



Yritystoiminnan suojaus sekä GDPR – yhdessä enemmän

Oikeat työt ja työnhaitat tietosuojasääntelyssä – miten tässä voi mitään töitä tehdä? yritysespooli 4.11.2020
Juha Sallinen, konsultti, eMBA ja insinööri

1

Juha Sallinen / GDPR Tech



Juha Sallinen

- 040-5666 900
- juha@gdprtech.com
- Insinööri, eMBA/International Business Management, yrittäjä
- Aiempia tehtäviä yhtiöissä, kuten Tieto, HP, Wipro, Symantec, Pedab, Veritas
- GDPR Tech toimii Pohjoismaissa sekä Baltiassa
- Koulutus, konsultointi, ratkaisut
 - Auditoinnit
 - Projektit
 - Rakenteettoman tiedon kartoitus
 - Tietosuojavastaava palveluna

Referenssiasiakkaitamme verkkosivullamme, mm.



TAPAUS

Sastamalan
Tukipalvelu Oy

Diax

FUJITSU

WANNADO[®]

Holiday Club

Etelä-Savo
SAIMAAN
MAAKUNTA

FCG

2

Muutama yleinen väärinkäsitys ja huomio

- GDPR:ssä ei ole käsitettä **“Rekisteriseloste”** tai **“tietosuojaseloste”**, joten sellaista ei tarvita verkkosivulle.
- Viittaukset **“henkilötietolakiin”**
- Tämä ei koske meitä, olemme pieni yritys/organisaatio/yhdistys
- Sen sijaan siinä on **“informointivelvoite”** – tästä myöhemmin
- Henkilötietolaki on kumottu jo 12/2018
- Asetus ja tietosuojalaki, koskevat kaikkia paitsi kotitalouksia
- Lisäksi Suomessa on uutena 1/2020 tiedonhallintalaki ja noin 700+ vanhaa lakia

© Copyright GDPR Tech 2016-2020

yritysespool 4.11.2020

3

3

Mikä muka voisi mennä pieleen?

Markkinointi, puhelin- tai sähköpostiviestit ja robottisoitot

Tekniset suojaukset, sopimukset, käsittely, ...

ACC Consulting / 7000 euroa sakkoja / 212 tuhatta liikevaihto

<https://tietosuoja.fi/-/yritykselle-seuraamusmaksu-sahkoisen-suoramarkkinoinnin-harjoittamisesta-ilman-ennalta-annettua-suostumusta-ja-rekisteroidyn-oikeuksien-laiminlyonnista>

YLE uutiset 10/2020

Selvitimme, millä tolalla yksityisten terveysfirmojen tietoturva-asiat ovat – ongelmia löytyi heti: **“Järjestelmiin kirjautuminen on ihan retuperällä”**

Valviran mukaan tietoturvaan liittyvät yhteydenotot ovat lisääntyneet erityisesti yksityisen terveydenhuollon asiakkailta.

No etelä-Euroopassa ei ainakaan ole tehty mitään...

No ei niitä sanktioita tule...					Quoted Art.	
Country	Date	Fine [€]	Company	Art.	Quoted Art.	
FINLAND	2020-08-05	7,000	Acc Consulting Varsinais-Suomi	Art. 5 GDPR, Art. 6 GDPR		
FINLAND	2020-05-29	72,000	Takal Helsinki			
FINLAND	2020-05-22	100,000	Posti Group Oyj			
FINLAND	2020-05-22	16,000	Kymen Vesi Oy			
FINLAND	2020-05-22	12,500	Unknown Company			
ITALY	2019-04-17	50,000				
ITALY	2019-12-11	8,500,000	Eni Gas e Luce	Art. 5 GDPR, Art. 6 GDPR, Art. 17 GDPR		
ITALY	2019-12-11	3,000,000	Eni Gas e Luce	Art. 5 GDPR, Art. 6 GDPR		
ITALY	2020-01-15	27,800,000	TIM (telecommunications operator)	Art. 5 GDPR, Art. 6 GDPR, Art. 17 GDPR, Art. 32 GDPR		
ITALY	2020-01-15	10,000	Community of Francavilla Fontana	Art. 5 GDPR, Art. 6 GDPR		

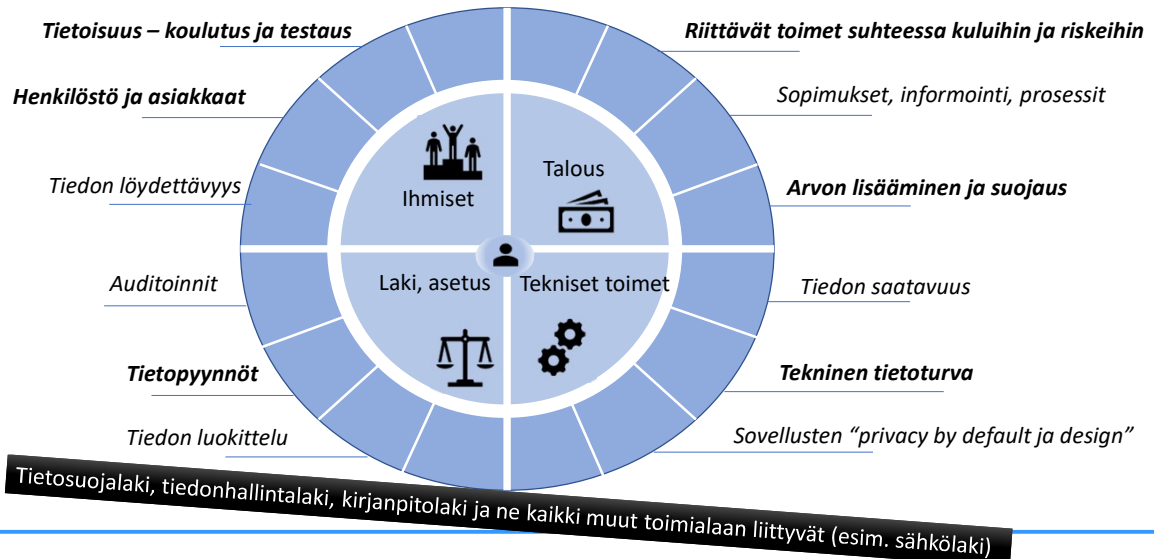
© Copyright GDPR Tech 2016-2020

yritysespool 4.11.2020

4

4

Käsittelytoimien ja tietojärjestelmien vaatimustenmukaisuuden arviointi



© Copyright GDPR Tech 2020

Käsittelytoimien ja tietojärjestelmien vaatimustenmukaisuuden arviointi

5

5



© Copyright GDPR Tech 2020

yritysespoo 4.11.2020

6

6

GDPR Tech

Tietosuojatyössä ja GDPR asioissa järjen käyttö on sallittua.
GDPR Tech, Juha Sallinen.

Helppoa. Suojaa henkilötiedot ja varmista toiminnan jatkuvuus. Suojaat samalla mainettasi sekä pienennät toimintahäiriöitä ja vältät mahdollisilta sanktioilta.

KOHTA 1
SELVITÄ, TARVITAANKO TEILLÄ TIETOSUOJAVASTAAVA

KÄYTÄNNÖSSÄ LÄHES KAIKILLA ORGANISAATIOILLA PITÄÄ OLLA NIMETTY VASTUUHENKILO, SE VOI OLLA MYÖS ULKOISTETTU DPO

KOHTA 2
KUVA, MITEN TEILLÄ KÄSITELLÄÄN HENKILÖTIETOJA

ESIMERKIKSI LIISA HAKEE TEILLE TOIHIN MIHIN KAIKKIALLE LIISAN TIETOJA TALLETETAAN?

KOHTA 3
ONKO HENKILÖTIETOJEN KÄSITTELYLLE LAILLINEN PERUSTE

YLEENSÄ TÄMÄ EI OLE ONGELMA, TIETOJEN KÄSITTELY VOI KUITENKIN VAATIA SUOSTUMUKSEN ONKO ALA-IRKASTEN TIETOJA?

KOHTA 4
MILLAISIA RISKEJÄ HENKILÖTIETOJEN KÄSITTELYYN VOI LIITTÄÄ? MINIMOI RISKIT!

ESIMERKIKSI JOKU VOI VARASTAA TIETOKONEESI, JOSSE EI OLLUTKAAN HYVÄÄ SUOJAUSTA TAI PEKKA LÄHETTÄÄ LIISAN HENKILÖTIETOJA VAARALLE VASTAANOTTAJALLE.

KOHTA 5
VALMISTAUDU HENKILÖN OIKEUKSIIN, KUTEN TIETOPYNTÖIHIN

PÄIVITÄ PROSESSIT TAMAN OSALTA JA NÄYTÄ, ETÄ OLET ASIAKKAAN TAI HENKILÖN PUOLELLA TESTAAMASSA TOIMIVUUS

KOHTA 6
HUOLEHDI TIETOTURVASTA RIITTÄVÄSTI

HUOMIOI ESIM. FYSINEN JA SÄHKÖINEN SUOJAUS, SAMOIN KUIN KÄYTÄNNÖN TOIMET TYÖSSÄ (ESIM. OVIEK LUKITUS, TYÖASEMA LUKKOON POISTUUN)

KOHTA 7
VARMISTA, ETÄ SOPIMUKSET OVAT AJANTASALLA KUMPPANEIDEN JA TOIMITTAJIEN OSALTA

MUISTA SIIS, OLETTE VASTUUNSSA MYÖS KUMPPANEISTANNE JA TOIMITTAJASTANNE. VALITKAA VIISAOSTI, VAIHTAKAA TARVITTAESSA, MUISTA SOPIMUKSET!!

KOHTA 8
HUOLEHDI INFORMOINNISTA

TIETOITA HENKILÖILLE, ETÄ KÄSITTELETTÄ HEIDÄN TIETOJA. ESIM. WEBSIVU SEKA TIETOLAHEET.

KOHTA 9
JOS TUOT UUSIA PALVELUITA, MUISTA VAIKUTUSTENARVIOINTI

UUSI TILANNE VOI LUODA UUSIA RISKEJÄ TAI PIENENTÄÄ OLEMASSA OLEVIA VARMENNA ETUKATEEN.

KOHTA 10
MUISTA NÄYTTÖVELVOITE - HYVÄ TAHTO EI RIITÄ

SUUNNITTELE, TOTEUTA, VALVO JA KORJAA TARVITTAESSA. DOKUMENTOI RIITTÄVÄSTI.

Kaikkessa tässä on tietenkin otettava organisaation koko ja vaikeudet huomioon. Tämä ei ole kuitenkaan vaikeaa.

OK

© Copyright GDPR Tech 2016-2020

yritysespool 4.11.2020

7

Tietosuojavaltuutetun ohjeistus / DPO

KOHTA 1 SELVITÄ, TARVITAANKO TEILLÄ TIETOSUOJAVASTAAVA

KÄYTÄNNÖSSÄ LÄHES KAIKILLA ORGANISAATIOILLA PITÄÄ OLLA NIMETTY VASTUUHENKILO, SE VOI OLLA MYÖS ULKOISTETTU DPO

- Tietosuojavastaava on pakollista nimittää, jos:
 - ”tietojenkäsittelyä suorittaa viranomainen tai julkishallinnon elin”
 - ”rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seuranta”
- Käytännössä – yrittäjä vastaa

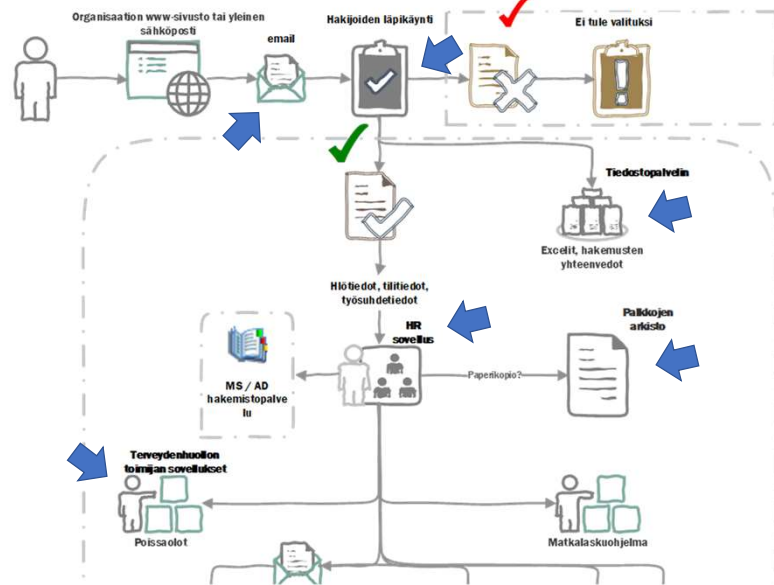
Tietojen käsittely

KOHTA 2

KUVAAMITEN TEILLÄ
KÄSITELLÄÄN
HENKILÖTIETOJA

ESIMERKIKSI LIISA HAKEE
TEILLE TÖIHIN. MIHIN
KAIKKIALLE LIISAN
TIETOJA TALLETETAAN?

"HEI, HAEN
TEILLE
TÖIHIN"



© Copyright GDPR Tech 2016-2020

yritysespooli 4.11.2020

9

9

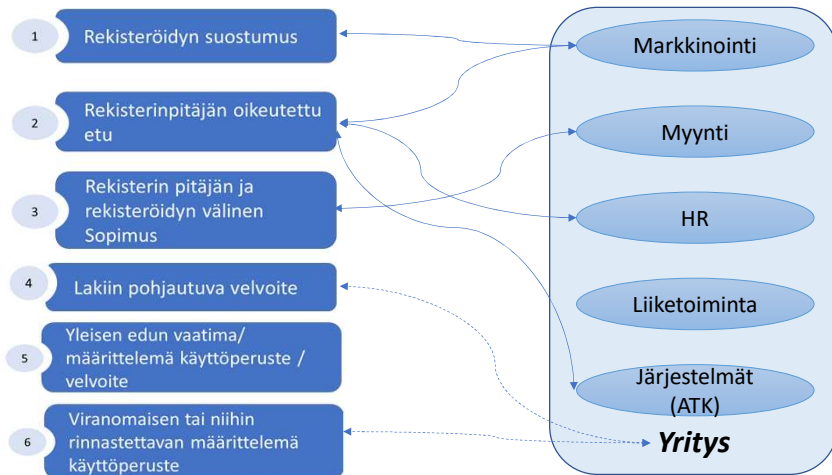
Perusteet tietojenkäsittelyyn (esim.)

KOHTA 3

ONKO HENKILÖTIETOJEN
KÄSITTELYLLE LAILLINEN
PERUSTE

YLEENSÄ TÄMÄ EI OLE
ONGELMA, TIETOJEN
KÄSITTELY VOI
KUITENKIN VAATIA
SUOSTUMUKSEN! ONKO
ALA-IKÄISTEN TIETOJA?

TIETOJANI KÄSITELLÄÄN
TYÖTEHTÄVÄÄN
LIITTYEN, OK.



© Copyright GDPR Tech 2018

yritysespooli 4.11.2020

10

10

Tehtävä – millaisia riskejä teillä voisi olla?

KOHTA 4

MILLAISIA RISKEJÄ HENKILÖTIETOJEN KÄSITTELYYN VOI LIITTYÄ? MINIMOI RISKIT!

ESIMERKIKSI JOKU VOI VARASTAA TIETOKONEESI, JOSSA EI OLLUTKAAN HYVÄÄ SUOJAUSTA TAI PEKKA LÄHETTÄÄ LIISAN HENKILÖTIETOJA VÄÄRÄLLE VASTAANOTTAJALLE.

OOPS!



Riski	Vaikutusarvio	Todennäköisyys	Kokonais pistemäärä (V * T)
Mitä voisi tapahtua	Vähäinen – Kriittinen (1-10)	Epätodennäköinen - Lähes varma (1-10)	
Riittämätön toimittajan ohjeistus (esim. tilitoimisto)	4	3	
Kannettavan häviäminen tai anastus			
Ei riittävää tietoa aiheesta, henkilöstö ei ole koulutettu			
Tekninen tietoturva (esim. heikot salasana)			

© Copyright GDPR Tech 2018

yritysespool 4.11.2020

11

11

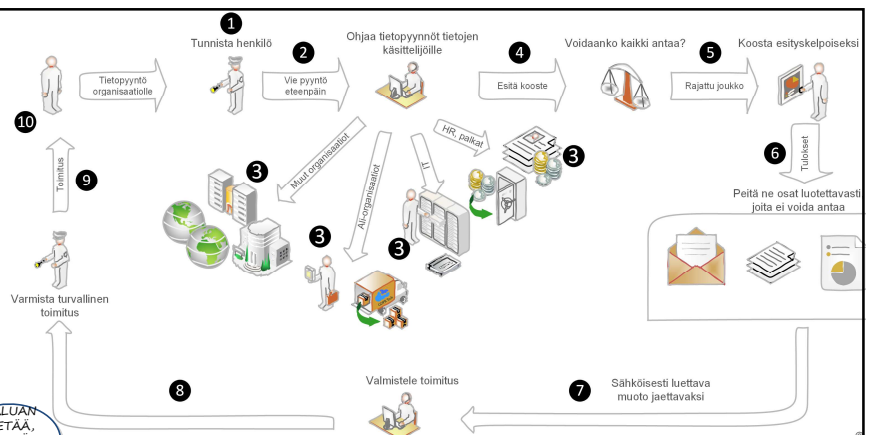
KOHTA 5

VALMISTAUDU HENKILÖN OIKEUKSIIN, KUTEN TIETOPYYNTÖIHIN

PÄIVITÄ PROSESSIT TÄMÄN OSALTA JA NÄYTÄ, ETTÄ OLET ASIAKKAAN TAI HENKILÖN PUOLELLA. TESTAA PROSESSIN TOIMIVUUS

HALUAN TIETÄÄ, MISSÄ TIETOJANI ON

ON



© Copyright GDPR Tech 2016-2020

yritysespool 4.11.2020

12

12

Tehtävä – miten voit huolehtia teillä tietosuojatyöstä ja turvallisuudesta?

KOHTA 6

HUOLEHDI
TIETOTURVASTA
RIITTÄVÄSTI

HUOMIOI ESIM. FYYSSINEN
JA SÄHKÖINEN SUOJAUS,
SAMOIN KUIN
KÄYTÄNNÖN TOIMET
TYÖSSÄ (ESIM. OVIERN
LUKITUS, TYÖASEMA
LUKKOON POISTUESSA)



Fyysinen murtautuminen toimistolle.

Suojauksena lukitus ja
murtohälytys
Tietokoneen lukitus
Lukkojen käyttö



Tietokoneen kadottaminen tai siihen kohdistuu virus

Suojauksena koneen
salasana ja ajantasaiset
päivitykset, ml.
tietoturvasuojaukset
Testattu
varmuuskopiointi
Salasanojen käyttö



Henkilö pyytää tietojaan poistettavaksi, miten tunnistan henkilön luotettavasti?

Oma tarkistuslista tai
käyttämällä sähköistä
tunnistamista
Sähköinen allekirjoitus



Itse tai työntekijät eivät ole tietoisia asetuksen käytännön toimista

Käytä verkosta löytyviä
koulutuksia tai hanki
apua luotettavalta
taholta
Yrittäjäjärjestöjen
koulutukset
Kaupalliset tahot

Alihankkijat ja sopimukset

KOHTA 7

VARMISTA, ETTÄ
SOPIMUKSET OVAT
AJANTASALLA
KUMPPANEIDEN JA
TOIMITTAJIEN OSALTA

MUISTA SIIS, OLETTE
VASTUUSSA MYÖS
KUMPPANEISTANNE JA
TOIMITTAJISTANNE.
VALITKAA VIISAASTI,
VAIHTAKAA
TARVITTAESSA. MUISTA
SOPIMUKSET!!!

- Huomattava muutos GDPR:ssä on sekä tietojen tallentajan (controller) että käsittelijän (processo) vastuut
- Tämä vaatii käytännössä sopimusmuutoksia
 - Salassapitosopimus
 - Tietojenkäsittelysopimus (DPA)
 - Vastuut ja velvoitteet

Huolehdi informoinnista

KOHTA 8

HUOLEHDI
INFORMOINNISTA

TIEDOITA HENKILÖILLE,
ETTÄ KÄSITTELETTE
HEIDÄN TIETOJA. ESIM.
WEBSIVU SEKÄ
TIETOLÄHTEET.

TAPASIMME
2016
MESSUILLA

"MISTÄ SAITTE
TIETONI!"

- Helpoin tapa – verkkosivulla
"tietosuojalupaus" tai
"tietosuojalausunto"
- "Käsitlemme tietoja
luottamuksellisesti ja GDPR:n mukaan"
 - Teksti, logo, lupaus
 - Helppoa tekstiä – kohde huomioiden
- HUOM! Ei sama kuin sisäinen seloste
käsittelytoimista
 - Ei siis "tietoja tallennetaan lukittuun
kaappiin, joka sijaitsee huoneessa x"

© Copyright GDPR Tech 2016-2020

yrittäjäseppä 4.11.2020

15

15

KOHTA 9

JOS TUOT UUSIA
PALVELUITA, MUISTA
VAIKUTUSTENARVIOINTI

UUSI TILANNE VOI LUODA
UUSIA RISKEJÄ TAI
PIENENTÄÄ OLEMASSA
OLEVIA. VARMENNA
ETUKÄTEEN.

EI VOI.

"VOIKO TIETOJANI
KÄYTTÄÄ KUKA
TAHANSÄ?"

Huipputurvallisena mainostetusta
suomalaissovelluksesta löytyi nolo
aukko – SK- vuotaa käyttäjätietoja
toisille käyttäjille

TIET 11.3.2019 14:34 TIETOTURVA DIGITEKNIIKKA



Turvallisena itseään mainostava suomalainen viestisovellus FoilChat ei
täytä Suomen henkilötietolain tai EU:n tietosuojalain vaatimuksia.

Tietosuojaskandaali pakotti
liikenneviraston toimiin – kaikkea ei
kerrota, osa tiedoista salattu

Karkimo 28.5.2019 11:06 | päivitetty 28.5.2019 11:08 TIETOSUOJA JULKISEN HALLINNON ICT



Liikenteen turvallisuusvirasto Trafi sai viime metreilläään ruman tahrn
takkiinsa: sen sähköisestä palvelusta pystyi kaivamaan kaikenlaista
tietoa, jota ei ollut tarkoitettu yleiseen jakoon.

© Copyright GDPR Tech 2016-2020

yrittäjäseppä 4.11.2020

16

16

KOHTA 10
MUISTA NÄYTTÖVELVOITE
- HYVÄ TAHTO EI RIITÄ

SUUNNITTELE, TOTEUTA,
VALVO JA KORJAA
TARVITTAESSA.
DOKUMENTOI
RIITTÄVÄSTI.


TIETOJÄRJESTELMÄT
Missä henkilötietoa on ja miten näitä
systeemejä valvotaan?


KUMPPANIT JA SOPIMUKSET
Ketkä käsittelevät kanssamme tietoja?
Mitä ollaan sovittu?


HENKILÖTIETOREKISTERIT
Mihin rekistereihin tietomme jakautuvat?
Ovatko vaaditut asiat kunnossa?


MUUT KÄSITTELYTOIMET
Käsittelemmekö muiden omistamia
henkilötietoja?


TURVALLISUUSTOIMENPITEET
Mitä teemme, jotta ihmisten henkilötiedot
pysyvät turvassa?


RISKIT
Minkä haitallisten tapahtumien suhteen
meidän on varauduttava?

© Copyright GDPR Tech 2016-2020

yrittäjäseppä 4.11.2020

17

17

+1 Evästeet ja markkinointi

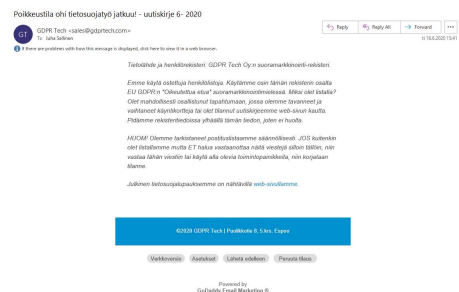
Pitää suunnitella, mitä toiminnallisia ja markkinointievästeitä halutaan käyttää www-sivulla

Evästeiden osalta tekniset/toiminnalliset ovat yleisesti hyväksytty

Markkinointievästeet (ja käytön seuranta), edellyttävät hyväksyntää

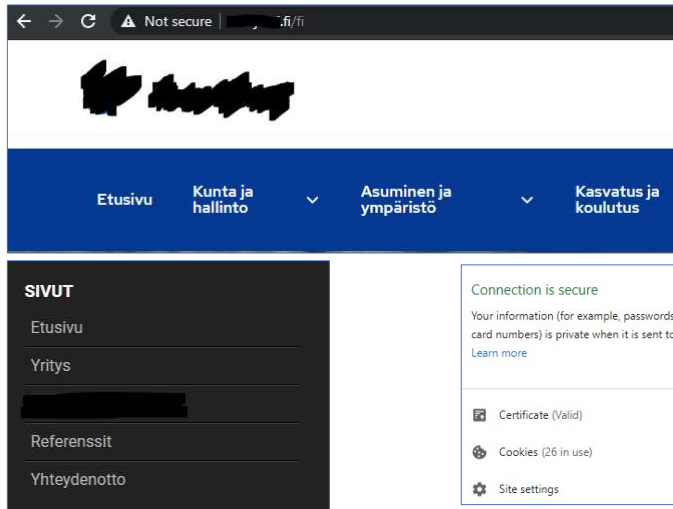
Hyväksynnän pitää olla OPT/IN tyyppinen

Pääosa evästeiden "hyväksyntä" jutuista ei toimi oikein – ja evästeitä on liikaa



18

Esimerkkejä riskien paikoista



- ☐ Onhan sivusto suojattu SSL osalta (https://)
- ☐ Informoiko sivusto GDPR:stä mitään (lupaus tietojen käsittelystä?)
- ☐ Onko evästeistä ilmoitus – toimiiko se?
- ☐ Miten tietopyyntö on rakennettu?
- ☐ Vastaako toiminta allekirjoitetun sopimuksen sisältöä?

© Copyright GDPR Tech 2020

Käsittelytoimien ja tietojärjestelmien vaatimustenmukaisuuden arviointi

19

19

Yhteenveto

- **Turvaamalla** henkilötietoja asiallisesti, suojaat myös henkilötietoja
- **Riskien tunnistaminen** auttaa myös liiketoiminnan jatkuvuuteen liittyvässä suunnittelussa
- **Maineriski** on pahempi kuin sanktio – menettämällä asiakkaat (henkilöt) – menetät ydintoiminnat
- **Kyberturva ja kyberuhat** (esim. verkkorikolliset) ovat tätä päivää – suojaudu myös näiltä uhilta
- **Normaali liiketoiminta** on sallittua, samoin järjen käyttö



© Copyright GDPR Tech 2020

yritysespooli 4.11.2020

20

20



Juha Sallinen
konsultti, eMBA,
insinööri

www.gdprtech.com

juha@gdprtech.com
+358-40 5666 900

 www.gdprtech.com

© Copyright GDPR Tech 2020

21