Tietosuoja on näyteikkuna yrityksen vastuulliseen toimintaan

Mikko Eloholma
Digiosaamisen vauhdittaja
TIEKE Tietoyhteiskunnan kehittämiskeskus ry

DiyKS – Digiosaavat yritykset ja yhteisöt Keski-Suomessa

6.9.2023

TIEKE

Tietosuoja on näyteikkuna yrityksen vastuulliseen toimintaan

Mikko Eloholma, TIEKE

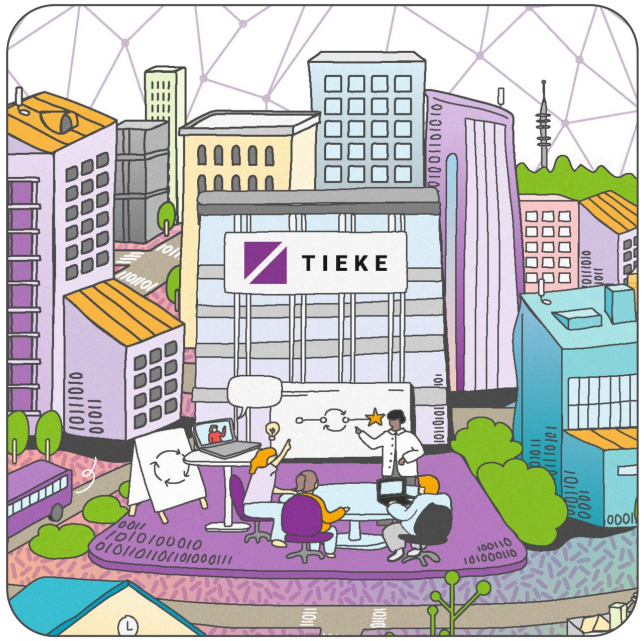
Webinaarissa perehdymme tietosuojan perusteisiin ja käsittelemme mm. seuraavia aiheita.

- Mitä tietosuojalla tarkoitetaan?
- Mitä henkilötietojen käsittelystä tulee kertoa, ja miksi?
- Vinkkejä tietosuojaselosteen laadintaan

Miksi tietosuojasta huolehditaan?

Tietosuojan peruskäsitteitä

Tietosuoja ja tietoturva
Tietosuojalainsäädäntö ja GDPR
Henkilötiedot ja niiden käsittely
Rekisteröity ja rekisterinpitäjä



Tietosuoja ja tietoturva

- **Tietosuoja** on perusoikeus, joka turvaa yksilön oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä.

- **Tietoturva** viittaa yleensä tietojen turvaamisen keinoihin. Voidaan ajatella, että tietoturva on myös tietosuojan toteuttamisen keino.

Tietosuoja ja tietoturva

Miten tietosuojasta huolehditaan?

- Riskien arviointi – minkälaisia riskejä yksilöihin kohdistuu henkilötietojen käsittelystä?
- Käsittelyn tarkoitusten ja perusteiden tunnistaminen ja dokumentointi
- Asiakkaiden ja muiden osallisten informointi esimerkiksi tietosuojaselosteella

Miten tietoturvasta huolehditaan?

- Käyttöoikeuksien hallinta yrityksen sisällä – tiedot ovat saatavilla vain niitä todella tarvitseville, ja käyttöoikeuksia myös poistetaan prosessien mukaisesti
- Laitteiden ja palvelimien pitäminen suojattuina
- Työntekijöiden perehdytys ohjeistusten noudattamiseen (ohjelmien päivitykset, vahvat salasanat jne.)

Tärkeitä tietosuojan käsitteitä

Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön, kuten esimerkiksi nimi, kotiosoite, auton rekisterinumero, valokuva henkilön kasvoista.

Henkilötietojen käsittely tarkoittaa esimerkiksi henkilötietojen keräämistä, säilyttämistä, käyttöä, siirtämistä ja luovuttamista, esimerkiksi digitaalisesti tai paperimuodossa.

Rekisteröity on se henkilö (esim. asiakas tai yhdistyksen jäsen), jonka henkilötietoja käsitellään.

Rekisterinpitäjä on ihminen tai organisaatio, joka määrittelee, mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään. Rekisterinpitäjä voi olla esimerkiksi jäsenistään tietoja keräävä yhdistys, potilastietoja käsittelevä sairaala, verkkokauppa tai sosiaalisen median palvelu.

EU:n yleinen tietosuoja-asetus (GDPR)

- General Data Protection Regulation.
- Henkilötietojen käsittelyä sääntelevä laki, jota alettiin soveltaa kaikissa EU-maissa keväällä 2018.

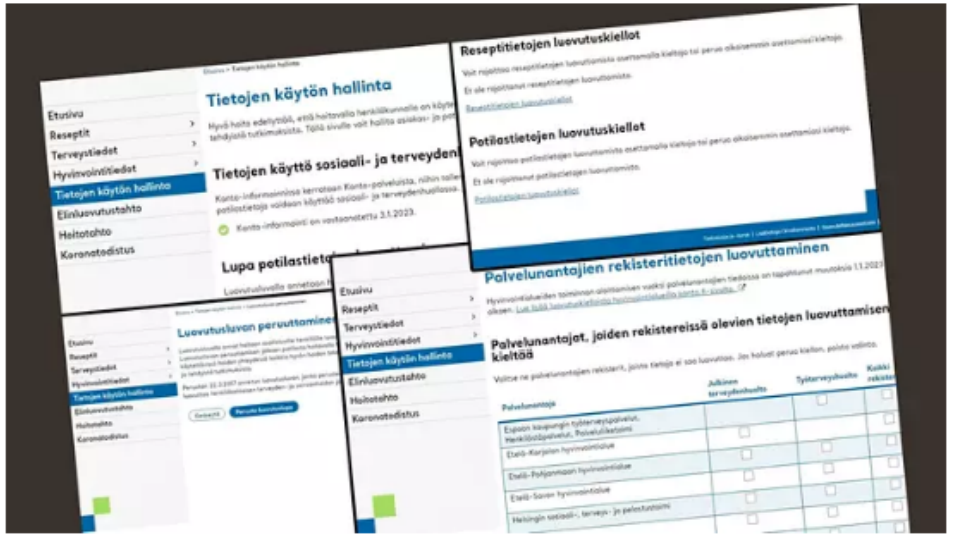
Henkilötietojen käsittelyn mahdollisia riskejä

- Terveystietojen käsittely liian laajasti, tietojen vuotaminen
- Sijaintitietojen käsittely ilman erillistä suostumusta
- Käyttäjien profilointi mainoksien kohdentamiseksi ilman läpinäkyvyyttä
- Asiakastietojen säilyttäminen ilman määriteltyä säilytysaikaa.

Kotimaa | Tietosuoja

Valtaosa suomalaisista jakaa terveystietojaan Kanta-palvelussa rajattomasti

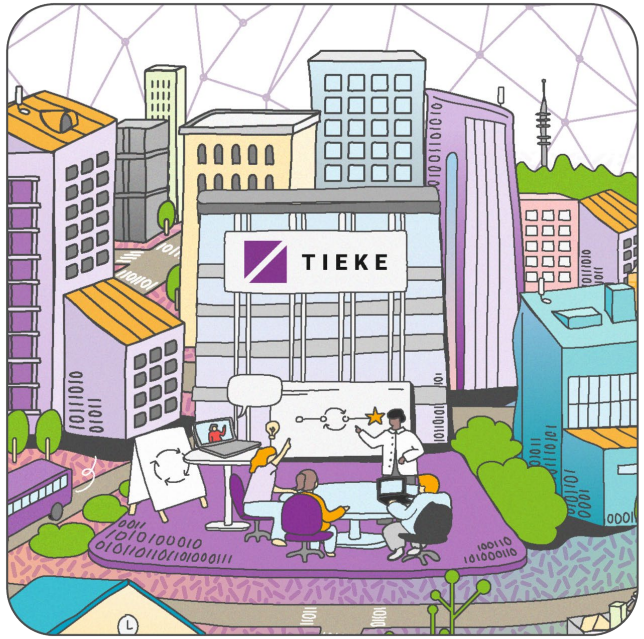
Omien terveystietojensa jakamista voi rajoittaa paitsi vastaanottojen yhteydessä myös itsenäisesti Omakannassa. HS kertoo, miten asetuksia muutetaan.



Omakannassa voi säätää hyvin tarkkaan, mitä terveystietoja jakaa ja mille tahoille.
KUVA: OMAKANTA

Mika Jyrävä HS
10.4. 14:53 | Päivitetty 12.4. 14:31

Miksi tietosuojasta tulee kertoa niille, joiden henkilötietoja käsitellään?



Miksi tietosuojasta tulee ja kannattaa kertoa niille, joiden henkilötietoja käsitellään?

- Lainsäädännön noudattaminen
- Viestitään esimerkiksi asiakkaille, potentiaalisille asiakkaille ja yhdistyksen jäsenille siitä, miten heidän henkilötietojen suojaa ja yksityisyyttään kunnioitetaan.
- Luodaan luottamusta omaan organisaatioon. Näytetään, että omassa organisaatiossa osataan toimia vastuullisesti myös laajemmin.

Luottamus datatalouden vaatimuksena

> Vastanneista 42 % on täysin tai samaa mieltä sen kanssa, että luottamuksen puute palvelutarjoajia kohtaan estää heitä käyttämästä digitaalisia palveluita. Osuus on suurin Saksassa (48 %) ja pienin Hollannissa (38 %).
>
> **- Sitran reilun datatalouden IHAN-hankkeen selvitys, 2019**

Lähde: Sitra – Oma päätösvalta datan käytössä on ihmisille tärkeää

Näyteikkuna yrityksen vastuullisuuteen?

Mikä mielikuva herää, jos organiaation
tietosuojaselosteen
yhteystiedoissa lukee esimerkiksi:

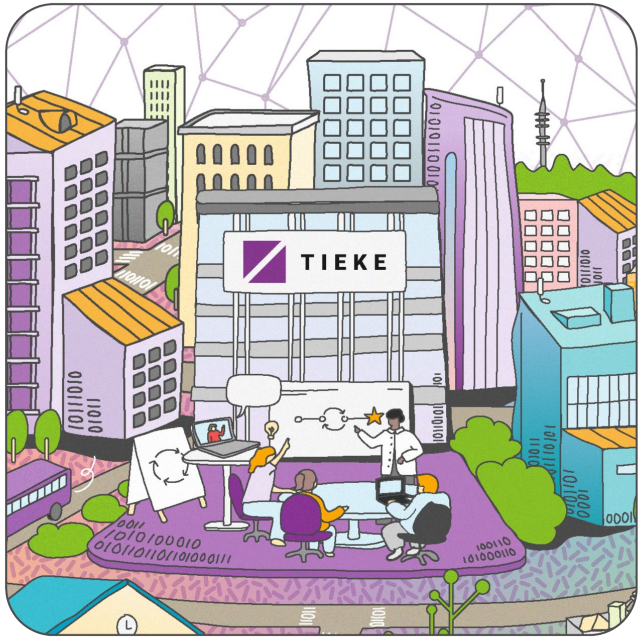
Oy Yritys AB
etunimi.sukunimi@organisaatio.fi

- Luotatko siihen, että organisaatio käsittelee tietojasi huolellisesti?
- Lähtisitkö tilaamaan yritykseltä palvelua, johon liittyy henkilötietojen käsittelyä?

Ajatusharjoitus: Ymmärrätkö asiakkaana sen, miten henkilötetojasi käsitellään?

Miten voisit toimia itse selkeämmin rekisterinpitäjänä?

Vinkkejä tietosuojaselosteen laadintaan



Dokumentointi: lähtökohta tietoturvaan ja tietosuojaan

Jos organisaatio ei ole dokumentoinut sitä, *minkälaista henkilötietoa sillä on, missä järjestelmissä tietoa on, mitä varten tietoa kerätään ja mitkä tahot tietoa käsittelevät*, sen on hyvin vaikeaa huolehtia tietosuojasta ja tietoturvasta riittävällä tasolla.

Dokumentointi: lähtökohta tietoturvaan ja tietosuojaan

Jos organisaatio ei ole dokumentoinut sitä, *minkälaista henkilötietoa sillä on, missä järjestelmissä tietoa on, mitä varten tietoa kerätään ja mitkä tahot tietoa käsittelevät*, sen on hyvin vaikeaa huolehtia tietosuojasta ja tietoturvasta riittävällä tasolla.

- Ilman dokumentointia on vaikeaa myöskään tehdä **tietosuojaselostetta -** tietosuojasta ei voi kertoa asiakkaille, jos ei ole itse käynyt asioita läpi.
- Kun dokumentointi tehdään huolellisesti, huolehditaan samalla myös tietosuojan **osoitusvelvollisuudesta.**

Miten kertoa henkilötietojen käsittelystä?

- Tietosuoja-asetuksessa ei säädetä tietystä muodosta (esim. selosteesta), jolla henkilötietojen käsittelystä tulisi kertoa.

- Tiedot voidaan antaa sähköisessä muodossa esimerkiksi verkkosivuilla. Tieto pitäisi julkaista verkkosivuilla yleisesti tunnetulla nimellä, kuten ”tietosuoja”, ”tietosuojaseloste”, ”yksityisyys” tai ”yksityisyyden suoja”.

- Pääsääntöisesti tiedot on annettava kirjallisesti. Henkilötietojen keräämiseen käytetty väline voi kuitenkin asettaa rajoitteita sille, millä tavalla informaatio voidaan tarjota (esim. kun henkilötietoja kerätään puhelimitse tai näytöttömien laitteiden kautta).

Miten kertoa henkilötietojen käsittelystä?

- Tiedon on oltava tiivistä, läpinäkyvää, ymmärrettävää ja helposti saatavilla.
- Informoinnissa on käytettävä selkeää ja yksinkertaista kieltä. Tämä on erityisen tärkeää, kun informoidaan lapsia.
- Tieto on annettava kirjallisesti ja tapauskohtaisesti sähköisessä muodossa. Jos rekisteröity pyytää, tiedot voidaan antaa myös suullisesti.
- Tiedot on annettava maksutta.

Mitä tulisi ainakin kertoa?

- kuka rekisterinpitäjä on
- mitä tarkoitusta varten henkilötietoja tarvitaan
- kuinka kauan henkilötietoja tarvitaan
- luovutetaanko henkilötietoja eteenpäin tai siirretäänkö niitä ETA-maiden ulkopuolelle
- miten rekisteröity voi käyttää henkilötietoihin liittyviä oikeuksiaan
- rekisteröidyn oikeuksiin ja vapauksiin kohdistuvista riskeistä

Miten edistää läpinäkyvyyttä informoinnissa?

- Voiko yksittäinen pitkä tietosuojaseloste olla läpinäkyvä ja ymmärrettävä?
  - Globaalien suuryritysten selosteet eivät tarjoa välttämättä hyvää esimerkkiä.

- Kuten muussakin toiminnassa, liikkeelle kannattaa lähteä tarpeista:
  - Erilaisten kohderyhmien erottelu (asiakkaat, työntekijät, yhdistyksen jäsenet jne.)
  - Mihin tarkoitukseen ryhmien henkilötietoja oikeastaan tarvitaan?
    Mitä niiden käsittelyllä saavutetaan?
  - Onko kohderyhmällä erityistarpeita (esim. lapset, näkövammaiset)
  - Minkälaisia riskejä henkilötietojen käsittelyyn liittyy?

Linkkejä ja lisätietoa

Tietosuojaapkyrityksille.fi – Kokeile itsearviointiin perustuvaa tietosuojatyökalua!

Tietosuojavaltuutetun toimisto – Ohjesivu informoinnista
https://tietosuoja.fi/rekisteroidyn-informointi

Suomen yrittäjät – Yrittäjän tietosuojaopas
https://www.yrittajat.fi/oppaat/yrittajan-tietosuojaopas/

Tietosuoja.fi – Usein kysyttyä yhdistystoiminnasta ja yhdistysopas
https://tietosuoja.fi/usein-kysyttya-yhdistystoiminta

Keskuskauppakamarin tietosuojaopas
https://kauppakamari.fi/wp-content/uploads/2020/05/tietosuoja-pahkinankuoressa.-tietosuojaopas-yrityksille.verkkoversio.pdf

Jamkin ja Poliisiammattikorkeakoulun CYBERDI-hankkeen digiturvallisuuden tietopankki:
https://www.jamk.fi/fi/Tutkimus-ja-kehitys/projektit/CYBERDI/tietopankki/

Kiitos!

Mikko Eloholma
mikko.eloholma@tieke.fi

DiyKS - Digiosaavat yritykset
ja yhteisöt Keski-Suomessa

TIEKE