

Yleistä

Tietosuojan vaikutustenarviointi (Data Protection Impact Assessment, DPIA) on työkalu, jolla arvioidaan henkilötietoja käsittelevän prosessin vaikutuksia tietosuojaan. Tietosuojan vaikutustenarvioinnin avulla arvioidaan, kuinka suuri riski suunnitellun henkilötietojen käsittelyprosessin vaikutus olisi rekisteröidyille - henkilöille, joiden tietosuojaan ja vapauksiin suunniteltu henkilötietojen käsittelyprosessi vaikuttaa. Vaikutustenarviointi on osa organisaation riskienhallintaa ja se saattaa olla monella liiketoiminta- ja julkisen vallan käyttöalueilla lakisääteinen velvollisuus. Tietosuojavaltuutettu on listannut Whistleblow - ilmoituskanavan yhdeksi asioista, joista tietosuojan vaikutusten arviointi on tehtävä.

Kuvaus henkilötietojen käsittelyprosessista

Navisec ilmoituskanavan kautta kerättäviä tietoja käytetään väärinkäytösilmoitusten käsittelyyn voimassa olevan lainsäädännön mukaisesti. Ilmoituskanavan kautta ilmoituksen voi tehdä luottamuksellisesti ja halutessaan nimettömänä. Henkilötietojen käsittelyperusteena on rekisterinpitäjän oikeutettu etu sekä lakisääteiset velvoitteet. Rekisterinpitäjä voi itse päättää pitääkö ilmoitus tehdä nimellä vai ei. Pääkäyttäjällä on hallintaominaisuus, jossa voidaan valita, otetaanko vastaan anonyymejä, nimellisiä tai molempia ilmoituksia.

Ruokolahden kunnassa otetaan vastaan vain anonyymejä ilmoituksia. Ilmoituksen tekijää ei voi identifioida. Järjestelmä muodostaa ilmoituksen jätön yhteydessä ilmoittajalle yksilöidyn tunnuksen ja koodin asian seuraamiseksi. Tunnusten unohtuessa niitä ei voi saada selville tai palauttaa. Rekisterissä käsitellään rekisterin käyttötarkoituksen kannalta tarpeellisia tietoja ilmoituksen tekijästä annettujen tietojen perusteella ja ilmoituksen kohteesta sekä niistä henkilöistä, joiden todetaan ilmoituksen perusteella kytkeytyvän epäiltyyn väärinkäyttöön.

Rekisterissä ei käsitellä sellaisia rekisteröidyn yksityiselämään liittyviä tietoja, joilla ei ole kytköstä rekisteröidyn työtehtäviin tai ilmoituksen kohteena olevaan asiaan.

Navisec - ilmoituskanava palvelun rekisterinpitäjänä toimii Ruokolahden kunnanhallitus. Rekisterinpitäjä vastaa henkilötietojen käsittelijöiden roolituksesta.

Henkilötietoja säilytetään Euroopan talousalueella. Henkilötietoja säilytetään ainoastaan niin kauan ja siinä laajuudessa kuin ne ovat tarpeellisia ja rekisterinpitäjä hyödyntää niitä ilmoitettuihin käsittelytarkoituksiin liittyvässä toiminnassa. Henkilötietojen käsittely toteutetaan sähköisessä muodossa. Henkilötietoja käsittelevät vain nimetyt henkilöt, joiden työtehtäviin käsittely liittyy. Maksimisäilytysaika on 5 vuotta, jos ei muusta muuta johdu.

Konsultaatiot

Konsultoidaan tietosuojavastaavaa tarvittaessa.

Käsittelyn välttämättömyys ja oikeasuhtaisuus

Käsittelyn välttämättömyyden perustana on rekisterinpitäjän oikeutettu etu sekä lakisääteiset velvoitteet. Ilmoittajasta kerätään vain tarpeelliset tiedot, jotta käsittelyprosessi saadaan järjestettyä lakisääteiset velvoitteet huomioiden.

Tietosuoja-asetuksen 35 artiklan 3 kohta.

Käsittelijöiden roolit ja vastuut

Käsittelijä	Rooli ja vastuu
Matti Backman	Tekninen pääkäyttäjä, vastuu käyttöoikeuksista
Kaisa Häkkinen-Paananen	Ilmoitusten vastaanottaja ja käsittelijä

Riskien tunnistaminen ja arviointi (1 – 4)

Kuvaile riski ja sen aiheuttama uhka rekisteröityjen oikeuksille ja vapauksille	Vahingon todennäköisyys?	Vahingon vakavuus?	Kokonaisriski
*Esimerkit			
Ilmoitustyökalun tietoihin pääsee käsiksi ulkopuolinen taho (esimerkiksi pääkäyttäjän / käsittelijän käyttäjätunnus ja salasana päätyy ulkopuolisen saataville)	1	3	1
Käsittelyoikeuden haltija omaa käsittelyoikeuden häneltä jo poistuneeseen vastuualueeseen	2	1	1
Käsittelyoikeus on	1	1	1

annettu virheellisesti väärälle henkilölle			
--	--	--	--

Toimenpiteet riskien pienentämiseksi

Riski *Esimerkit	Toimenpiteet riskin pienentämiseksi	Toimenpiteen vaikutus	Jäännösriski	Toimenpide hyväksytty
Ilmoitustyökalun tietoihin pääsee käsiksi ulkopuolinen taho (esimerkiksi pääkäyttäjän / käsittelijän käyttäjätunnus ja salasana päätyy ulkopuolisen saataville)	Tietoja käsitellään vain työkoneella, johon pääsy vain henkilökohtaisella käyttäjätunnuksella. Palvelu käyttää vahvaa salausta.	Tunnukset ovat suojassa ulkopuolisilta.	1	Kyllä
Käsittelyoikeuden haltija omaa käsittelyoikeuden häntä jo poistuneeseen vastualueeseen	Käyttöoikeudet muutetaan heti henkilöstön vaihtuessa.	Ei vääriä oikeuksia. Kaikilla käsittelijöillä vaitiolo-velvollisuus.	1	Kyllä
Käsittelyoikeus on annettu virheellisesti väärälle henkilölle	Organisaation koon vuoksi ei ole todennököistä.	Ei vääriä oikeuksia. Kaikilla käsittelijöillä vaitiolo-velvollisuus.	1	Kyllä

Yhteenveto ja hyväksyntä

Aihe	Nimi ja päiväys	Huomiot
Toimenpiteet riskien vähentämiseksi on hyväksynyt:	Jukka-Pekka Bergman 6.3.2023 Kaisa Häkkinen-Paananen 6.3.2023	
Jäännösriskit on hyväksynyt:	Jukka-Pekka Bergman 6.3.2023 Kaisa Häkkinen-Paananen 6.3.2023	
Tietosuojavastaavan kannanottoa / neuvoa on pyydetty asiaan liittyen:	Matti Backman (tietosuojavastaava) 3.3.2023	Tietosuojavastaava yhtenä DPIA:n tekijöistä