

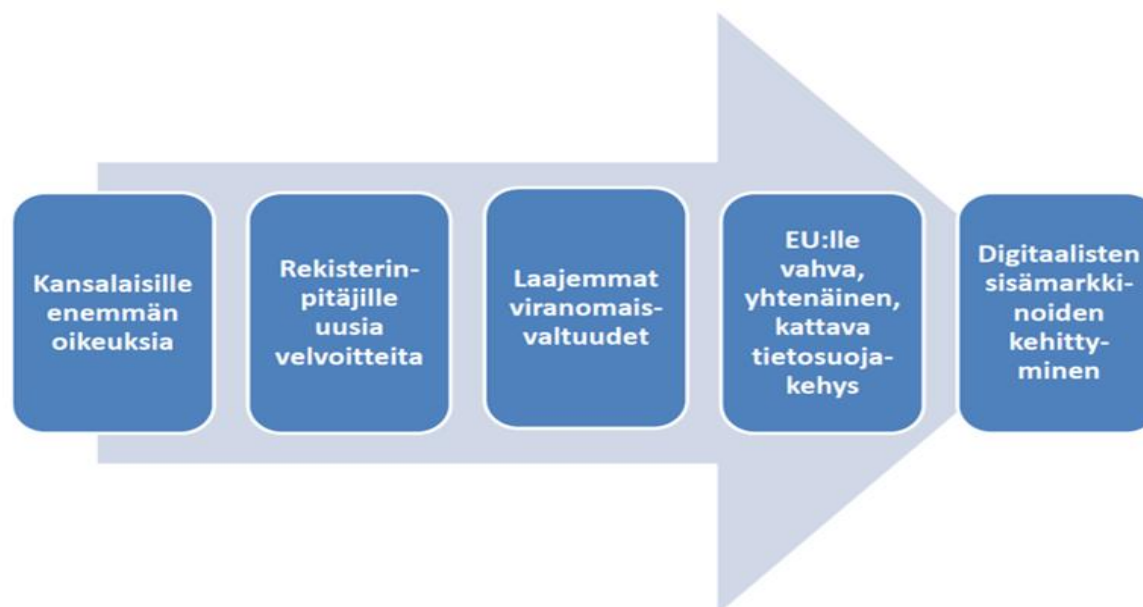
Tietopaketti tietosuojasta ProAgrian ja Maa- ja kotitalousnaisten jäsenyhdistyksille



Tietosuoja-asetuksesta

- Asetus astui voimaan 24.5.2016 ja sitä ryhdytään soveltamaan 25.5.2018 alkaen.
- Asetuksen sisältö on suoraan sovellettavaa oikeutta, eikä riipu kansallisesta lainsäädännöstä. Toisin sanoen asiakas voi halutessaan suoraan vedota asetuksen sisältämään lainsäädäntöön.
- Taustalla on henkilötietolaki ja Suomessa on vireillä sen päivittäminen, hallituksen esitys tietosuojalaksi.
- EU:ssa on vireillä myös hanke EU:n sähköisen viestinnän tietosuoja-asetuksen (ePrivacy) säätämiseksi, aikataulutavoite on 25.5.2018.
- Tietosuoja-asetus säätelee henkilötietojen käyttöä.

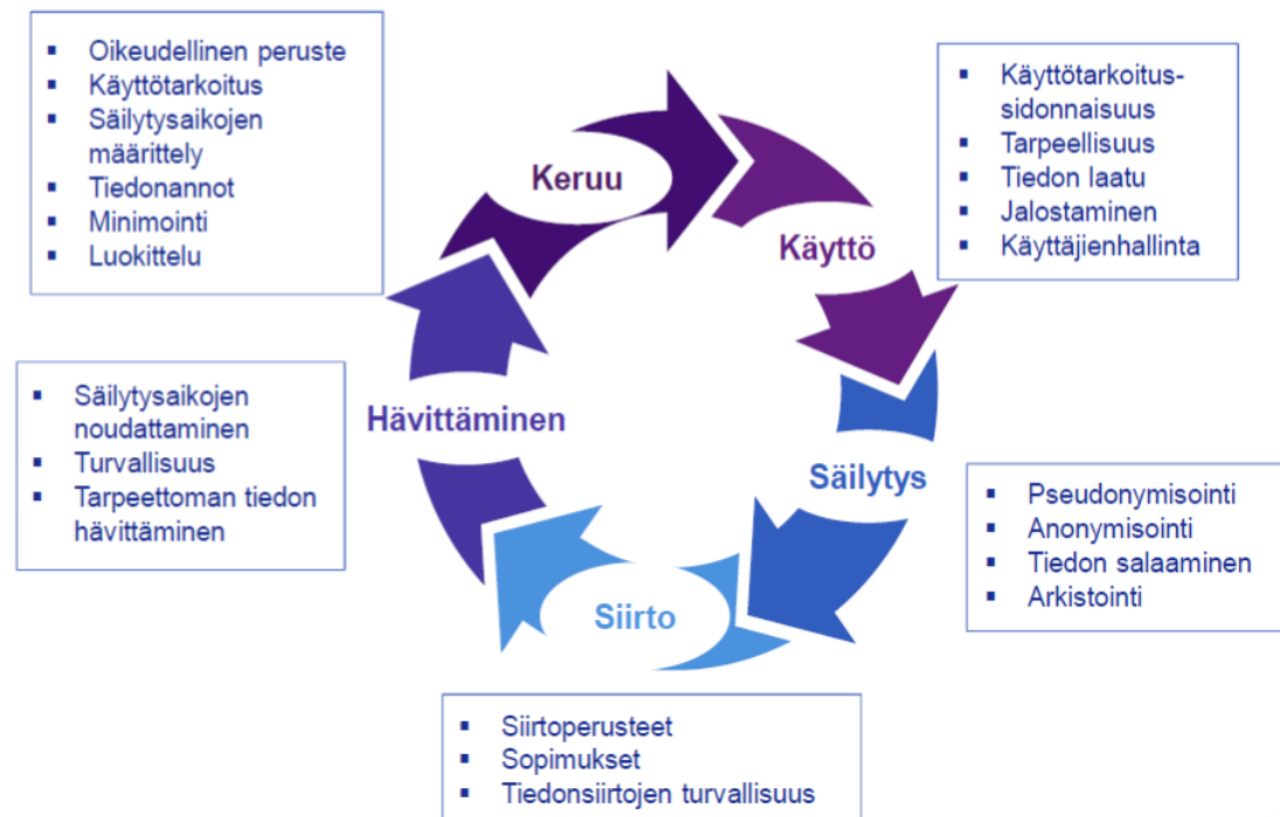
Asetuksen sisältö ja tavoite



Tietosuojakoulutus



Henkilötiedon elinkaari



Mikä on henkilötieto?

- Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja
- Tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen tai yhden tai useamman hänelle ominaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella

Mikä muuttuu?

1. Henkilötietoja käsitteleville yrityksille ja myös yhdistyksille tulee näyttövelvollisuus asetuksen noudattamisesta
2. Henkilötietojen käsittely on kuvattava ja dokumentoitava
3. Yhdistyslaki velvoittaa jäsenluettelon pitämiseen: jäseneksi hakiessa jäsen antaa suostumuksensa tietojen käsittelyyn
4. Henkilötietojen käsittelyn kaikki vaiheet (lisäys-muutos-poisto) on voitava esittää

Mikä muuttuu?

5. Tietojen minimointi – saadaan kerätä vain toiminnan vaatimat tiedot
6. Henkilötietojen säilytysaika on rajallinen => voidaan säilyttää vain niin kauan, kun on peruste säilyttää tieto: jäsenyyteen liittyvien asioiden käsittely kesken ja/tai velvoittava lainsäädäntö (kirjanpitolaitosten säilytysvelvoite 6 v) vaatii, ja sen jälkeen tiedot on poistettava
7. Jäsenten riittävä informointi => vaatii käytännössä esim. tietosuojaselosteen

Mikä muuttuu?

8. Rekisteröidyn oikeuksien toteutuminen käytännössä => tietojärjestelmissä pitää pystyä muokkaamaan, poistamaan ja tuomaan ulos henkilötietoja (esim. pyydettäessä on jäsenelle toimitettava kirjallinen yhteenveto henkilötiedoista)
9. Jos henkilötietojen käsittelyä on ulkoistettu (esim. jäsentiedot ProAgrian ja Maa- ja kotitalousnaisten jäsenrekisterissä), pitää näiden ulkoisten palveluntuottajien kanssa olla kirjalliset tietojenkäsittelysopimukset

Mikä muuttuu?

10. Tietosuojaloukkauksista on informoitava viranomaisia (72 tunnin aikaraja) ja tarvittaessa rekisteröityjä sekä roolista riippuen tiedon omistajaa (rekisterinpitäjä) esimerkiksi viranomaispalveluissa
11. Oikeus tulla unohdetuksi oltava aina mahdollista
12. Tietosujoaohjeistus, rooleista riippuen on eri näkökulmia
13. Tietosuojavastaava
14. Koulutusta ja tiedottamista (jäsentietoja käsittelevät)

Suostumuksesta

Henkilötietolain 3 §:n mukaan suostumuksella tarkoitetaan kaikenlaista vapaaehtoista, yksilöityä, tietoista tahdonilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn (esim. jäsenhakemus).

Henkilölle, jolta suostumusta pyydetään, tulee antaa tieto mm. seuraavista seikoista:

- kuka käsittelee tietoja eli kenelle suostumus tietojen käsittelyyn annetaan (kuka on rekisterinpitäjä)
- mitä tietoja kerätään ja talletetaan
- mitä käyttötarkoitusta varten tietoja kerätään
- onko tietoja tarkoitus hankkia muutoin kuin kyseisen suostumuksen perusteella (jos on: mitä tietoja hankitaan, mistä ja millä perusteella)
- luovutetaanko tietoja ulkopuolisille (jos tietoja luovutetaan: mitä tietoja luovutetaan, kenelle ja mihin käyttötarkoituksiin)
- miten kauan tietoja säilytetään.

Tietosuojakoulutus

Tietojen toimittaminen jäsenelle

Pyydettäessä yhdistyksen on toimitettava henkilötietojen käsittelyä koskevat tiedot rekisteröidylle tiiviisti esitetystä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa. Tiedot tulee antaa viivytyksettä ja enintään kuukauden kuluessa pyynnön vastaanottamisesta. Rekisteröidyllä on oikeus saada jäljennös häntä koskevista henkilötiedoista. Jos pyyntö tulee sähköisesti, on vastaus annettava sähköisessä muodossa, ellei toisin sovita. Rekisteröidyllä on oikeus tietojen oikaisuun tai tietojen poistoon rekisteristä (oikeus tulla unohdetuksi).

Ohjeissa suositellaan tietojen toimittamista sähköisessä muodossa ja tietojen on oltava rekisteröidylle maksuttomia.

Tietosuojakoulutus

Sisäänrakennettu tietosuoja uutena velvollisuutena (23 artikla)

Rekisterinpitäjän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet joilla taataan henkilötietojen käsittely siten, että käsittely vastaa asetuksen vaatimuksia ja rekisteröityjen oikeudet suojataan. Tämä voi tarkoittaa esimerkiksi:

- Henkilötietojen pseudonymisointi
- Järjestelmien kyky taata turvallisuus
- Kyky palauttaa pääsy ja saatavuus tietoihin fyysisen tai teknisen tapahtuman jälkeen
- Säännöllinen testauksen prosessi, jolla arvioidaan teknisten ja organisatoristen toimenpiteiden tehokkuutta

Tietosuojakoulutus

Tietoturvaloukkauksesta ilmoittaminen

Uutena asiana on rekisterinpitäjän velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksista tietosuojaviranomaiselle ja rekisteröidylle. Tietoturvaloukkauksella tarkoitetaan loukkausta, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin. Rekisterinpitäjän on tehtävä loukkausta koskeva ilmoitus valvontaviranomaiselle 72 tunnin kuluessa loukkauksen ilmitulosta. Rekisterinpitäjällä on velvollisuus ilmoittaa loukkauksesta myös rekisteröidylle.

HUOM! Kaikki tietoturvaloukkaukset on dokumentoitava, sisältäen vaikutukset ja tehdyt korjaavat toimenpiteet. Viranomaiselle tehtävää ilmoitusta varten on olemassa valmis dokumenttipohja.

Tietosuojakoulutus

Tietoturvaloukkauksesta ilmoittaminen

- Kuvaus mitä on tapahtunut.
- Mikäli mahdollista, niiden rekisteröityjen ryhmät ja lukumäärät, joita loukkaus koskettaa.
- Tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta valvontaviranomainen voi kysyä lisätietoja.
- Millaisia vaikutuksia henkilötietojen tietoturvaloukkauksella voi todennäköisesti olla rekisteröidyille.
- Kuvaus niistä toimenpiteistä, joita rekisterinpitäjä aikoo toteuttaa tai jotka se on jo toteuttanut haittavaikutusten lieventämiseksi ja tilanteen ratkaisemiseksi.

Tietosuojakoulutus

Lähdeluettelo

- VAHTI-ohjeet: https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128
- Rekisterinpitäjän vastuu: 24 artikla ja johdanto-osan kohdat 74-77
- Sisäänrakennettu ja oletusarvoinen tietosuoja: 25 artikla ja johdanto-osan kohta 78
- Seloste käsittelytoimista: 30 artikla ja johdanto-osan kohta 82
- Käytännösäännöt: 40–41 artiklat ja johdanto-osan kohdat 98–99
- Sertifiointi: 42 artikla ja johdanto-osan kohta 100
- Tietosuoja koskeva vaikutustenarviointi: 35 artikla ja johdanto-osan kohdat 84, 89– 93 ja 95
- Ennakkokuuleminen: 36 artikla ja johdanto-osan kohdat 94–96
- Käsittelyn turvallisuus: 32 artikla ja johdanto-osan kohta 83
- Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle: 33 artikla sekä johdanto-osan kohdat 85, 87 ja 88 Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle: 34 artikla ja johdanto-osan kohdat 86–88