Tietosuoja-asetus ja riskiarvio – miksi ja mitä?

Meri Sariola
Projektitutkija, UEF Oikeustieteiden laitos

21.4.2020

AnalytiikkaÄly
AnalyticsAI

GDPR: Riskiperusteinen lähestymistapa

- Tietosuoja-asetusta sovelletaan sekä automaattiseen että manuaaliseen henkilötietojen käsittelyyn
- Rekisterinpitäjä on kokonaisvastuussa henkilötietojen käsittelystä, ja sillä on osoitusvelvollisuus siitä, että toiminnassa noudat. tietosuoja-asetusta
- Tietosuoja-asetuksessa on omaksuttu ns. **riskiperusteinen lähestymistapa**

= tietosuoja-asetuksen *velvoitteet ja asianmukaiset suojatoimet (ja myös esim. tietosuojaan liittyvät periaatteet)* on suhteutettava henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin

- Mitä suuremmat riskit, sitä suuremmat velvoitteet ja edellytetyt suojatoimet
- Riskiperusteisen henkilötietojen hallinnan on oltava jatkuvaa (ei liity vain käyttöönottoon)
- On mahdollista vaikutustenarviointia edeltävä prosessi!

AnalytiikkaÄly
AnalyticsAI

Mitä riskeihin liittyen on arvioitava?

- Dokumentoidaan ja arvioidaan kirjallisesti
- UEF Oppimisanalytiikan riskiarviotyökalu perustuu näihin osa-alueisiin (sitä kautta parempi käsitys mitä osa-alueet pitävät sisällään) → On organisaation tueksi, jotta osataan lisäkysymyksillä kohdistaa arviointi oikeisiin asioihin ja kartoittaa mahdolliset riskit
- Selkeä käsitys aiotusta henkilötietojen käsittelystä on hyvä lähtökohta riskiarviolle
- Ei voi arvioida yleensä pelkästään yksin GDPR perusteella, vaikuttaa myös muu tietojenkäsittelyyn ja -vastuisiin liittyvä sääntely

AnalytiikkaÄly
AnalyticsAI

Mitä **riskit** ovat?

- Voi olla monenlaisia, näitä ei ole lueteltu tietosuoja-asetuksessa
- Avattu WP29 tietosuojatyöryhmän lausunnoissa myös tietosuojavaltuutettu ohjeistanut
- Oikeuskirjallisuudessa tuotu esille, esim:
  - Uusi teknologia / uusi innovaatio (ohjelmistorobotiikka, tekoäly)
  - Esineiden Internet
  - Palveluiden ulkoistukset
  - Data-analytiikka
  - Datan avaaminen
  - Käyttöoikeuksien ja käsittelyvaltuuksien hallinnan puutteet
  - Vähäinen tietoturvakoulutus henkilöstölle
  - Huono sopimus- ja hankintaosaaminen
  - Tietojen luovutukset
  - Tietosuojattavan jätteen käsittelyprosessin puutteet
  - **Jos riskejä ei ole mahdollista arvioida, voi sekin itsessään muodostaa riskin (jos ei esim. tiedetä kuinka suuren opiskelijamäärän tietoja aiotaan käsitellä)**

AnalytiikkaÄly
AnalyticsAI

Mitä riskit eivät ole?

- Riski ei ole esim. se, että rekisterinpitäjä havaitsee jo olemassa olevassa toiminnassaan jonkin lainvastaisuuden (tällöin kyseessä on jo toteutunut riski)

Kysymykset, joilla pääsee alkuun riskien kartoituksessa:

- Mitä henkilötietojen käsittelyprosesseja organisaatiolla on?
- Mitä tietoja käsitellään missäkin prosessissa ja missä tietojärjestelmissä?
- Minkälaiset tietoturvavaatimukset tietojärjestelmille on hankintavaiheessa asetettu?
- Miten tietojärjestelmien tietoturvallisuus on varmistettu ja kontrolloitu?
- Miten tietojärjestelmien tietoturvallisuusjärjestelyjen ajantasaisuus on varmistettu?
- Missä tietoa säilytetään ja onko paikka suojattu riittävästi?
- Ketkä organisaatiossa ja sen ulkopuolella käsittelevät organisaation henkilötietoja?
- Miten henkilötietojen säilytysajat on määritelty ja onko säilytysajat liian pitkiä?
- Onko tietojen arkistointi eriytetty alkuperäisestä käsittelystä esimerkiksi käyttöoikeuksia rajaamalla?
- Onko tietojenkäsittelyn ohjeistus ajantasaista ja päivitetäänkö sitä säännöllisesti?
- Onko koulutus suunniteltu systemaattisesti?
- Minkälaiset ovat tietojen luovutuskäytännöt?

Tomi Voutilainen 2019: Oikeus tietoon. Informaatio-oikeuden perusteet, s. 124–125.

AnalytiikkaÄly
AnalyticsAI

Miten riskiarvio toteutetaan?

- Tietosuojan huomioiminen alusta alkaen esim. uuden teknologian käyttöönoton suunnittelussa
- Oikeuskirjallisuudessa suositellaan, että perustetaan organisaation keskeisistä toiminnoista koostuva **työryhmä** > viedään riskien analysointi, dokumentointi ja kuvaus **käytännön tasolle**
- Keitä työryhmään kuuluu? Esim. Johtoa, mahd. tietosuojavastaava, lakitoiminnoista/hankinnoista vastaava yksikkö, ne, joiden työnkuvaan kuuluu esimerkiksi tietojärjestelmäkokonaisuuden tai tietosuojaratkaisujen suunnittelu
- Työryhmän työsuunnitelma, säännölliset kokoontumiset ja niiden dokumentointi
- Työryhmän työn tavoite: että muodostuisi selkeä suunnitelma /prosessinkuvaus aiotusta henkilötietojen käsittelystä ja riskiarvio voidaan toteuttaa onnistuneesti
- AnalytiikkaÄly-hankkeessa laaditut apukeinot!

AnalytiikkaÄly
AnalyticsAI

UEF Oppimisanalytiikan riskiarviotyökalu:

https://blogs.uef.fi/oppimisanalytiikanriskiarvio/

Kommentteja ja palautetta voi lähettää Tommille ja Merille:

tommi.haapaniemi@uef.fi
meri.sariola@uef.fi

Kiitos!

UNIVERSITY OF EASTERN FINLAND

AnalytiikkaÄly
AnalyticsAI
Oppimisanalytiikka opiskelun, ohjauksen ja johtamisen tukena yliopistoissa