TIEKE

Tietosuojan perusteita yrityksille ja yhteisöille

Mikko Eloholma
Digiosaamisen vauhdittaja
TIEKE Tietoyhteiskunnan kehittämiskeskus ry

DiyKS – Digiosaavat yritykset ja yhteisöt Keski-Suomessa

18.04.2023

18.4. klo 15-16 | Webinaari: Tietosuojan perusteita yrityksille ja yhteisöille

Mikko Eloholma
Digiosaamisen vauhdittaja, TIEKE

Webinaarissa perehdymme tietosuojan perusteisiin ja käsittelemme mm. seuraavia aiheita.

- Mitä tietosuojalla tarkoitetaan?
- Tietosuojan ja tietoturvan keskeisimmät riskit
- Yritysten ja yhdistysten roolit GDPR:n näkökulmasta
- Käsittelyn tarkoitusten ja perusteiden tunnistaminen
- Vinkit avoimista materiaaleista ja työkaluista

DiyKS-hankkeen webinaarisarja tietosuojasta ja tietoturvasta

- **18.4. Tietosuojan perusteita yrityksille ja yhteisöille**
- 26.4. Tietoturvan inhimilliset riskit ja ratkaisut

- Syksy 2023: Tietosuoja: läpinäkyvyys, informointi ja tietosuojaseloste
- Syksy 2023: Tietoturva: organisaation riskit ja ratkaisut

Mitä tänään käsitellään?

- Tietosuojalainsäädännön perusteita ja peruskäsitteitä
- Henkilötietojen käsittelyn tunnistaminen ja dokumentointi
- Käsittelyn tarkoituksien ja perusteiden tunnistaminen

Tietosuojan kokonaisuus organisaatiolle

tietosuoja.fi/organisaatiot

ORGANISAATIOILLE

Tunne vastuusi ja rakenna luottamusta

Tästä osiosta löydät tietoa siitä, mitä organisaatioiden on otettava huomioon henkilötietojen käsittelyssä.
Osiossa on tietoa rekisterinpitäjille, henkilötietojen käsittelijöille ja tietosuojavastaaville.

Henkilötietojen käsittely


Tietosuojaperiaatteet


Arvioi käsittelyn riskit ja vaikutukset


Osoita noudattavasi tietosuojasäännöksiä


Kerro käsittelystä rekisteröidylle


Rekisteröidyn oikeudet


Tietosuojavastaavat


Henkilötietojen käsittelijät


Tietoturvaloukkaukset

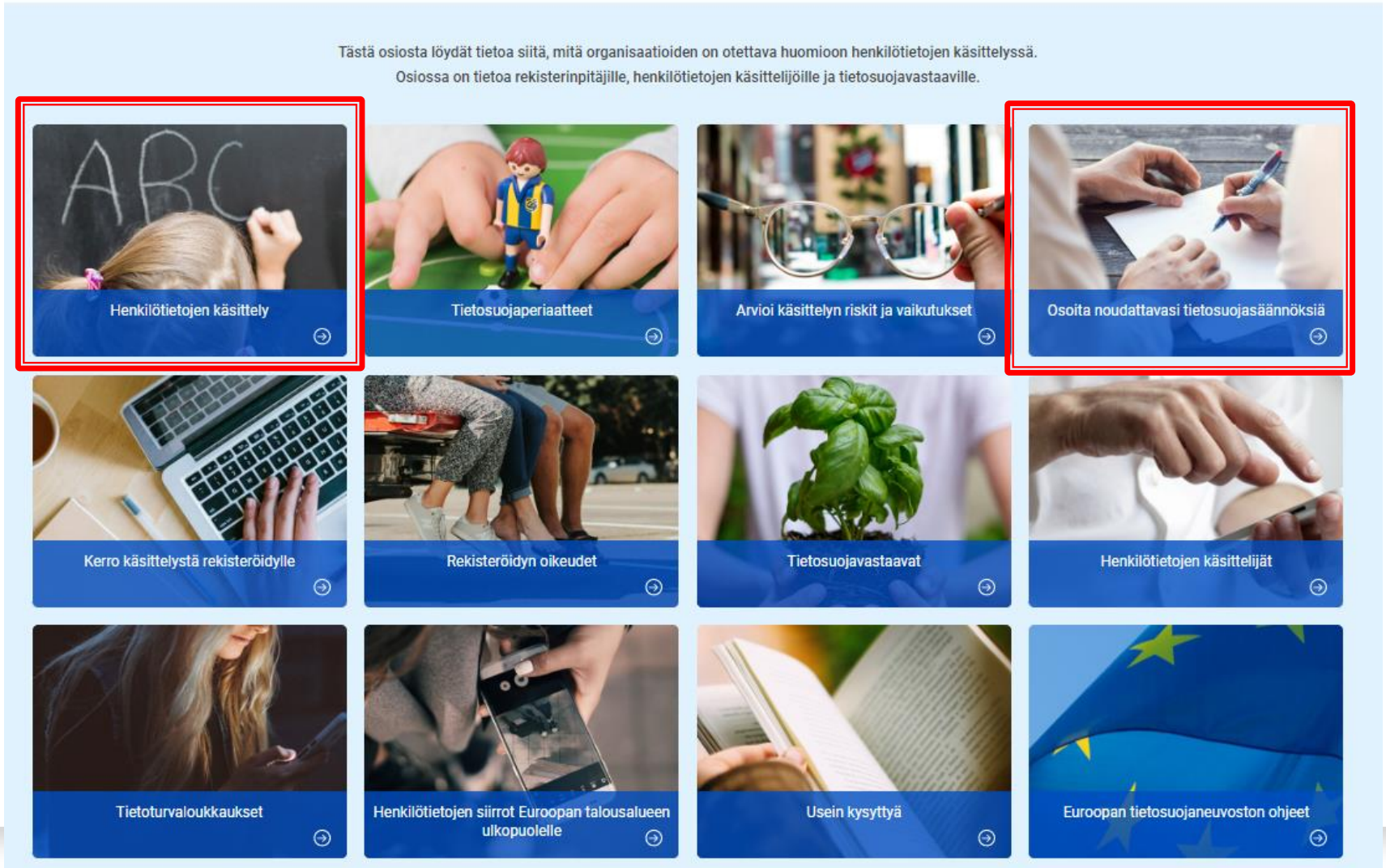

Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle


Usein kysyttyä


Euroopan tietosuojaneuvoston ohjeet

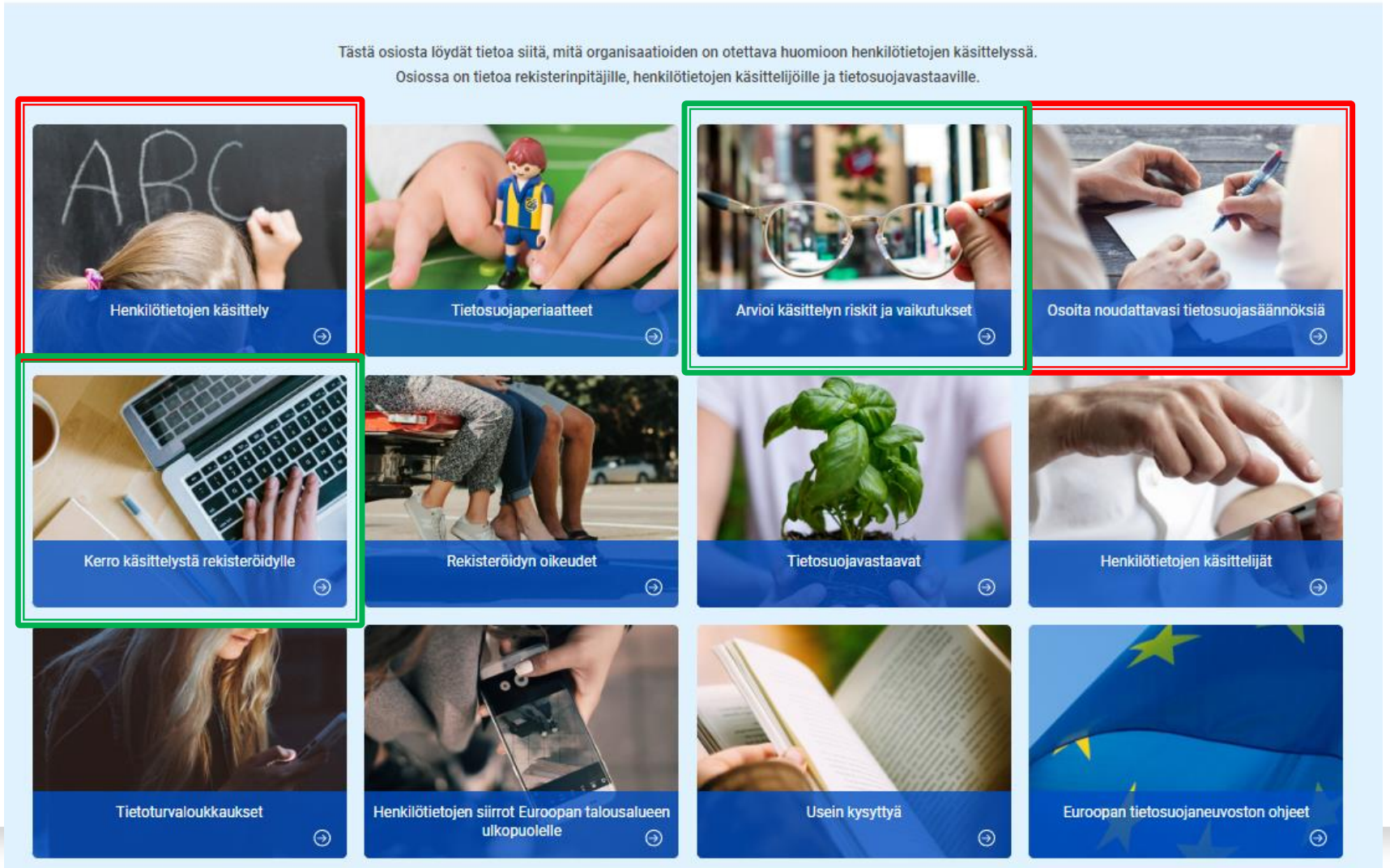
Tietosuojan kokonaisuus organisaatiolle

tietosuoja.fi/organisaatiot



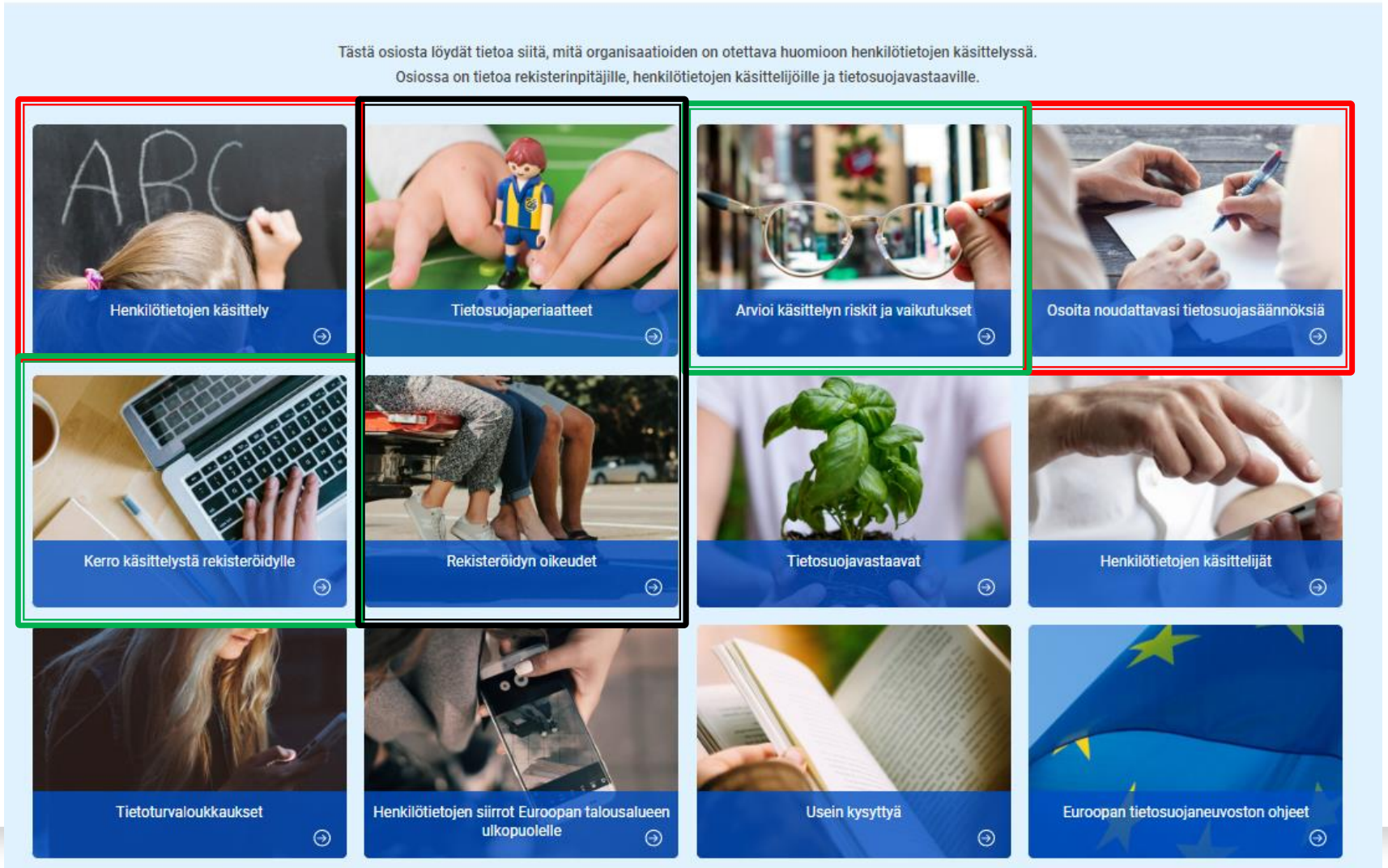
Tietosuojan kokonaisuus organisaatiolle

tietosuoja.fi/organisaatiot



Tietosuojan kokonaisuus organisaatiolle

tietosuoja.fi/organisaatiot



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.)

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

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.

Tärkeitä tietosuojan käsitteitä

- **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.
- **Rekisteröity** on se henkilö (esim. asiakas tai yhdistyksen jäsen), jonka henkilötietoja käsitellään.
- **Henkilötietojen käsittelijä** on taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Henkilötietojen käsittelijä voi olla esimerkiksi ohjelmistopalveluiden tarjoaja.

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.**

Omien käsittelytoimien dokumentointi:
Esimerkki 1: Taulukkomalli

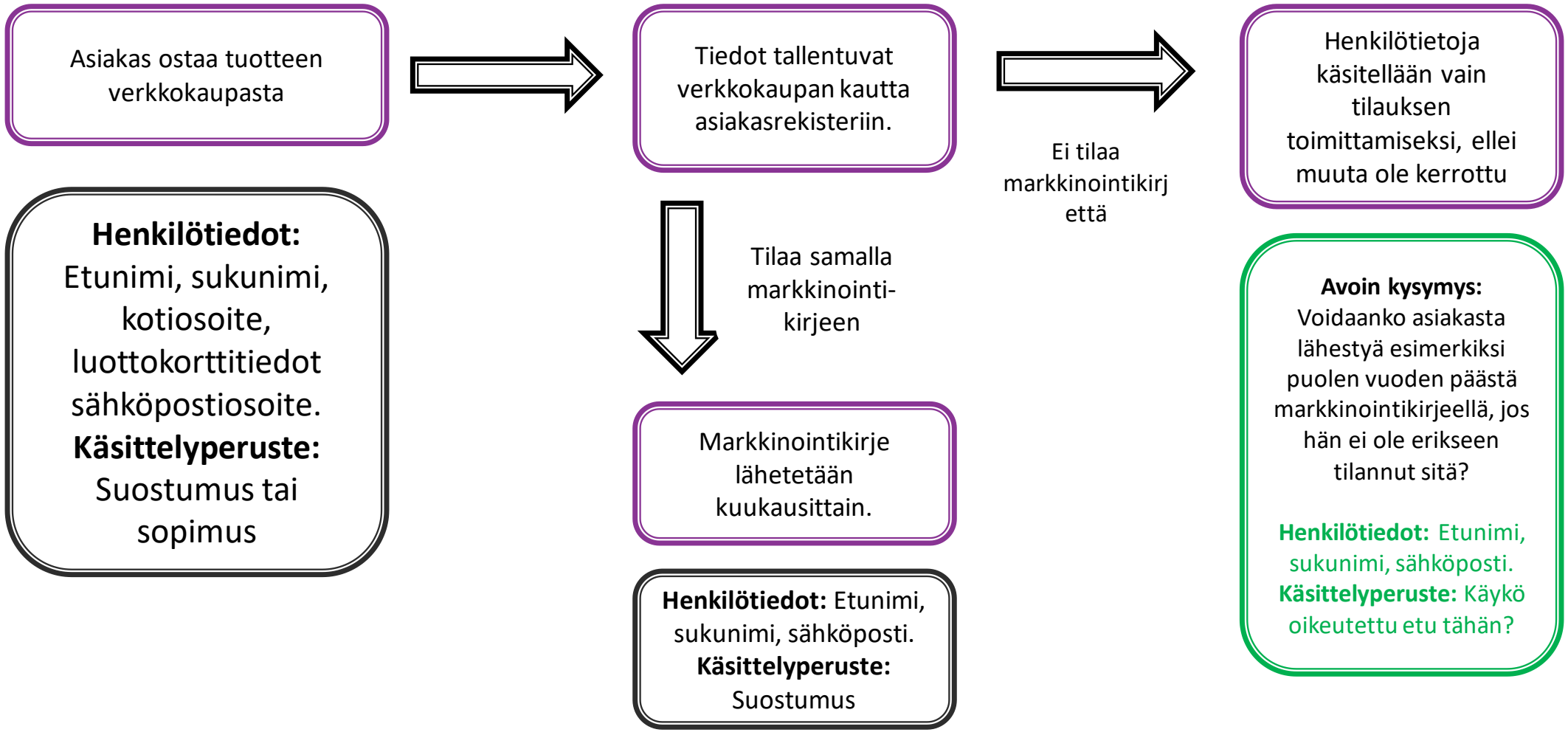
https://tietosuoja.fi/rekisterinpitajan-seloste-kasittelytoimista

Rekisterinpitäjä					
Nimi ja yhteystiedot		**Tietosuojavastaava (jos nimitetty)**		**Edustaja (tarvittaessa)**	
Nimi	Rekisterinpitäjä Esimerkki	**Nimi**	Tietosuojavastaava Esimerkki	**Nimi**	N/A
Osoite	Katuosoite	**Osoite**	Katuosoite	**Osoite**	N/A
Sähköposti	Sähköpostiosoite	**Sähköposti**	Sähköpostiosoite	**Sähköposti**	N/A
Puhelin	Puhelinnumero	**Puhelin**	Puhelinnumero	**Puhelinnumero**	N/A

Seloste käsittelytoimista					
Tehtävä, johon tietoja käsitellään	**Käsittelyn tarkoitus**	**(Tarvittaessa) yhteisrekisterinpitäjä ja tämän yhteystiedot**	**Rekisteröityjen ryhmät**	**Henkilötietojen ryhmät**	**Vastaanottajaryhr**
Taloushallinto	Palkanmaksu	N/A	Työntekijät	Yhteystiedot	HMRC
Taloushallinto	Palkanmaksu	N/A	Työntekijät	Pankkitiedot	HMRC
Taloushallinto	Palkanmaksu	N/A	Työntekijät	Eläketiedot	HMRC
Taloushallinto	Palkanmaksu	N/A	Työntekijät	Verotiedot	HMRC
HR	Työsuhde	N/A	Työntekijät	Yhteystiedot	N/A
HR	Työsuhde	N/A	Työntekijät	Palkkaustiedot	N/A
HR	Työsuhde	N/A	Työntekijät	Vuosilomatiedot	N/A
HR	Työsuhde	N/A	Työntekijät	Sairaslomatiedot	N/A
HR	Rekrytointi	N/A	Potentiaaliset kandidaatit	Suositukset	N/A
HR	Rekrytointi	N/A	Potentiaaliset kandidaatit	Työhistoria	N/A
HR	Rekrytointi	N/A	Muut kandidaatit	Yhteystiedot	N/A
HR	Rekrytointi	N/A	Muut kandidaatit	Suositukset	N/A
HR	Rekrytointi	N/A	Muut kandidaatit	Työhistoria	N/A
Myynti	Suoramarkkinointi	N/A	Olemassaolevat asiakkaat	Yhteystiedot	Käsittelijä – markkinoint
Myynti	Suoramarkkinointi	N/A	Olemassaolevat asiakkaat	Ostohistoria	Käsittelijä – markkinoint
Myynti	Suoramarkkinointi	N/A	Potentiaaliset asiakkaat	Yhteystiedot	Käsittelijä – markkinoint

Jatkuu…

Omien käsittelytoimien dokumentointi: Esimerkki 2: Tietovirtojen visualisointi



Tietosuojaseloste?

- Tietosuojaselosteen tehtävänä on kertoa rekisteröidyille (esim. asiakkaille tai yhdistyksen jäsenille), miten heidän henkilötietojaan käsitellään.
- Rekisteröityjä on mahdollista informoida tietosuojasta selosteella vasta, kun käsittelyprosessit ovat selkeitä organisaatiolle itselleen.
- Informoinnista lisää syksyn webinaarissa!

Käsittelyn tarkoitukset

- Rekisterinpitäjän (esim. yritys tai yhdistys) on määriteltävä, mitä tarkoitusta varten henkilötietoja käsitellään.
- Tarkoitus tulee määritellä itse omaan toimintaan perustuen ennen käsittelyn aloittamista.
- Tietoja ei saa käsitellä alkuperäisten tarkoitusten kanssa yhteensopimattomalla tavalla myöhemmin.

Käsittelyn perusteet

- Rekisterinpitäjän on myös määriteltävä, mihin *kuudesta mahdollisesta käsittelyperusteesta* henkilötietojen käsittely milloinkin pohjautuu.
  - **1) rekisteröidyn suostumus**
  - **2) sopimus**
  - **3) rekisterinpitäjän lakisääteinen velvoite**
  - 4) elintärkeiden etujen suojaaminen
  - 5) yleistä etua koskeva tehtävä tai julkinen valta
  - **6) rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu**

Käsittelyn perusteet: 1) Suostumus

- Suostumuksen on oltava
  - **Yksilöity** – tiettyyn käyttötarkoitukseen, ei kaikkeen kerralla
  - **Tietoinen**
  - **Aidosti vapaaehtoinen ja yksiselitteinen tahdonilmaisu** – ei voi antaa esimerkiksi vaikenemalla tai valmiiksi rastitetulla ruudulla
  - Suostumuksen peruuttamisen on oltava yhtä helppoa kuin suostumuksen antamisen

- **Esimerkkejä:**
  - Uutiskirjeen tilaaminen
  - Palvelun käyttöehtojen hyväksyminen
  - Suostumuksen pyytäminen markkinointiin tarkoitettujen evästeiden käyttöön.
  - Tapahtumaan ilmoittautuminen

Käsittelyn perusteet: 2) Sopimus

- Kun rekisteröity on osapuolena sopimuksessa, hänen henkilötietojaan saa käsitellä sopimuksen täytäntöön panemiseksi.

- **Esimerkkejä**
  - Jos rekisteröity esimerkiksi tilaa verkosta tuotteita, yritys voi käsitellä hänen osoitetietojaan, jotta tuotteet saadaan toimitettua perille.
  - Luottosopimus, jolloin luotonantaja voi käsitellä henkilön luottotietoja arvioidakseen tämän luottokelpoisuutta.

  - ”…verkkokauppaa harjoittava vähittäismyyjä haluaa rakentaa käyttäjien mieltymyksiä ja elämäntapavalintoja koskevia profiileja, jotka perustuvat käyttäjien vierailuihin verkkosivustolla. **Ostosopimuksen** tekeminen ei ole riippuvainen kyseisenlaisten profiilien rakentamisesta. Vaikka profilointi mainitaan erityisesti sopimuksessa, tämä seikka ei tee siitä tarpeellista sopimuksen täytäntöön panemisen kannalta. Jos verkkokauppaa harjoittava vähittäismyyjä haluaa suorittaa tällaista profilointia, sen täytyy käyttää muuta oikeusperustetta.”

    Lähde: European Data Protection Board Guidelines, 8.10.2019

Käsittelyn perusteet:
3) Rekisterinpitäjän lainsäädännöllinen velvoite

- Lakisääteinen velvoite voi koskea niin yksityisellä kuin julkisella sektorilla toimivaa rekisterinpitäjää
- **Esimerkkejä**
  - työnantajan on ilmoitettava työntekijänsä palkkatiedot veroviranomaisille
  - peruskoulun oppilaitoksen on käsiteltävä oppilaiden henkilötietoja
  - Yhdistyksen jäsenen nimen ja kotipaikan käsittely perustuu yhdistyslakiin

Käsittelyn perusteet:
4) Elintärkeiden etujen suojaaminen

- Henkilötietojen käsittely on sallittua, kun se on tarpeen rekisteröidyn tai jonkun toisen henkilön elintärkeiden etujen suojaamiseksi.
- **Esimerkiksi**
  - Humanitääriset hätätilanteet
  - Luonnonkatastrofit
  - Epidemiat

Käsittelyn perusteet:
5) Yleistä etua koskeva tehtävä tai julkinen valta

- Henkilötietoja saa käsitellä, kun yleinen etu tai rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen sitä edellyttää.
- **Esimerkiksi:**
  - Henkilötietojen käsittely tieteellisen tai historiallisen tutkimuksen tai tilastoinnin tarkoituksia varten.

Käsittelyn perusteet: 6) Rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu

- Henkilötietojen käsittely voi **olla rekisterinpitäjän oikeutetun edun** mukaista esimerkiksi silloin, kun tämän ja rekisteröidyn välillä on jokin merkityksellinen suhde. Se tarkoittaa, että rekisteröity on esimerkiksi rekisterinpitäjän asiakas tai alainen.
- Oikeutetun edun hyödyntäminen vaatii **tasapainotestin tekemistä.**
- Esimerkkejä tilanteista, joissa rekisterinpitäjän etu voi olla oikeutettu ja voi mahdollistaa henkilötietojen käsittelyn:
  - Suoramarkkinointi
  - tieteellinen ja historiallinen tutkimus sekä tilastointi
  - henkilötietojen siirtäminen hallinnollisista syistä konsernin sisällä.

Lähde: https://tietosuoja.fi/rekisterinpitajan-oikeutettu-etu

Käsittelyn perusteet: 6) Rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu

Suoramarkkinoinnin tasapainotesti

Palveluidemme ja tuotteidemme markkinointia tehdään yrityksemme toiminnan kehittämiseksi ja jatkuvuuden varmistamiseksi osittain oikeutettuun etuun perustuen.

Oikeutetut edut ovat: elinkeinon harjoittamisen vapaus ja suoramarkkinointi (tietosuoja-asetus, 47 resitaali)

Olemme tehneet tasapainotestin oikeutetun edun käyttämisestä henkilötietojen käsittelyn perusteena, minkä tuloksena todettiin, ettei se aiheuta kohtuuttomia riskejä markkinoinnin kohteena olevien luonnollisten henkilöiden oikeuksille tai vapauksille.

Voit vastustaa tietojesi käsittelyä koska tahansa. Lisätietoja saat tarvittaessa tietosuojavastaavaltamme.

1. Onko oikeutettu etu sopivin käsittelyperuste?

2. Edun välttämättömyys ja lainmukaisuus

3. Onko henkilötietojen käsittely tarpeen edun saavuttamiseksi?

4. Rekisteröidyn oikeudet ja edut sekä vertailu oikeutettuun etuumme

5. Tietosuojan lisätakeet ja henkilötietojen käsittelyn turvallisuus

Lähde: opsec.fi/fi/tasapainotesti

Kertaus

- Omien tietosuojan käsittelytoimien tunnistaminen ja dokumentointi on lähtökohta tietosuojasta huolehtimiselle ja **osoitusvelvollisuuden** täyttämiselle.
- Dokumentointia voi tehdä taulukkoon, ja tietovirtoja on helpointa hahmottaa visuaalisesti. Osana dokumentointia tulee pohtia **käsittelyn tarkoitukset sekä perusteet**
- **Tarkoitus** tulee määritellä itse omaan toimintaan perustuen ennen käsittelyn aloittamista. Tietoja ei saa käsitellä alkuperäisten tarkoitusten kanssa yhteensopimattomalla tavalla myöhemmin.
- Mahdolliset **käsittelyperusteita** on tietosuojalainsäädännössä määritelty 6 kpl: *rekisteröidyn suostumus, lakisääteinen velvoite, elintärkeiden etujen suojaaminen, yleistä etua koskeva tehtävä tai julkinen valta ja oikeutettu etu.*

Vinkkejä ja lukemista

- Tietosuojaapkyrityksille.fi – Kokeile itsearviointiin perustuvaa tietosuojatyökalua!
- Tietosuojaapkyrityksille.fi – Ohjesivu käsittelyperusteista
  https://www.tietosuojaapkyrityksille.fi/ohjesivut/kasittelyn-peruste/
- 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/