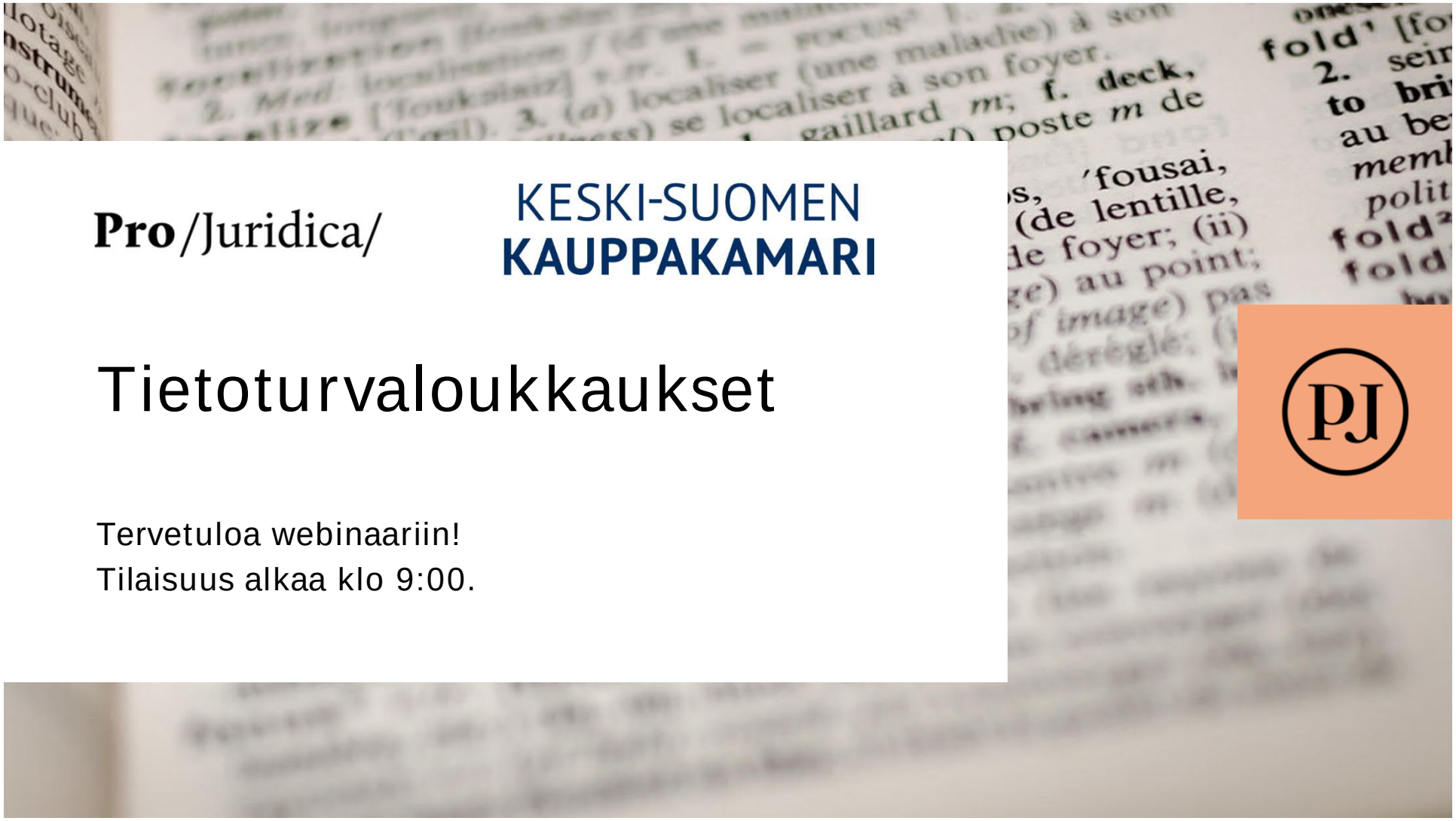
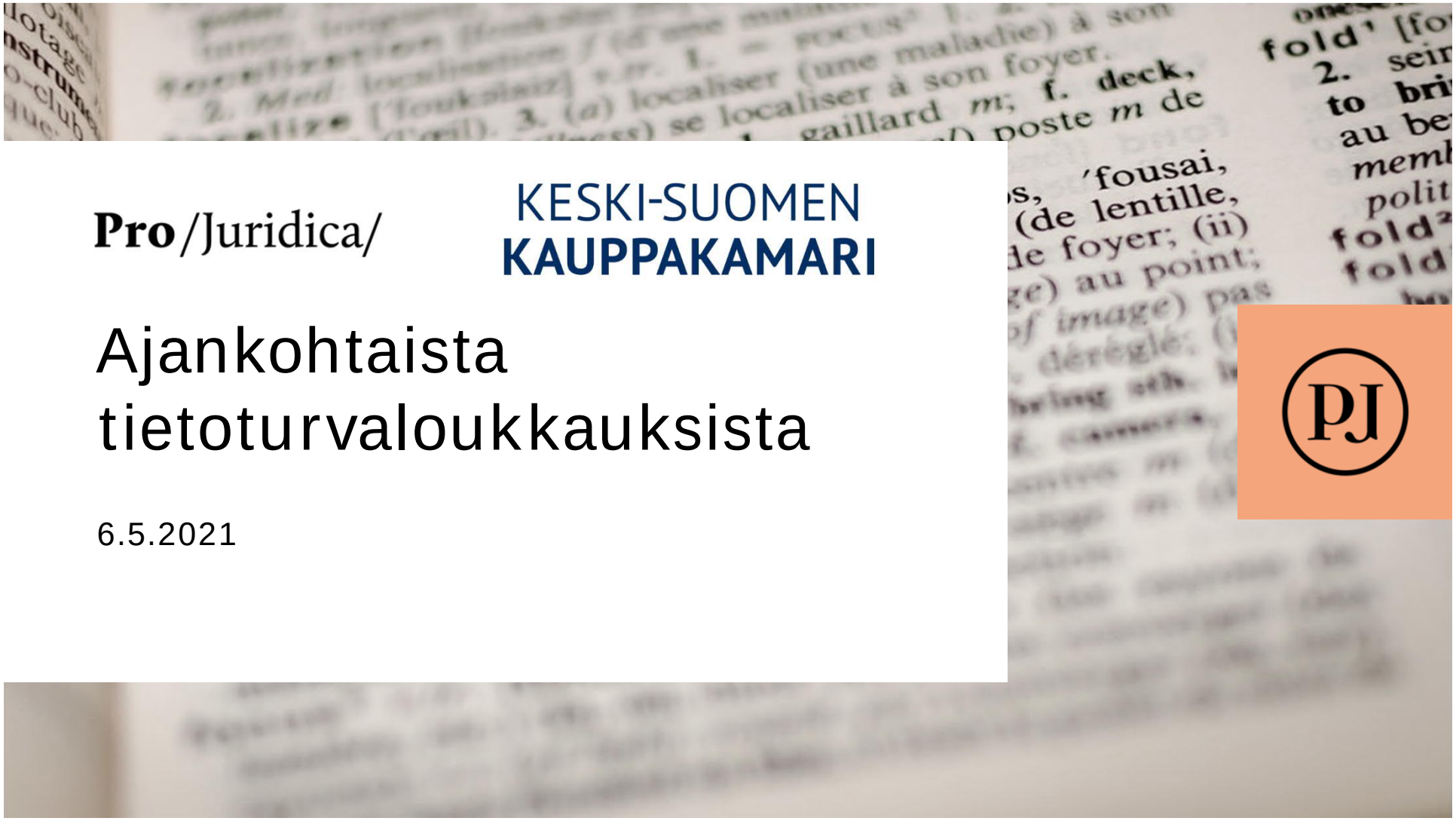


Pro/Juridica/

KESKI-SUOMEN KAUPPAKAMARI

Tietoturvaloukkaukset

Tervetuloa webinaariin!
Tilaisuus alkaa klo 9:00.



Pro/Juridica/

KESKI-SUOMEN KAUPPAKAMARI

Ajankohtaista tietoturvaloukkauksista

6.5.2021

Esityksen rakenne

I Tietoturvaloukkausten tunnistaminen ja niihin reagointi

II Käytännön kokemuksia

Tietoturvaloukkausten tunnistaminen ja niihin reagointi

Mikä on henkilötietojen tietoturvaloukkaus?

- Rekisterinpitäjän vastuulla olevien henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoutuminen, häviäminen, muuttaminen, luvaton luovuttaminen tai lainvastainen pääsy tietoihin

- Rekisterinpitäjän on tunnistettava poikkeamatilanne ja arvioitava ripeästi jatkotoimet!

Tietoturvaloukkaus voi olla esimerkiksi:

- varastettu tai väärään paikkaan unohtunut tietokone/puhelin/muistitikku
- sähköpostin lähettäminen väärälle vastaanottajalle
- arkaluonteisten henkilötietojen vuotaminen
- haittaohjelmatartunta
- hakkerointi
- verkkohyökkäys
- virhe verkkopalvelussa
- suoramarkkinointisähköpostiviesti lähetetään ”vastaanottaja”- tai ”kopio”-kentissä

Siinä missä kaikki
henkilötietojen tietoturvaloukkaukset ovat
tietoturvaongelmia,
kaikki tietoturvaongelmat eivät ole
henkilötietojen tietoturvaloukkauksia.

Mitä rekisterinpitäjän tulee tehdä tultuaan tietoiseksi tietoturvaloukkauksesta?

Riskiarvio toimenpiteiden lähtökohtana

- Minkä tasoinen riski tietoturvaloukkauksesta aiheutuu sen kohteena oleville henkilöille?
  - Ei aiheudu riskiä
  - Aiheutuu riski
  - Aiheutuu korkea riski
- Riskin taso määrittää ne toimenpiteet, joihin rekisterinpitäjän on ryhdyttävä
  - Dokumentointi
  - Ilmoitus valvontaviranomaiselle
  - Ilmoitus rekisteröidyille

Miten tietoturvaloukkaukseen tulee reagoida?

Ilmoittaminen valvontaviranomaiselle (1/2)

- Pakollista, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille

  → paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä

- Ilman aiheetonta viivytystä

- Mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta toimivaltaiselle valvontaviranomaiselle

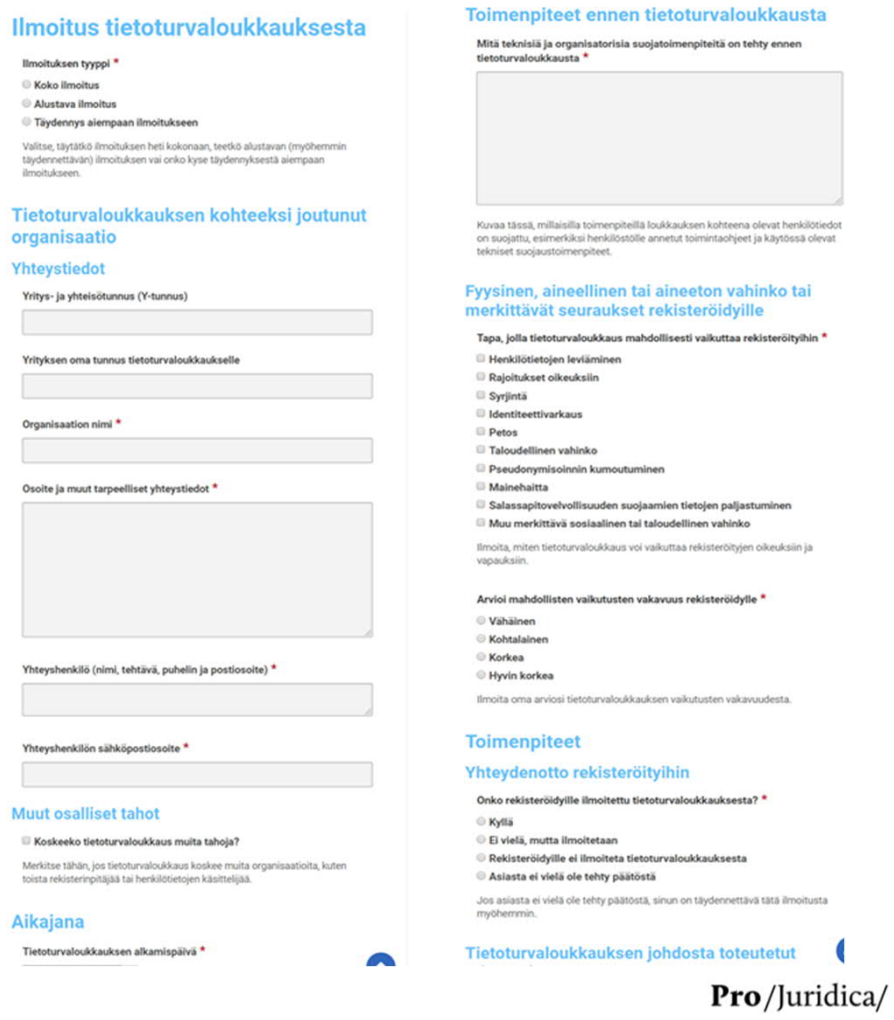
- *Milloin loukkaus on tullut ilmi*? → kohtuullinen varmuus

Ilmoittaminen valvontaviranomaiselle (2/2)

- Koko ilmoitus/alustava ilmoitus/täydennys aiempaan
- Käsittelijä ilmoittaa rekisterinpitäjälle, vrt. DPA:t
- Dokumentointi!

ViranomaisIlmoituksen sisältö

https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta



Ilmoitus tietoturvaloukkauksesta

Ilmoituksen tyyppi *
- Koko ilmoitus
- Alustava ilmoitus
- Täydennys aiempaan ilmoitukseen

Valitse, täytätkö ilmoituksen heti kokonaan, teetkö alustavan (myöhemmin täydennettävän) ilmoituksen vai onko kyse täydennyksestä aiempaan ilmoitukseen.

Tietoturvaloukkauksen kohteeksi joutunut organisaatio

Yhteystiedot

Yritys- ja yhteisötunnus (Y-tunnus)

Yrityksen oma tunnus tietoturvaloukkaukselle

Organisaation nimi *

Osoite ja muut tarpeelliset yhteystiedot *

Yhteyshenkilö (nimi, tehtävä, puhelin ja postiosoite) *

Yhteyshenkilön sähköpostiosoite *

Muut osalliset tahot

Koskeeko tietoturvaloukkaus muita tahoja?

Merkitse tähän, jos tietoturvaloukkaus koskee muita organisaatioita, kuten toista rekisterinpitäjää tai henkilötietojen käsittelijää.

Aikajana

Tietoturvaloukkauksen alkamispäivä *

Toimenpiteet ennen tietoturvaloukkausta

Mitä teknisiä ja organisatorisia suojatoimenpiteitä on tehty ennen tietoturvaloukkausta *

Kuvaa tässä, millaisilla toimenpiteillä loukkauksen kohteena olevat henkilötiedot on suojattu, esimerkiksi henkilöstölle annetut toimintaohjeet ja käytössä olevat tekniset suojaustoimenpiteet.

Fyysinen, aineellinen tai aineeton vahinko tai merkittävät seuraukset rekisteröidyille

Tapa, jolla tietoturvaloukkaus mahdollisesti vaikuttaa rekisteröityihin *
- Henkilötietojen leviäminen
- Rajoitukset oikeuksiin
- Syrjintä
- Identiteettivarkaus
- Petos
- Taloudellinen vahinko
- Pseudonymisoinnin kumoutuminen
- Mainehaitta
- Salassapitovelvollisuuden suojaamien tietojen paljastuminen
- Muu merkittävä sosiaalinen tai taloudellinen vahinko

Ilmoita, miten tietoturvaloukkaus voi vaikuttaa rekisteröityjen oikeuksiin ja vapauksiin.

Arvioi mahdollisten vaikutusten vakavuus rekisteröidyille *
- Vähäinen
- Kohtalainen
- Korkea
- Hyvin korkea

Ilmoita oma arviosi tietoturvaloukkauksen vaikutusten vakavuudesta.

Toimenpiteet

Yhteydenotto rekisteröityihin

Onko rekisteröidyille ilmoitettu tietoturvaloukkauksesta? *
- Kyllä
- Ei vielä, mutta ilmoitetaan
- Rekisteröidyille ei ilmoiteta tietoturvaloukkauksesta
- Asiasta ei vielä ole tehty päätöstä

Jos asiasta ei vielä ole tehty päätöstä, sinun on täydennettävä tätä ilmoitusta myöhemmin.

Tietoturvaloukkauksen johdosta toteutetut

Pro/Juridica/

Esimerkkejä tilanteista, jolloin viranomaiselle ei tarvitse ilmoittaa

- Tiedot ovat jo julkisesti saatavilla eikä ko. tietojen vuotaminen rekisterinpitäjän järjestelmästä todennäköisesti enää aiheuta lisää riskiä rekisteröidyille.

- Henkilötietojen tallennusväline on joutunut vääriin käsiin, mutta data on koko ajan ollut salattuna niin, ettei ulkopuolinen voi ottaa siitä selvää, ja rekisterinpitäjällä on datasta kopio.

- Tapauskohtainen arviointi!

Ilmoittaminen rekisteröidylle

- Kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin yksilöiden oikeuksille ja vapauksille (vrt. ”voi aiheutua riski”)

- Ilman aiheetonta viivytystä

Milloin kyseessä on rekisteröidylle aiheutuva korkea riski?

- Korkea riski on olemassa, jos tietoturvaloukkaus voi aiheuttaa fyysisiä, aineellisia tai aineettomia vahinkoja rekisteröidylle
- Yleisiä vahinkoja korkean riskin tapauksissa ovat syrjintä, petos tai taloudellinen vahinko
- Jos tietoturvaloukkaukseen liittyy henkilötietoja, jotka koskevat ns. erityisiä henkilötietoryhmiä, vahinkojen aiheutumista on pidettävä todennäköisenä.

Esimerkkejä ilmoitustilanteista

- **Esimerkki 1.** Rekisterinpitäjä ylläpitää verkkopalvelua. Palveluun tehdyn verkkohyökkäyksen seurauksena henkilöiden henkilötietoja varastetaan. Rekisterinpitäjällä on asiakkaita vain yhdessä jäsenvaltiossa. // Kyllä, ilmoitetaan valvontaviranomaiselle, jos henkilöille todennäköisesti aiheutuu seurauksia.// Kyllä, ilmoitetaan henkilöille kohteena olleiden henkilötietojen luonteesta riippuen ja jos henkilöille todennäköisesti aiheutuvien seurausten vakavuus on suuri.

- **Esimerkki 2.** Rekisterinpitäjään kohdistuu kiristysohjelmahyökkäys, jonka seurauksena kaikki tiedot salataan. Varmuuskopioita ei ole, eikä tietoja voida palauttaa. Tutkinnassa käy ilmi, että kiristysohjelma ainoastaan salasi tiedot eikä järjestelmässä ollut muita haittaohjelmia // Kyllä, ilmoitetaan valvontaviranomaiselle, jos henkilöille todennäköisesti aiheutuu seurauksia, koska käytettävyys on hävinnyt. // Kyllä, ilmoitetaan henkilöille kohteena olleiden henkilötietojen luonteesta ja mahdollisesta tietojen käytettävyyden häviämisestä sekä muista todennäköisistä seurauksista riippuen.
  - Jos saatavilla oli varmuuskopio ja tiedot pystyttiin palauttamaan nopeasti, turvapoikkeamasta ei tarvitse ilmoittaa valvontaviranomaiselle tai henkilöille, koska käytettävyys tai luottamuksellisuus ei hävinnyt pysyvästi. Jos valvontaviranomainen kuitenkin saa turvapoikkeaman tietoonsa muilla keinoin, se voi harkita tutkintaa arvioidakseen 32 artiklan laajempien turvallisuusvaatimusten noudattamista.

Esimerkkejä ilmoitustilanteista

- **Esimerkki 3.** Sairaalan potilastiedot ovat poissa käytöstä 30 tunnin ajan verkkohyökkäyksen vuoksi. // Kyllä, sairaalalla on velvollisuus ilmoittaa tästä valvontaviranomaiselle, koska potilaiden hyvinvoinnille ja yksityisyydensuojalle saattaa aiheutua korkea riski. // Kyllä, kohteena oleville henkilöille ilmoitetaan.

- **Esimerkki 4.** Suoramarkkinointisähköpostiviesti lähetetään ”vastaanottaja”- tai ”kopio”-kentissä oleville vastaanottajille, jolloin kaikki vastaanottajat voivat nähdä muiden vastaanottajien sähköpostiosoitteet. // Kyllä, valvontaviranomaiselle ilmoittaminen saattaa olla pakollista, jos tämä vaikuttaa suureen määrään henkilöitä, jos paljastetaan arkaluonteisia tietoja (esim. psykoterapeutin postituslista) tai jos muut tekijät aiheuttavat korkeita riskejä (sähköpostiviesti sisältää esim. salasanoja). // Kyllä, ilmoitetaan henkilöille, henkilötietojen laajuudesta ja tyypistä sekä mahdollisten seurausten vakavuudesta riippuen.
  - Ilmoittaminen ei ehkä ole tarpeen, jos arkaluonteisia tietoja ei paljastu ja jos paljastuneita sähköpostiosoitteita on vain vähän.

Milloin ilmoitusta rekisteröidylle ei vaadita?

Ilmoitusta rekisteröidylle ei vaadita, mikäli jokin kohta seuraavista täyttyy:

1) rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet

2) rekisterinpitäjä on tehnyt jatkotoimenpiteitä varmistaen, ettei rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski enää todennäköisesti toteudu; tai

3) ilmoittaminen vaatisi kohtuutonta vaivaa.

- Dokumentointi!

Tietosuojaviranomaisen ratkaisukäytäntöä tietoturvaloukkauksista - Suomi ja EU

Ajankohtaista tietosuojaviranomaisten ratkaisukäytäntöä

- Psykoterapiakeskus Vastaamon tietomurto 2018-2019
- Espanja 15.3.2021
- Belgia 22.1.2021
- Puola 11.1.2021
- Puola 5.1.2021
- Irlanti 15.12.2020
- Tanska 30.6.2020

Vastaamon tietomurto 2018-2019

- Tietomurron seurauksena noin 33 000 asiakkaan henkilö- ja potilastiedot varastettiin sekä näitä tietoja julkaistiin Tor-verkossa.

- Aluksi Vastaamo ilmoitti tapahtuneesta tietomurrosta ainoastaan verkkosivuillaan, jonka jälkeen apulaistietosuojavaltuutettu määräsi Vastaamon ilmoittamaan rekisteröidyille tietoturvaloukkauksesta henkilökohtaisesti ilman aiheetonta viivytystä.

- Vastaamon tietoturvan ja tietosuojan taso ei ollut riittävä erittäin arkaluontoisten henkilötietojen käsittelyyn. Asian selvitys kesken.

Espanja, 15.3.2021, sakko 600 000 euroa

- Espanjalaiseen lentoyhtiöön kohdistui vakava tietomurto, jonka seurauksena ulkopuoliset henkilöt pääsivät käsiksi noin 489 000 henkilön yhteystietoihin ja pankkitileihin. Lentoyhtiö ilmoitti tietoturvaloukkauksesta tietosuojaviranomaiselle vasta 41 päivän kuluttua tapahtuneesta tietomurrosta. Tietoturvaloukkauksen vakavuutta lisäsi se, että tapaus ei rajoittunut paikallisesti Espanjan alueelle, vaan se vaikutti suureen määrään ihmisiä myös Espanjan ulkopuolella. Tuhansien ihmisien arkaluonteiset pankki- ja taloustiedot olivat vaarassa.

- Tapauksessa on kyse riittämättömistä teknisistä ja organisatorisista toimenpiteistä tietoturvan varmistamiseksi. Lentoyhtiön toiminta rikkoi tietosuoja-asetuksen artikloja 32 (1) ja 33.

Belgia, 22.1.2021, sakko 25 000 euroa

- Matkapuhelinoperaattori oli antanut yksityishenkilön puhelinnumeron luvatta kolmannen osapuolen käyttöön, jonka seurauksena yksityishenkilö menetti pääsyn puhelimeensa. Kolmannen osapuolen oli mahdollista päästä yksityishenkilön erilaisiin henkilötietoihin, kuten puheluhistoriaan ja numeroon liittyvien erilaisten palveluiden tileihin (esim. Paypal, WhatsApp ja Facebook) 16.-19. syyskuuta 2019 välisenä aikana.

- Tapauksessa on kyse riittämättömistä teknisistä ja organisatorisista toimenpiteistä tietoturvan varmistamiseksi. Matkapuhelinoperaattorin toiminta rikkoi tietosuoja-asetuksen artikloja 5, 24, 32, 33 ja 34.

Puola, 11.1.2021, sakko 30 000 euroa

- Puolan tietosuojaviranomainen määräsi puolalaiselle sähköteollisuusyritys Enea S.A:lle 30 000 euron sakon, sillä se ei rekisterinpitäjänä ollut ilmoittanut tapahtuneesta henkilötietojen tietoturvaloukkauksesta. Rikkomuksessa oli kyse salaamattoman sähköpostin lähettämisestä, joka sisälsi useiden satojen yksityishenkilöiden henkilötietoja koskevan liitteen. Sähköpostin lähettäjä oli rangaistuksen kohteena olevan yrityksen työntekijä. Tietosuojaviranomainen sai tiedon tietoturvaloukkauksesta henkilöltä, josta oli tullut luvaton henkilötietojen vastaanottaja. Yritys ei itse tiedottanut tietoturvaloukkauksesta.

- Tapauksessa on kyse tietoturvaloukkauksia koskevien ilmoitusvelvoitteiden riittämättömästä täyttämisestä. Yrityksen toiminta rikkoi tietosuoja-asetuksen artiklaa 33.

Puola, 5.1.2021, sakko 5500 euroa

- Sleesian lääketieteellisessä yliopistossa videoneuvottelujen muodossa pidettyjen tenttien aikana järjestettiin myös opiskelijoiden tunnistaminen. Tentin suorittamisen jälkeen tenttien tallenteet ja sisältö olivat tenttijöiden lisäksi myös muiden järjestelmään pääsevien käytettävissä. Lisäksi kuka tahansa ulkopuolinen pääsi suoran linkin kautta tentteihin kirjattuihin tietoihin sekä opiskelijoiden tunnistautumisen aikana esittämiin tietoihin. Yliopisto ei ilmoittanut tietomurrosta tietosuojaviranomaiselle eikä rekisteröidyille.

- Tapauksessa on kyse tietoturvaloukkauksia koskevien ilmoitusvelvoitteiden riittämättömästä täyttämisestä. Yliopiston toiminta rikkoi tietosuoja-asetuksen artikloja 33 (1) ja 34 (1).

Irlanti, 15.12.2020, sakko 450 000 euroa

- Twitter International Company ei ilmoittanut tietosuojaviranomaiselle ajoissa tietomurrosta eikä dokumentoinut tietomurtoa asianmukaisesti. Tietomurto koski Twitter-käyttäjien käyttäjäviestien yksityisyysasetuksia, jossa käyttäjillä on mahdollisuus asettaa viestiensä näkyvyys yksityiseksi tai julkiseksi. Yksityisiä viestejä voivat nähdä vain kyseisen käyttäjäprofiilin tilaajat, kun taas julkiset viestit ovat nähtävissä kaikille. Twitterin Android-sovelluksen ohjelmointivirhe johti siihen, että yksityiset viestit näkyivät kaikille. Twitter ei täyttänyt asianmukaisesti raportointi- ja dokumentointivelvoitteitaan, sillä Twitterin lakitiimi sai tiedon virheestä 2. tammikuuta 2019, mutta ilmoitti vasta 8. tammikuuta asiasta tietosuojaviranomaiselle.

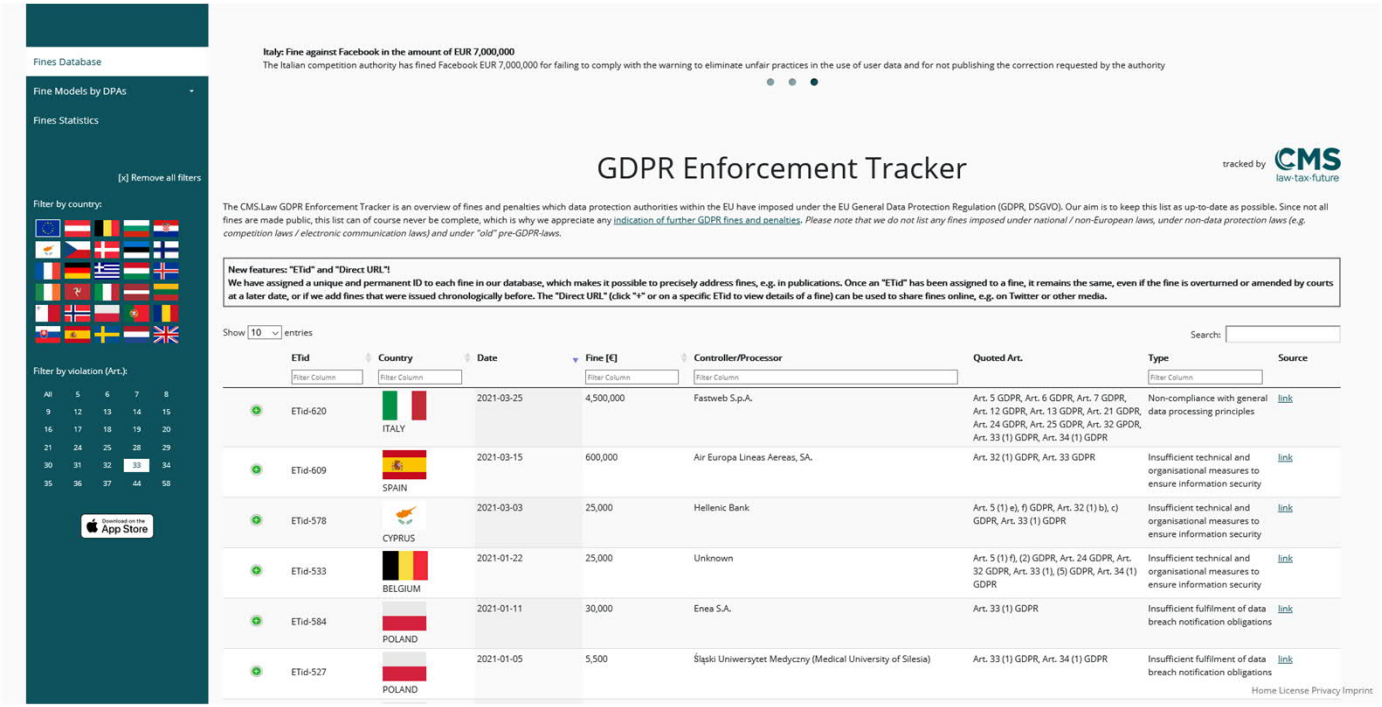
- Tapauksessa on kyse tietoturvaloukkauksia koskevien ilmoitusvelvoitteiden riittämättömästä täyttämisestä. Twitterin toiminta rikkoi tietosuoja-asetuksen artiklaa 33.

Tanska, 30.6.2020, sakko 6700 euroa

- Tanskalaisen Lejren kunnan lapsi- ja nuorisokeskus oli säännöllisesti ladannut tapaamista käsitteleviin kokouspöytäkirjoihin erityisen arkaluontoisia henkilötietoja. Tiedot oli ladattu kunnan henkilöstöportaaliin, johon oli pääsy Lejren kunnan työntekijöillä, riippumatta siitä, työskentelivätkö kyseiset työntekijät näitä tapauksia koskevien asioiden parissa vai eivät. Kunnan tietosuojaviranomainen kiisti laiminlyöneensä ilmoitusvelvollisuuden.

- Tapauksessa on kyse yleisten tietojenkäsittelyperiaatteiden noudattamatta jättämisestä. Lejren kunnan toiminta rikkoi tietosuoja-asetuksen artikloja 5, 6, 33 ja 34.

Lähde


Fines Database
Fine Models by DPAs
Fines Statistics
[x] Remove all filters
Filter by country:
Filter by violation (Art.):
Download on the App Store
Italy: Fine against Facebook in the amount of EUR 7,000,000
The Italian competition authority has fined Facebook EUR 7,000,000 for failing to comply with the warning to eliminate unfair practices in the use of user data and for not publishing the correction requested by the authority
GDPR Enforcement Tracker
tracked by CMS law-tax-future
The CMS.Law GDPR Enforcement Tracker is an overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation (GDPR, DSGVO). Our aim is to keep this list as up-to-date as possible. Since not all fines are made public, this list can of course never be complete, which is why we appreciate any indication of further GDPR fines and penalties. Please note that we do not list any fines imposed under national / non-European laws, under non-data protection laws (e.g. competition laws / electronic communication laws) and under "old" pre-GDPR-laws.
New features: "ETid" and "Direct URL"!
We have assigned a unique and permanent ID to each fine in our database, which makes it possible to precisely address fines, e.g. in publications. Once an "ETid" has been assigned to a fine, it remains the same, even if the fine is overturned or amended by courts at a later date, or if we add fines that were issued chronologically before. The "Direct URL" (click "+" or on a specific ETid to view details of a fine) can be used to share fines online, e.g. on Twitter or other media.
Show 10 entries
Search:
ETid
Country
Date
Fine [€]
Controller/Processor
Quoted Art.
Type
Source
ETid-620
ITALY
2021-03-25
4,500,000
Fastweb S.p.A.
Art. 5 GDPR, Art. 6 GDPR, Art. 7 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 21 GDPR, Art. 24 GDPR, Art. 25 GDPR, Art. 32 GPDR, Art. 33 (1) GDPR, Art. 34 (1) GDPR
Non-compliance with general data processing principles
link
ETid-609
SPAIN
2021-03-15
600,000
Air Europa Lineas Aereas, SA.
Art. 32 (1) GDPR, Art. 33 GDPR
Insufficient technical and organisational measures to ensure information security
link
ETid-578
CYPRUS
2021-03-03
25,000
Hellenic Bank
Art. 5 (1) e), f) GDPR, Art. 32 (1) b), c) GDPR, Art. 33 (1) GDPR
Insufficient technical and organisational measures to ensure information security
link
ETid-533
BELGIUM
2021-01-22
25,000
Unknown
Art. 5 (1) f), (2) GDPR, Art. 24 GDPR, Art. 32 GDPR, Art. 33 (1), (5) GDPR, Art. 34 (1) GDPR
Insufficient technical and organisational measures to ensure information security
link
ETid-584
POLAND
2021-01-11
30,000
Enea S.A.
Art. 33 (1) GDPR
Insufficient fulfilment of data breach notification obligations
link
ETid-527
POLAND
2021-01-05
5,500
Śląski Uniwersytet Medyczny (Medical University of Silesia)
Art. 33 (1) GDPR, Art. 34 (1) GDPR
Insufficient fulfilment of data breach notification obligations
link
Home License Privacy Imprint

Miten varautua?

Ennakointi

- Ennakolta varmistauduttava, että tietoturvaloukkaukset tulevat nopeasti ilmi.
  - Sisäiset prosessit loukkauksen tunnistamiseksi ja arvioimiseksi.
- Roolit, vastuunjako, avainhenkilöiden yhteystiedot (tekninen tuki, viestintä, lakiapu jne.)
- ”Harjoitukset”
- Tietoturva-auditoinnit
- Henkilöstön kouluttaminen
- Sopimukset käsittelijöiden kanssa

Kiitos!

Aino-Kaisu
Renko

Asianajaja, osakas, CIPP/E, HHJ

+358 50 307 4456

aino-kaisu.renko@projuridica.fi