

Yhteenveto työpajojen purusta

Digitaalisen liiketoiminnan tietosuojafoorumi kokoontui 22.11.2016. Seminaarin teemana olivat tietosuoja-asetuksen siirtymä-ajan toimenpiteet sekä osoitusvelvollisuus.

Työpajakeskusteluissa osallistujat tuovat esille heidän omia näkemyksiään käsiteltäviin kysymyksiin.

Työpajojen purku: tietosuoja-asetuksen vaatimat toimenpiteet siirtymäajalle

Tietosuoja-asetuksen vaatimat toimenpiteet riippuvat toimijasta sekä siitä, millaista työtä organisaatiossa on jo tehty.

Työpajoissa nostettiin esille seuraavia toimenpiteitä:

1. Analysoidaan organisaation henkilötietovarannot:

- Kartoitetaan, mitä tietovarantoja organisaatiolla on.
- Kartoitetaan organisaation tietovirrat: mistä tietoja tulee, millä perusteella nämä tiedot tulevat, kuka tietoja käsittelee, mihin tarkoitukseen tietoja käsitellään ja milloin tiedot poistetaan?
- Selvitetään, millainen riskitaso käsittelyllä on.
- Kootaan edellä mainitut kysymykset esimerkiksi vuosittaiseen tietotilinpäätökseen.

Parempaa digitaalista liiketoimintaa: Tietovarantojen kartoittaminen kertoo, miten tietovarantoja voidaan käyttää sallitusti ja jopa entistä tehokkaammin.

2. Sitoutetaan henkilöstö ja johto sekä pidetään osaamisesta huolta:

- Tietosuojasta ja -turvasta huolehtiminen on koko organisaation asia. Kaikkien ei tarvitse osata lakipykälää, mutta kaikkien on ymmärrettävä sääntelyn tavoite ja miksi tietosuojasta huolehtiminen on tärkeää.
- Tärkeää on johdon sitoutuminen, ajantasainen tietosuojaohjeistus sekä säännöllinen raportointi ja valvonta.

3. Selvitetään, miten asetuksen uudet tai tarkennetut säännökset vaikuttavat nykyisiin prosesseihin ja tietojärjestelmiin:

- Asetuksessa on vaatimus lisääntyneestä läpinäkyvyydestä henkilötietojen käsittelyssä sekä yksityiskohtaisempaa sääntelyä rekisteröidyn oikeuksien toteuttamisesta.
- Uudet oikeudet: oikeus tulla unohdetuksi, oikeus siirtää tiedot, oikeus käsittelyn rajoittamiseen, laajempi vastustamisoikeus sekä laajempi oikeus kieltää automatisoidut yksittäispäätökset ja profilointi.
- Uudet velvollisuudet: ilmoittamisvelvollisuus tietosuojaloukkauksista, tietosuojavastaavan nimittäminen, osoitusvelvollisuuden toteuttaminen ja tietosuoja koskeva vaikutustenarviointi.

Yhteenveto työpajojen purusta

4. Tietojärjestelmien läpikäyminen:

- Tarkistetaan, ovatko tiedot yhdessä järjestelmässä vai ovatko ne hajautettu useaan eri järjestelmään.
- Käydään läpi, vastaako järjestelmän kokonaisarkkitehtuuri tiedonkäsittelyn tarpeita ja tietosuojavaatimuksia. Esimerkiksi löytyvätkö tiedot helposti ja pääsevätkö niihin käsiksi vain oikeat henkilöt.
- Varmistetaan, että järjestelmien ja prosessien tietoturva on kunnossa. Tietosuojasetuksen myötä tietosuojan on oltava oletusarvoista ja sisäänrakennettua järjestelmissä ja prosesseissa.
- Käydään läpi prosessit tietosuojaloukkausten varalta.

Parempaa digitaalista liiketoimintaa: [MyData-malli](#) on ihmiskeskeinen henkilötiedon hallintamalli. Sen avulla voidaan parantaa rekisteröidyn oikeuksien toteuttamista ja lisätä luottamusta tietojenkäsittelyyn.

5. Käydään läpi asiakasyhteydenottojen prosessit:

- Varmistetaan, että rekisteröidyn helppo saada tietoa henkilötietojensa käsittelystä.
- Varmistetaan, että rekisteröidylle on olemassa kanavat oikeuksien toteuttamiseen.
- Luodaan malliprosessi rekisteröidyn yhteydenottoihin reagoimiseen.
- Tehdään viestintäsuunnitelma, jossa tuodaan esiin organisaatiosi tietosuojasioita.

Parempaa digitaalista liiketoimintaa: Läpinäkyvät prosessit eivät ole vain tietosuojasetuksen vaatimus. Läpinäkyvyys on osa luottamuksellista asiakassuhdetta, ja sillä voidaan erottautua kilpailijoista.

6. Sopimusten läpikäyminen:

- Tarkistetaan, että henkilötietojen käsittelystä on sovittu kirjallisesti ulkopuolisen tietojen käsittelijän kanssa.
- Käydään sopimukset läpi vastuiden näkökulmasta: kuinka vastuut jakautuvat yksityisoikeudellisesti?

7. Kansainvälinen organisaatio?

- Luodaan yhdenmukaiset toimintamallit EU-alueella.
- Asetuksen one-stop-shop-mekanismi tulee sovellettavaksi.

Organisaatiot ovat saaneet apua valmistumiseen:

- liitoilta.
- tietosuojavaltuutetun toimistolta.
- asianajo-, konsultti- ja auditointiyrityksiltä.
- verkossa vapaasti saatavissa olevista ohjeista, kuten [Vahti-ohje](#) ja sen [excel-työkalu](#).