Tärkeimmät asiat tietosuojasta yhdistyksille

Kaisa Päivinen

DITTMAR & INDRENIUS

Sisältö

- Keskeiset käsitteet
- Tietosuoja-asetuksen keskeiset periaatteet ja velvoitteet
  - Käsittelyperusteet
  - Dokumentaatio
  - Tietoturva
  - Rekisteröidyn oikeudet

DITTMAR & INDRENIUS

Tietosuojaa koskeva keskeinen lainsäädäntö

- Tietosuojan yleislaki
  - Henkilötietolaki (523/1999) ⟶ korvautuu EU:n tietosuoja-asetuksella
- Keskeiset erityislait
  - Tietoyhteiskuntakaari (917/2014)
  - Laki yksityisyyden suojasta työelämässä (759/2004)
- Rangaistussäännökset
  - Rikoslain 24 luku ja 38 luku

Tietosuoja-asetuksen soveltuminen

- Tietosuoja-asetusta ei sovelleta sellaiseen henkilötietojen käsittelyyn, jota henkilö suorittaa yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa
  - Vrt. esim yhdistyksen toiminnassa suoritettu henkilötietojen käsittely, johon tietosuoja-asetus soveltuu

Henkilötiedon käsite

'henkilötiedoilla' kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä 'rekisteröity', liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella

Jos pystyt yhdistämään tiedon henkilöön
nähtyäsi hieman vaivaa asian eteen,
se on henkilötietoa

7

(Henkilö)rekisteri

- Jäsennelty henkilötietoja sisältävä tietojoukko
  - Kortisto, excel, tietojärjestelmä…
- Tiedot ovat saatavilla

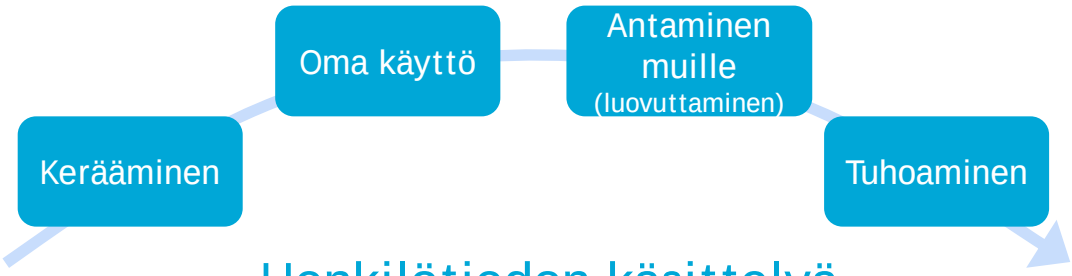
8

Käsittely

- Henkilötietoihin kohdistuva toiminto
  - Manuaalinen ja automaattinen käsittely

9

Tiedon elinkaari



Henkilötiedon käsittelyä

10

Rekisteröity

- Henkilö, jota henkilötieto koskee
  - Esimerkiksi yhdistyksen jäsen

Rekisterinpitäjä

- Taho, jolla tosiasiallinen päätösvalta tietojen käsittelystä
  - Määrittelee käsittelyn tarkoitukset ja keinot
  - Esimerkiksi yhdistys

Käsittelijä

- Rekisterinpitäjän lukuun toimiva taho
  - Luonnollinen henkilö, oikeushenkilö, viranomainen, virasto…
  - Esimerkiksi it-palveluntarjoaja

13

Siirto

- Rekisterinpitäjä vaihtaa henkilötietojen tallennuspaikkaa
  - Esim. pilvipalvelun käyttöönotto
- Rekisterinpitäjä antaa henkilötietojen käsittelytehtäviä kolmannelle taholle, mutta säilyttää vallan tietoihin itsellään
  - Esim. palkkahallinnon ulkoistaminen

14

Luovutus

- Tietojen vastaanottajalle annetaan itsenäinen oikeus käsitellä henkilötietoja omia tarkoituksiaan varten
  - Esim. markkinointia varten ostettavat osoitelistat

Anonymisointi

- Ei tunnistettavissa
  - Yhdistyksen käytössä olevat tiedot
  - Muiden käytössä olevat tiedot
- Ei palautettavissa tunnistettavaan muotoon
- Ei henkilötietoa → tietosuojasääntely ei sovellu
  - Vrt. pseudonymisointi

17

EU:n tietosuoja-uudistuksen ydin

1. Sääntely harmonisoituu
   - EU:n digitaaliset sisämarkkinat
2. Yksilöiden oikeudet laajentuvat
   - Kontrolli omaan dataan
3. Toimijoiden velvollisuudet lisääntyvät
   - Riskit kasvavat
4. Valvonta voimistuu
   - Sanktiot ja laaja soveltamisala

18

Keskeisimmät periaatteet

- Tarpeellisuusvaatimus ja tietojen minimointi
  - Henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista tietojen käsittelytarkoituksia varten
  - Mitkä tiedot ovat tarpeellisia yhdistyksen toiminnassa?
- Käyttötarkoitussidonnaisuus
  - Tiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla

19

Keskeisimmät periaatteet

- Tietojen ajantasaisuus
  - Tietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä
  - Epätarkkojen ja virheellisten henkilötietojen poistaminen tai oikaiseminen
  - Päivitättekö henkilötietoja?
- Säilytyksen rajoittaminen
  - Tietoja voi säilyttää ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten
  - Milloin/miten poistatte käsittelemiänne henkilötietoja?
  - Kuinka pitkään säilytätte tietoja esimerkiksi jäsenyyden päättymisen jälkeen?

20

Suunnittelu

- Kuka (=yhdistys ym.) käsittelee tietoja?
- Miksi tietoja käsitellään?
- Ketä tiedot koskevat?
- Mitä tietoja käytetään?
- Kenelle saatuja tietoja annetaan?
- Mitä haittaa käsittelystä on yksittäisille henkilöille?
- Missä maassa tietoja säilytetään?
- Kauanko tietoja säilytetään?
- Miten kaikki tämä on suojattu?
- Kenen vastuulla käsittely on?
- Mikä käsittelyperuste oikeuttaa käsittelyn?
- Mitä yksittäisille henkilöille on tarkoitus kertoa? Miten?

21

Osoitusvelvollisuus

Compliance

- ”Vaatimustenmukaisuus”
- Lainsäädännön noudattamisen varmistaminen

→ Do it

Accountability

- "Tilivelvollisuus"/ "Osoitusvelvollisuus"
- Lainsäädännön noudattamisen osoittaminen

→ Prove it

22

Aineiston laatiminen ja ylläpito

- *”Syyllinen kunnes toisin todistetaan”*
- Sisäinen asiakirja-aineisto
  - Suunnittelu
  - Ohjeistusten päivittäminen
  - Todisteet aiemmista toimista (esim. koulutuksen osallistujalistat, kirjeenvaihto)
- Ulkoinen asiakirja-aineisto
  - Rekisteröityjen (mm. jäsenet & työntekijät) informointi
  - Sopimusten päivittäminen

23

Henkilötietojen käsittelyperuste

- Kaikelle käsittelylle (= kerääminen, käyttäminen, luovuttaminen jne.) tulee olla tietosuoja-asetuksen mukainen käsittelyperuste, esimerkiksi:
  - Oikeutettu etu
    - Jäsenyys, asiakkuus, työsuhde, markkinointi
  - Lakisääteisen velvoitteen noudattaminen
    - Esimerkiksi yhdistyslain 11 §:n mukainen jäsenluettelo
  - Suostumus
    - Esimerkiksi sähköinen suoramarkkinointi
  - Sopimuksen täytäntöön paneminen
    - Käsittely tarpeen sopimuksen yhteydessä tai suunnitellun sopimuksen tekemistä varten

24

Suostumus

- Tulee olla:
  - Vapaaehtoinen
  - Tietoinen (kieli, tekstin helppous, laajuus)
  - Yksilöity
  - Yksiselitteinen
  - Aktiivista toimenpidettä edellyttävä
- Rekisterinpitäjällä todistusvelvollisuus
  - Ymmärrettävyys kaiken A ja O
  - Pyyntö pidettävä muusta tekstistä erillään
  - Liian yleinen/epäselvä = mitätön
- Rekisteröidyllä aina oikeus peruuttaa

25

Tietosuoja-asetuksen mukainen tietoturvavelvoite

32 artikla *Käsittelyn turvallisuus*

1. Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten

a) henkilötietojen pseudonymisointi ja salaus;

b) kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;

c) kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;

d) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

2. Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi.

26

Käyttöoikeudet ja tietojen turvallinen säilyttäminen

- Henkilötietoja saavat yhdistyksessä käsitellä vain ne henkilöt, joilla on siihen heidän tehtäviensä kannalta perusteltu syy
- Tiedot tulisi säilyttää siten, että ulkopuoliset henkilöt eivät pääse tarkastelemaan aiheettomasti tietoja
  - Lukolliset kaapit, salasanat yms.
  - Tietojen hävittämistapaan kiinnitettävä huomiota
- Maalaisjärkeä saa ja pitää käyttää!

27

Tietoturvaloukkauksesta ilmoittaminen

- Monet asetuksen velvoitteet edellyttävät etukäteen varautumista
- Kaikille rekisterinpitäjän roolissa oleville organisaatioille yleinen ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle sekä rekisteröidyille
  - Ilmoitus tehtävä ”ilman aiheetonta viivytystä ja mahdollisuuksien mukaan **72 tunnin kuluessa sen ilmitulosta**”
    - Tietoja sopimuksen nojalla käsittelevän palveluntarjoajan on ilmoitettava tietoturvaloukkauksesta rekisterinpitäjän roolissa olevalle asiakkaalleen viipymättä saatuaan sen tietoonsa

28

Yhdistyksen on informoitava rekisteröityjä

- Kuka on rekisterinpitäjä? (Kuka käsittelee henkilötietoja?)
- Rekisterinpitäjän yhteystiedot
- Miksi henkilötietoja käsitellään?
- Mikä on tietojen tietosuoja-asetuksen mukainen käsittelyperuste?
- Mitä tietoja käsitellään?
- Mistä tietoja kerätään?
- Kuinka kauan tietoja säilytetään?
- Luovutetaanko tietoja muille organisaatioille?
- Missä tietoja käsitellään?
- Mitä oikeuksia rekisteröidyllä on ja kuinka rekisteröidyn tulisi toimia käyttääkseen oikeuksiaan?

29

Rekisteröidyllä on oikeus tarkastaa tietonsa

- Oikeus saada kopio kaikista henkilötiedoista
- 1 kk aikaa toteuttaa
- Veloituksetta ensimmäisen kerran
- Missä tiedot sijaitsevat?
- Kuka vastaa tarkastuspyyntöihin?

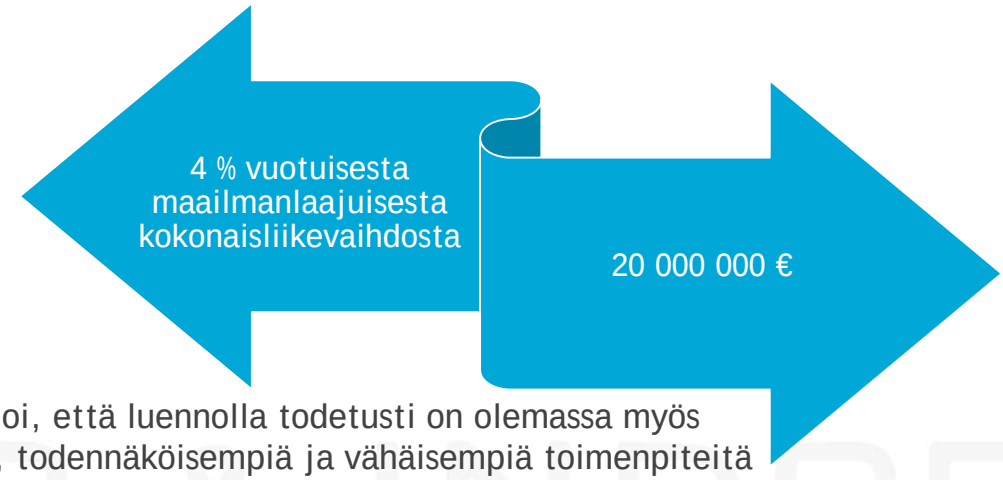
30

Muita rekisteröidyn oikeuksia

- Tietojen oikaiseminen
- Tietojen poistaminen
- Oikeus vastustaa tietojen käsittelyä
- Huomioitava, että eivät välttämättä tule sovellettaviksi kaikissa tilanteissa

31

Enimmäissakot



Huomioi, että luennolla todetusti on olemassa myös muita, todennäköisempiä ja vähäisempiä toimenpiteitä

32

Rajoitetusti aikaa – mihin kiinnittää huomiota?

1. Mitä henkilötietoja yhdistyksellänne on? Missä ja miksi?
Tietojen löytäminen & perusteleminen (sisältö & säilytysajat)

2. Dokumentaation laatiminen
Tietosuojaseloste ja ohjeistus henkilötietoja käsitteleville

3. Tietojen turvallisen säilyttämisen ja ajantasaisuuden varmistaminen
Turhien tietojen poistaminen

4.Kenen vastuulla, kenen tästä pitäisi tietää?
Roolitus ja vastuunjako, mahdolliset sopimukset, jatkuvuuden varmistaminen

5. Entä, jos jotain menee pieleen?
Varautuminen (prosessit + viestintä)

Yhteystiedot

Kaisa Päivinen
Associate, OTM
Puh. (09) 681 70182
Sähköposti: kaisa.paivinen@dittmar.fi