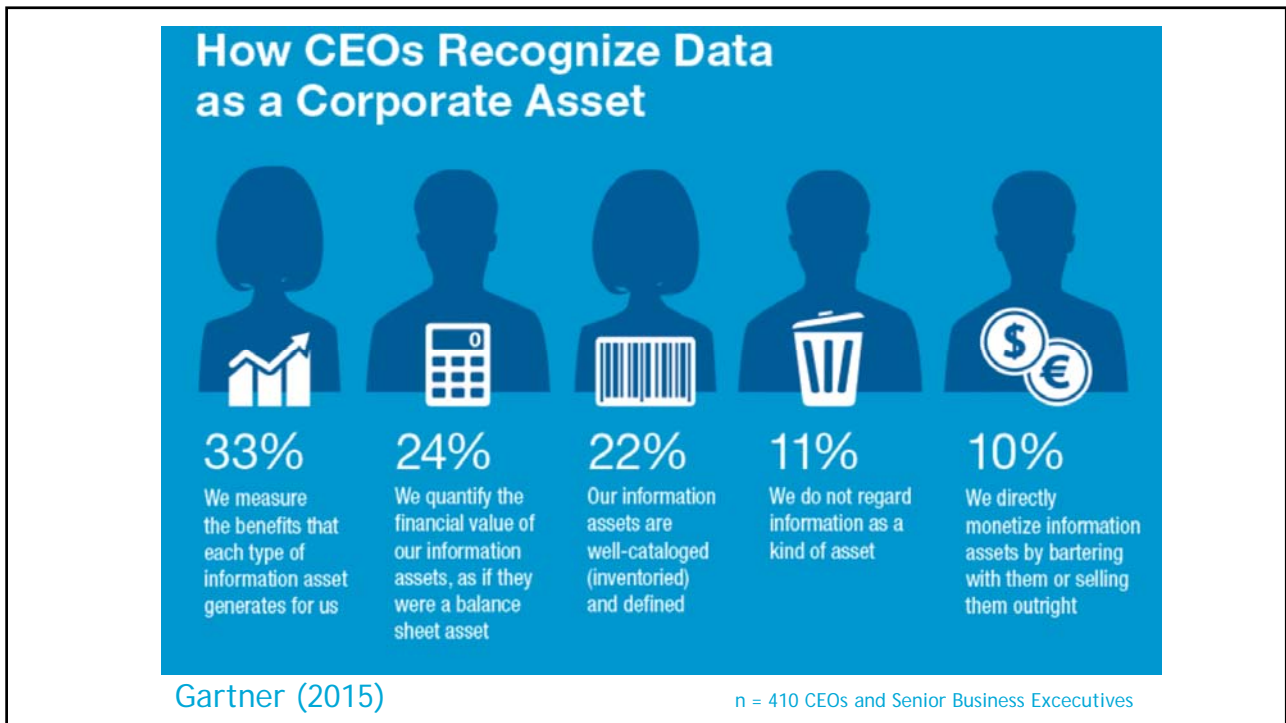
DITTMAR & INDRENIUS

Dataintensiivinen teknologia korostaa yksityisyyden suojan merkitystä

- Yksilön **”digitaalinen jalanjälki”** kasvaa jatkuvasti
 - **Henkilötiedon** lakiperusteinen määritelmä on hyvin kattava
- Yksityisyys on perustuslaissa turvattu oikeus
 - Itsemääräämisoikeus omista tiedoista
 - Oikeus tietää omien tietojen käsittelystä

> 23.3.2017

DITTMAR & INDRENIUS



Maailman arvokkaimmat brändit 2008 ja 2016

2008		2016	
Brändi	Arvo (MUSD)	Brändi	Arvo (MUSD)
1 Google	86.057	1 Google	229.198
2 General Electric	71.379	2 Apple	228.460
3 Microsoft	70.887	3 Microsoft	121.284
4 Coca-Cola	58.208	4 AT&T	107.387
5 China Mobile	57.225	5 Facebook	102.551
6 IBM	55.335	6 VISA	100.800
7 Apple	55.206	7 Amazon	98.988
8 McDonald's	49.499	8 Verizon	93.220
9 Nokia	43.975	9 McDonald's	88.654
10 Marlboro	37.324	10 IBM	86.206

Lähde: Kantar Millward Brown

Datasta tullut tuotannontekijä

- Data digitalisaation mahdollistajana
 - Datan määrä on kasvanut räjähdysmäisesti
 - Innovaatiot perustuvat yhä useammin *henkilötietojen* hyödyntämismahdollisuudelle
- Datan taloudellisen arvon kasvulla juridisia seurauksia
 - Kysymys omistus- ja määräysvallasta syntyvään dataan
 - Sopimusten merkityksen kasvu
 - Data-assetien suojaamisintressi

> 23.3.2017

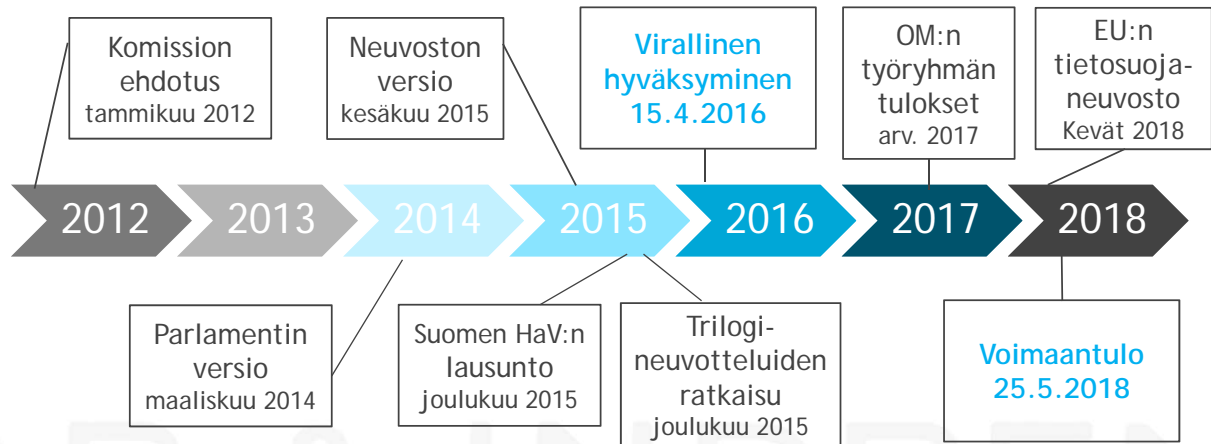
DITTMAR & INDRENIUS



EU:N TIETOSUOJAUUDISTUS

DITTMAR & INDRENIUS

Tietosuojauudistuksen vaiheet



> 23.3.2017

DITTMAR & INDRENIUS

The Telegraph

HOME » TECHNOLOGY » TECHNOLOGY NEWS

EU Privacy regulations subject to 'unprecedented lobbying'

EU Commissioner Viviane Reding says new regulations on digital privacy are designed 'to stand for 30 years' but were subject to the most aggressive lobbying she has ever witnessed.

f 11
t 11
p 0
in 0
11
Email



EU commissioner Viviane Reding Photo: REUTERS

8 February 2012

Keskeisimmät muutokset pähkinänkuoressa

1. Yksilöiden oikeudet laajentuvat
 - Kontrollia omaan dataan tehostetaan
2. Yritysten velvollisuudet lisääntyvät
 - Datan käsittelyyn liittyvät kasvavat riskit
3. Valvonta tehostuu
 - Sanktiot tulevat ohjaamaan toimintaa

> 23.3.2017

DITTMAR & INDRENIUS

Uusi sanktiouhka

- Asetuksen rikkomisesta voi seurata rikkomuksen vakavuuden perusteella määräytyvä hallinnollinen sakko
 - Ylempi sakkoluokka 20.000.000 euroa tai 4 % liikevaihdosta
 - Lasketaan yrityksen (konsernin) edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta
- Kansallisella tietosuojaviranomaisella merkittävä harkinnanvara sakon määrästä

> 23.3.2017

DITTMAR & INDRENIUS



UK firms could face £122bn in data breach fines in 2018

Warwick Ashford
Security Editor
ComputerWeekly.com

17 Oct 2016 9:10

[Twitter](#) [G+](#) [LinkedIn](#) [Email](#)

The PCI Security Standards Council is urging firms to act now to avoid exponentially increased penalties under new EU data protection regulations

"The new EU legislation will be an absolute game-changer for both large organisations and SMEs as the regulator will be able to impose a stratospheric rise in penalties for security breaches, and it remains to be seen whether businesses facing these fines will be able to shoulder the costs," said Jeremy King, international director at PCI SSC.

"Companies, both large and small, need to act now and start putting in place robust standards and procedures to counter the cyber security threat, or face the prospect of paying astronomical costs in regulatory fines and reputational harm to their brand."

“ Asetuksen ensisijaisena tavoitteena on edistää digitaalisten sisämarkkinoiden kehittymistä, kilpailukykyä ja talouskasvua. Siksi olen huolestuneena seurannut tietosuojaihteistä viestintää, jonka kärkenä on suoranaisesti pelotella toimijoita sanktioilla. Se on mielestäni erinäisiltä kouluttajilta ja konsulteilta lyhytnäköistä kerman kuorintaa, joka kääntyy itseään vastaan.

Tietosuojavaltuutettu Reijo Aarnio blogi 1.3.2017,
"Totuus hallinnollisista sanktioista"



Uusia velvoitteita

- **Oman toiminnan suunnitteleminen ja perustelevminen**
 - tietosuojanäkökulma osaksi kaikkea (*Privacy by Design*)
 - vaikutustenarviointi (*Privacy Impact Assessment*)
 - suostumusten varmistaminen tulevalle käsittelylle
- **Asiakkaiden informoiminen**
 - tietosuojaselosteen päivittäminen
 - erityisesti profiloinnin osalta
- **Sanktioihin ja vastuisiin varautuminen**
 - myyntiehdot ja sopimukset
- **Osoitusvelvollisuus**
 - toimenpiteiden dokumentointi
 - compliancen varmistaminen

> 23.3.2017

DITTMAR & INDRENIUS

Esimerkki - Asiakkaiden informoiminen

Tieto	HTL	TSA
Rekisterinpitäjän nimi ja yhteystiedot	10, 24, 25 §	14 artikla
Rekisterinpitäjän edustajan nimi ja yhteystiedot	10, 24 § (vain tarvittaessa)	14 artikla (sis. tietosuojavastaavan tiedot)
Henkilötietojen käsittelyn tarkoitus	10, 24 §	14 artikla
Kuvaus rekisteröityjen ryhmästä ja näihin liittyvistä tiedoista tai tietoryhmistä	10 §	
Kuvaus rekisteröityihin liittyvistä tiedoista tai tietoryhmistä	10 §	
Tietojen saajat	10, 24 § (vain säännönmukaiset luovutuskohteet)	14 artikla (tietojen vastaanottajat tai -ryhmät)
Tieto siitä, siirretäänkö tietoja EU/ ETA ulkopuolelle	10 §	14 artikla (sis. myös kv-organisaatiot, siirtoperusteet ym.)
Kuvaus rekisterin suojausten periaatteista	10 §	
Tiedot, jotka tarpeen rekisteröidyn oikeuksien käyttämiseksi	24 §	14 artikla
Henkilörekisterin nimi	25 §	
Rekisterinpitäjän käsittelyperusteena toimiva oikeutettu etu		14 artikla (jos käsittely perustuu 6(1)(f) artiklaan)
Tieto säilytysajoista		14 artikla
Tieto oikeudesta perua suostumus + tietyt lisätiedot		14 artikla (ei koske kaikkea käsittelyä)
Tieto oikeudesta saattaa asia viranomaisen käsiteltäväksi		14 artikla
Tieto siitä, että käsittely perustuu sopimus- tai lakiperusteiseen vaatimukseen + tietyt lisätiedot		14 artikla
Tieto automaattiseen tietojen käsittelyyn perustuvasta profiloinnista		14 artikla

> 23.3.2017

DITTMAR & INDRENIUS

Esimerkki - Suostumus käsittelyperusteena

- Nykyistä tiukemmat kriteerit sen arvioimiselle, onko yksilö hyväksynyt henkilötietojensa käsittelyn
 - Suostumus saatava selkeästi suostumusta ilmaisevalla toimella
 - "Vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu"
 - Vapaaehtoisuudelle asetettu kriteereitä
 - Tietoisuus varmistettava informoinnilla
 - Ei sallittua "niputtaa" erillisiä käsittelytoimia saman suostumuksen alle
 - Suostumusta ei saa asettaa palvelun tarjoamisen edellytykseksi, jos tällainen suostumus ei ole tarpeellista sopimuksen täytäntöön panemiseksi
- Suostumus on yksipuolisesti peruutettavissa
- Uudet vaatimukset eivät vaikuta taannehtivasti

> 23.3.2017

DITTMAR & INDRENIUS



TIETOSUOJA -
VÄLTTÄMÄTTÖMYYDESTÄ HYVE

DITTMAR & INDRENIUS

Tietosuoja nousemassa uuteen rooliin

- Tietosuojasta tullut yrityksille osa vastuullista liiketoimintaa ja riskienhallintaa
- Haettaessa uudesta teknologiasta tehokkuutta ja kilpailuetua tietosuojan on ymmärrettävä olevan olennainen osatekijä

> 23.3.2017

DITTMAR & INDRENIUS

Tietosuojasta menestystekijä?

First thoughts

- uusia compliance-kustannuksia ja ylimääräistä työtä
- abstrakteja ja epäselviksi jääviä velvollisuuksia
- tuotteiden ja palveluiden toteutuksen sääntely
- suomalaisille vierasta ajattelua
- pakottaa tietosuojan osaksi muita toimintoja

Second thoughts

- + konkreettisia työkaluja käytännön ongelmien ratkaisemiseksi
- + joustavaa sääntelyä ja mahdollisuus parhaiden käytäntöjen etsimiseen
- + laadullisesti paremmat tuotteet ja palvelut
- + globaalien markkinoiden avautuminen
- + tuo tietosuojan osaksi muita toimintoja

> 23.3.2017

DITTMAR & INDRENIUS

Key Insights

- 1) Tietosuoja-asetuksen ottaminen haltuun on mittava hanke
- valmistautumista koskeva toimintasuunnitelma agendalle
- 2) Data luo merkittäviä mahdollisuuksia lisäarvon synnyttämiseen
- menestyvissä konsepteissa lisäarvoa jaetaan myös asiakkaille
- 3) Tietosuoja-asetus tarjoaa vahvan kannustimen tekemiselle
- välttämättömyydestä kannattaa tehdä hyve!

> 23.3.2017

DITTMAR & INDRENIUS

Kiitos!

Jukka Lång

Head of Data Protection, Marketing & Consumers

Osakas, OTK, FM, CIPP/E

Tel. +358 40 719 4317

Email: jukka.lang@dittmar.fi

Twitter: @JukkaLang



> 23.3.2017

DITTMAR & INDRENIUS