Tietosuojaa koskevan vaikutustenarvioinnin tekeminen

Ohje
Tietosuojatiimi, Helsingin kaupunki

Helsinki

Mitä henkilötiedot ovat ja mitä niiden käsittelyllä tarkoitetaan?

Helsinki

Tietosuojatiimi

Henkilötiedot ja niiden käsittely

- Henkilötietoa on kaikki se tieto, jolla yksin tai yhdessä muun tiedon kanssa ihminen voidaan tunnistaa

- Henkilötietojen käsittelyllä tarkoitetaan kaikkia toimia, joita kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti.

- Käsittelyä ovat tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, haku, kysely, käyttö, tietojen luovuttaminen siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhdistäminen, rajoittaminen, poistaminen ja tuhoaminen.

- Myös pelkkä tietojen katselu on niiden käsittelyä

Mikä on tietosuojaa koskeva vaikutustenarviointi?

Helsinki

Tietosuojatiimi

Tietosuojaa koskevan vaikutustenarvioinnin tarkoitus

- Tietosuojaa koskevan vaikutustenarvioinnin (jatkossa vaikutustenarvioinnin) tarkoituksena on tunnistaa, arvioida ja hallita henkilötietojen käsittelyyn liittyviä riskejä.

- Vaikutustenarvioinnista säädetään EU:n yleisessä tietosuoja-asetuksessa.

- Rekisterinpitäjän tulee etukäteen, jo käsittelyä suunnitellessaan, arvioida ja dokumentoida, millaiset riskit henkilötietojen käsittelystä ihmisille aiheutuu.

- Kun riskit on arvioitu, niihin tulee varautua sopivilla suojatoimilla.

Milloin vaikutustenarviointi tulee tehdä?

Vaikutustenarvioinnin tarpeen tunnistaminen

- Vaikutustenarviointi on pakollinen mm. silloin, kun uutta teknologiaa otetaan käyttöön, käsitellään arkaluonteisia tai muutoin hyvin henkilökohtaisia tietoja tai henkilötietoja käsitellään laajamittaisesti.

- Vaikutustenarviointi tulee tehdä ennen kuin palvelu tai järjestelmä otetaan käyttöön.

- Vaikutustenarvioinnin tekemisen tarve tunnistetaan tekemällä siihen liittyvä alkukartoitus aina, kun ryhdytään suunnittelemaan uutta prosessia, järjestelmähankintaa tai järjestelmän rakentamista omin voimin

- Jos vaikutustenarviointi jätetään tekemättä silloin, kun se olisi tullut tehdä, voi kansallisen tietosuojavaltuutetun mukaan olla kyseessä rikoslain mukainen tietosuojarikkomus.

Vaikutustenarvioinnin työkalut

Helsinki

Tietosuojatiimi

Helsingin kaupungin työkalut vaikutustenarviointien tekemiseen

- Kaupungilla on omat työkalut vaikutustenarviointiin. Niillä selvitetään mm. mitä henkilötietoja käsitellään, millä perusteella niitä käsitellään, missä niitä käsitellään, miten tiedot suojataan ja miten rekisteröityjen oikeudet toteutetaan.

- Työkaluja ovat alkukartoitus, tietosuojan tarkistuslista, vaikutustenarvioinnin työkalu ja riskianalyysilomake. Työkalujen käyttö aloitetaan aina alkukartoituksella, joka ohjaa eteenpäin tarvittaviin muihin työkaluihin.

- Työkalut ja ohjeet löytyvät Helsingin kaupungin internet-sivuilta https://www.hel.fi/helsinki/fi/kaupunki-ja-hallinto/tietoa-helsingista/tietosuoja/tietosuojan-vaikutustenarviointi.

Alkukartoituksen tekeminen

Helsinki

Tietosuojatiimi

Milloin alkukartoitus tehdään

- Vaikutustenarvioinnin alkukartoitus tulee tehdä aina, kun ryhdytään suunnittelemaan uutta prosessia, järjestelmähankintaa tai järjestelmän rakentamista omassa järjestelmäkehityksessä.

- Alkukartoitus on tehtävä myös silloin, kun suunnitellaan merkittäviä muutoksia olemassa oleviin prosesseihin ja järjestelmiin.

- Alkukartoituksessa selvitetään ensin, käsitelläänkö henkilötietoja.

- Jos henkilötietoja käsitellään, alkukartoituksen kysymyksiin vastaamalla selviää, tuleeko tehdä vaikutustenarviointi vai ottaa tietosuoja kehittämisessä huomioon tietosuojan tarkistuslistan avulla.

Esimerkkejä alkukartoituksen kysymyksistä

- Alkukartoituksessa vastataan kyllä/ei-kysymyksiin siitä, käsitelläänkö henkilötietoja ja jos, niin millaisia ne ovat.

- Jos kysymykseen vastataan kyllä, pyydetään antamaan lisätietoja.

- Esimerkkikysymyksiä:

  - Ollaanko ottamassa käyttöön uutta teknologiaa, jota ei ole aiemmin käytetty?
  - Käsitelläänkö arkaluonteisia tai muuten hyvin henkilökohtaisia tietoja?
  - Käytetäänkö henkilötietoja arviointiin ja analysointiin, kuten profilointiin ja ennakointiin?
  - Siirretäänkö henkilötietoja kolmansiin maihin EU:n ulkopuolelle?

Varsinaisen vaikutustenarvioinnin tekeminen

Helsinki

Tietosuojatiimi

Vaikutustenarvioinnin tekeminen

- Jos alkukartoitus on osoittanut, että vaikutustenarviointi tulee tehdä, otetaan käyttöön vaikutustenarviointityökalu

- Vaikutustenarvioinnin tekemisessä on havaittu hyväksi työpajamenetelmä, jossa pidetään ensin alkukokous, johon kutsutaan tarvittavat asiantuntijat. Alkukokouksessa sovitaan vastuunjaosta. Alkukokouksen jälkeen olevassa vaikutustenarvioinnin työpajassa (tai työpajoissa) asiantuntijat ovat jo ennakkoon selvittäneet vastuualueillaan olevia asioita, jolloin tietojen dokumentointi työkaluun voidaan tehdä yhteisesti.

Alkukokous / osallistujat

- puheenjohtajana on se, joka vastaa asiasta, ”projektipäällikkö” (vastuulla aikataulutus, vastuunjako yms.)
- substanssiasiantuntija (toiminnan edustaja, tuntee tarpeen, johon järjestelmää tai prosessia ollaan hankkimassa)
- ”käyttäjä” (se, joka käyttää prosessia tai järjestelmää, tuntee päivittäisen työn)
- tietosuojan vastuuhenkilö (ohjaa ja neuvoo vaikutustenarvioinnin tekemisessä ja kysymyksenasetteluissa)
- tietoturvan asiantuntija (kertoo, millaista suojaustasoa edellytetään)

- Tarvittaessa myös
    - hankinnan asiantuntija (neuvoo hankintaprosessissa)
    - riskienhallinnan asiantuntija
    - muita asiantuntijoita

Alkukokous / agenda

- Hankkeen yhteenveto, mitä ollaan tekemässä (puheenjohtaja)
- Henkilötietojen käsittelytoimen kuvaus (työpajatehtävä [diat 19-24], jos halutaan tehdä)
- Vaikutustenarviointi:
  - Vaikutustenarvioinnin tarkoitus (tietosuojan vastuuhenkilö)
  - Työkalun esittely (tietosuojan vastuuhenkilö)
    - Käydään vaatimukset läpi (2. sarake, ”Vaatimus”)
  - Riskianalyysityökalun esittely
- Vastuunjako:
  - Työkaluun tai kokousmuistioon kirjataan vastuut (kuka täyttää minkäkin rivin vaikutustenarvioinnin työkalusta
- Aikataulu:
  - Ajankäytön varmistaminen, vaikutustenarvioinnin tekeminen vie aikaa
  - Työkalun täytön ja työpajojen aikataulusta sopiminen

Vaikutustenarvioinnin työpaja 1

- Ennen työpajaa:
  - Kukin vastuuhenkilö täyttää työkaluun omat rivinsä, myös tunnistetut riskit
  - Kukin vie riskit riskianalyysityökaluun alustavalla tasolla

- Työpajassa:
  - Käydään vaikutustenarvioinnin työkalu läpi
    - Kukin esittelee omat rivinsä

  - Päätetään, mitkä riskit viedään riskianalyysityökaluun
  - Ryhmä luokittelee riskit
  - Ryhmä täyttää riskianalyysityökaluun riskienhallinnan toimenpiteet

  - Aikataulu:
  - Seuraavasta työpajasta sopiminen

Vaikutustenarvioinnin lopputoimet

- Yhteenveto-välilehden täyttäminen, vaikutustenarvioinnin lopputuloksen arviointi (aina)
- Loppuraportin laatiminen päätöksentekoa varten (tarvittaessa)
- Tietosuojaviranomaisen ennakkokuuleminen, jos riskit ovat suuria eikä niitä itse saada pienennettyä (tarvittaessa)

Työpajatehtävä vaikutustenarvioinnin työpajaan: käsittelytoimien kuvaus

Käsittelytoimien kuvauksen osat

- Valitkaa jokin tuttu oikea järjestelmä tai järjestelmäkokonaisuus, jossa käsitellään henkilötietoja

- Fläppilakanan yläotsikoiden alle kuvataan mitä niihin kuuluu (yhdellä otsikolla yhden väriset laput)
  - Yhdelle post-it lapulle tunnistetaan konkreettisia käsittelyn osia

Lakana 1
Mitä henkilötietoja käsitellään ja mihin tarkoitukseen?

- Mitä **henkilötietoryhmiä** käsitellään
  - Esim. nimi, osoite, hetu
- Mitä **rekisteröityjen ryhmiä** on
  - Esim. asiakkaat, kuntalaiset, työntekijät
- Mikä on **henkilötiedon luonne**
  - Esim. julkinen, salassa pidettävä, arkaluonteinen
- Mikä on eri henkilötietojen **käyttötarkoitus**

Lakana 2:
Missä henkilötietoja säilytetään ja käsitellään?

- Mistä tieto tulee ja miten se liikkuu
- Missä sitä säilytetään
- Missä käsitellään (konkreettisesti + alueellinen ulottuvuus)
- Kuka tietoja käsittelee

Lakana 3: Miten ja milloin henkilötiedot poistetaan

- Onko säilytysaika määritelty
  - Toteuttaako järjestelmä automaattisia poistoja säilytysajan lopussa?
  - Pitääkö tiedot arkistoida ja tapahtuuko se sähköisesti?

- Saadaanko tiedot ulos eheästi käsittelyn päättyessä

Yhdistäkää osat käsittelytoimien kuvaukseksi

- Pöydällä on iso lakana
- Piirtäkää lakanalle kokonaiskuva käsittelytoimista ja sijoittakaa siihen aiemmin laaditut laput lakanoista 1-3

Vaikutustenarvioinnin työkalun välilehdet

Taustatiedot-välilehti

- Taustatiedot-välilehdelle kirjataan perustiedot siitä, millaista käsittelyä ollaan suunnittelemassa.

Lyhyt selostus siitä, millaista henkilötietojen käsittelyä suunnitellaan:	
Arvioinnin tekijä(t):	
Organisaatio:	
Arvioinnin ajankohta:	

Arviointitaulukko-välilehti

- Arviointitaulukko-välilehti on jaettu kolmeen eri osa-alueeseen. Nämä ovat:
  - ❖Järjestelmällinen kuvaus suunnitelluista käsittelytoimista
  - ❖Henkilötietojen käsittelyn tarpeellisuuden ja oikeellisuuden arviointi
  - ❖Rekisteröidyn oikeuksille aiheutuvien riskien arviointi

- Kussakin osa-alueessa on tietosuojavaatimuksia, joiden toteutumista arvioidaan.

- Seuraavilla dioilla kuvataan arviointitaulukon eri sarakkeiden käyttöä tarkemmin.

Vaatimus-sarake

- Tässä sarakkeessa ovat ne tietosuojavaatimukset, jotka käsittelyssä tulee huomioida.
- Esimerkkejä vaatimuksista:

Henkilötietojen käsittelytoimesta on laadittu toiminnallinen kuvaus, josta ilmenevät seuraavat asiat:

- Mitä henkilötietoja käsitellään (nimi, osoite, hetu jne.)?
- Järjestelmässä olevien tietojen luokittelu (julkinen, salassapidettävä, arkaluonteinen jne.)
- Miten tiedot poistetaan?
- Tietojen säilytysaika on määritelty niiden käyttötarkoituksen mukaisesti ja niiden poistaminen säilytysajan päätyttyä toteutetaan (myös varmuuskopiot)
- Mitä tietoja voi katsoa, mitä muokata, mitä poistaa?

Henkilötietojen käsittelijän kanssa tehtyyn sopimukseen on sisällytetty tietoturvallisuusliite.

Kun käsittely suoritetaan rekisterinpitäjän lukuun, rekisterinpitäjä saa käyttää ainoastaan sellaisia käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi niin, että käsittely täyttää tietosuoja-asetuksen vaatimukset.

Tietojen säilytysaika on määritelty niiden käyttötarkoituksen mukaisesti ja niiden poistaminen säilytysajan päätyttyä toteutetaan (myös varmuuskopiot).

Tiedon koko elinkaaren hallinta suunnitellaan jo alussa.

Rekisterinpitäjän on ennen käsittelyä kuultava valvontaviranomaista, jos tämä tietosuojaa koskeva vaikutustenarviointi osoittaa, että käsittely aiheuttaisi korkean riskin, jos rekisterinpitäjä ei ole toteuttanut toimenpiteitä riskin pienentämiseksi.

Tällaisessa tapauksessa tietosuojavaltuutetulle on toimitettava arviointia varten:
a) rekisterinpitäjän, yhteisrekisterinpitäjien ja käsittelyyn osallistuneiden henkilötietojen käsittelijöiden vastuualueet erityisesti konsernin sisällä suoritettavaa käsittelyä varten;
b) suunnitellun käsittelyn tarkoitus ja keinot;
c) toimenpiteet ja toteutetut suojatoimet rekisteröidyille kuuluvien oikeuksien ja vapauksien suojaamiseksi tämän asetuksen nojalla;
d) tapauksen mukaan tietosuojavastaavan yhteystiedot;
e) edellä artiklassa 35 säädetty tietosuojaa koskeva vaikutustenarviointi; ja
f) muut valvontaviranomaisen pyytämät tiedot.

Rekisteröidyllä on mahdollisuus saada pääsy omiin henkilötietoihinsa.

Henkilöllä on oikeus tarkastaa, mitä henkilötietoja kaupungilla hänestä on käsiteltävänä, sisältäen myös tallennetun tiedon.

Helsinki

Kuvaa tähän, miten vaatimus toteutetaan-sarake

- Tähän kuvataan se, miten vaatimus ollaan konkreettisesti toteuttamassa ja jääkö jotain toteutumatta.

- Esimerkkejä:
  - Vaatimus: Henkilötietoja kerätään ja käsitellään yhtä tai useampaa nimenomaista ja laillista käyttötarkoitusta varten, eikä niitä käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla.
  - Vastaus: Henkilötietojen käyttötarkoitus on terveydenhuollon järjestäminen ja toteutus. Henkilötietoja ei käsitellä muussa käyttötarkoituksessa.
  - Vaatimus: Henkilötietojen käsittelytoimesta on laadittu toiminnallinen kuvaus, josta ilmenevät seuraavat asiat:
    - Mitä henkilötietoja käsitellään (nimi, osoite, hetu jne.)?
    - Järjestelmässä olevien tietojen luokittelu (julkinen, salassapidettävä, arkaluonteinen jne.)
    - Miten tiedot poistetaan?
    - Tietojen säilytysaika on määritelty niiden käyttötarkoituksen mukaisesti ja niiden poistaminen säilytysajan päätyttyä toteutetaan (myös varmuuskopiot)
    - Mitä tietoja voi katsoa, mitä muokata, mitä poistaa?
  - Vastaus: Käsittelytoimen kuvaus on laadittu (linkki dokumenttiin on sarakkeessa ”Linkit tarkempaan dokumentaatioon”). Käsittelytoimen kuvauksesta ilmenevät vaatimuksessa mainitut asiat. Tietojen säilytysaikaan ja poistamiseen liittyen tullaan vielä tarkentamaan automaattisiin poistoihin liittyviä tietoja.

Linkit tarkempaan dokumentaatioon, jos muualla-sarake

- Jos kattavaa kuvausta ei ole kirjattu Kuvaa tähän miten vaatimus toteutetaan-sarakkeeseen, tähän sarakkeeseen voi lisätä linkit tarpeellisiin dokumentteihin.

Täyttyykö vaatimus? -sarake

- Tässä arvioidaan, onko käsittely tällä hetkellä suunnitellussa muodossaan Vaatimus-kentän mukaista, vai onko esiin noussut riskejä, joiden pienentämiseksi tarvitaan vielä riskienhallinnallisia toimenpiteitä.

- Jos vastataan Kyllä, tämä osa-alue on kunnossa. Jos kuitenkin tunnistetaan riskejä, ne kirjataan Tunnistetut riskit-kenttään.

- Jos vastataan Ei, siirrytään Tunnistetut riskit-kenttään.

Tunnistetut riskit-sarake

- Tähän kirjataan luettelo niistä tunnistetuista riskeistä, jotka vaikeuttavat tai estävät tietosuojan toteutumista. Riskit käsitellään tarkemmin Vaikutustenarviointi riskianalyysi-taulukon avulla.

- Riskianalyysitaulukon käyttöohje on tässä dokumentissa (dia 35→).

Täyttyykö vaatimus, voidaanko riskienhallinnan toimenpiteiden jälkeen edetä? -sarake

- Tässä arvioidaan, täytyykö vaatimus toteutettujen riskienhallinnan toimenpiteiden jälkeen, joita käsitellään Vaikutustenarviointi riskianalyysi-taulukossa.

- Jos kyllä, tämä osa-alue on kunnossa.

- Jos ei, arvioidaan, luovutaanko suunnitellusta käsittelystä liian korkeiden riskien vuoksi vai onko syytä tehdä vaikutustenarviointitaulukon rivillä 16 mainittu ennakkokuuleminen. Ennakkokuulemisesta löytyy ohjeistus tästä dokumentista (dia 47 →).

Huomioitavaa-sarake

- Tähän kirjataan tarpeelliset lisätiedot ja huomiot.

Yhteenveto päätöksentekoon-välilehti

- Tälle välilehdelle kirjataan
  - Vaikutustenarvioinnin tärkeimmät havainnot
  - Keskeisimmät korkeat jäännösriskit ja toimenpiteet niiden pienentämiseksi
  - Vaikutustenarvioinnin tekijöiden loppuarvio ja johtopäätökset

- Välilehden avulla tuotetaan yleiskuva vaikutustenarvioinnista sellaisellekin lukijalle, joka ei ole käynyt koko vaikutustenarvioinnin dokumentaatiota läpi.

Riskianalyysilomakkeen käyttäminen

Helsinki

Tietosuojatiimi

Riskianalyysilomakkeen käyttäminen

- Kun tehdään vaikutustenarviointi, riskianalyysilomaketta käytetään riskien vaikuttavuuden ja todennäköisyyden arvioimiseen sekä riskien hallintatoimenpiteiden dokumentoimiseen ja seuraamiseen.

- Vaikutustenarvioinnin työkalun Tunnistetut-riskit sarakkeeseen kirjataan riskit otsikkotasolla. Riskien tarkempi käsittely tehdään riskianalyysilomakkeella.

- Seuraavilla dioilla kuvataan riskianalyysilomakkeen käyttöä tarkemmin.

Yleistiedot-välilehti

- Täytä Yleistiedot- välilehdelle riskienhallintasuunnitelman laatineen organisaation sekä suunnitelman laatimiseen liittyvät tiedot.

Toimiala / Virasto / Liikelaitos:	
Yksikkö:	
Vaikutustenarvioinnin/riskienarvioinnin kohde:	

Laatijat:	
Laatimispäivämäärä:	
Edellinen vaikutustenarviointi laadittu:	

Muut aiheeseen liittyvät arvioinnit ja suunnitelmat	Päivämäärä	Laatijat / osallistujat	Huomioitavaa

Vaikuttavuus ja todennäköisyys-välilehti

- Tällä välilehdellä esitellään Helsingin kaupungilla käytettävät riskin vaikuttavuuden ja todennäköisyyden arviointikriteerit.

Vaikuttavuus:

Arvo	Seurauksen vakavuus
5 Merkittävä	• Riskin toteutuminen koskee erityisiä henkilötietoryhmiä, salassa pidettäviä henkilötietoja, henkilötunnuksia tai hyvin suurta määrää o Riskin toteutuessa henkilötietoja pääsee käsittelemään ulkopuolinen taho. Ulkopuolinen taho voi olla myös kaupungin toimija o Tietoja käsitellään alkuperäisen käyttötarkoituksen kanssa yhteensopimattomalla tavalla • Riskin toteutuminen voi johtaa esimerkiksi identiteettivarkauteen, kiristykseen, merkittävään taloudelli • Riskin toteutuessa kriittisen tietojärjestelmän (esim. terveystietoja sisältävän järjestelmän) käyttö est • Riskin toteutuminen edellyttää välitöntä reagointia • Suunniteltu henkilötietojen käsittely on lainvastaista • Rekisteröity ei pysty toteuttamaan oikeuksiaan lainkaan • Riskin toteutuminen aiheuttaa pysyvän luottamuksen menetyksen • Riskin toteutuminen velvoittaa ilmoittamaan tietosuojavaltuutetulle ja rekisteröidylle tietoturvaloukkauk • Suunnitellaan uudenlaista toimintaa, jonka riskit ovat vaikeasti hahmotettavissa • Seuraukset rekisteröidylle ovat pitkäaikaisia (useita kuukausia tai jopa vuosia)
4 Korkea	• Riskin toteutuminen koskee pienessä määrin erityisiä henkilötietoryhmiä, salassa pidettäviä henkilötietoja tai henkilötunnuksia. o Riskin toteutuessa henkilötietoja pääsee käsittelemään ulkopuolinen taho. Ulkopuolinen taho voi olla myös kaupungin toimija o Tietoja käsitellään alkuperäisen käyttötarkoituksen kanssa yhteensopimattomalla tavalla • Riskin toteutuminen voi johtaa esimerkiksi identiteettivarkauteen, kiristykseen, korkeaan taloudelliseen vahinkoon, henkilötietojen pa • Riskin toteutuessa kriittisen tietojärjestelmän (esim. terveystietoja sisältävän järjestelmän) käyttö vaikeutuu, josta voi aiheutua henk • Riskin toteutuminen edellyttää nopeaa reagointia • Suunniteltu henkilötietojen käsittely on kaupungin ohjeistuksen vastaista • Rekisteröidyn oikeuksien toteuttaminen on vaikeaa • Riskin toteutuminen aiheuttaa väliaikaisen luottamuksen menetyksen

Todennäköisyys:

Arvo	Luokka	Todennäköisyys	Frekvenssi
5	Odotettavissa oleva	> 90 %	Useammin kuin kerran vuodessa
4	Erittäin todennäköinen	< 90 %	Kerran 1 – 5 vuodessa
3	Todennäköinen	< 60 %	Kerran 5 – 10 vuodessa
2	Epätodennäköinen	< 30 %	Kerran 10 – 20 vuodessa
1	Mitätön	< 10 %	Harvemmin kuin kerran 20 vuodessa

Riskianalyysi-välilehti

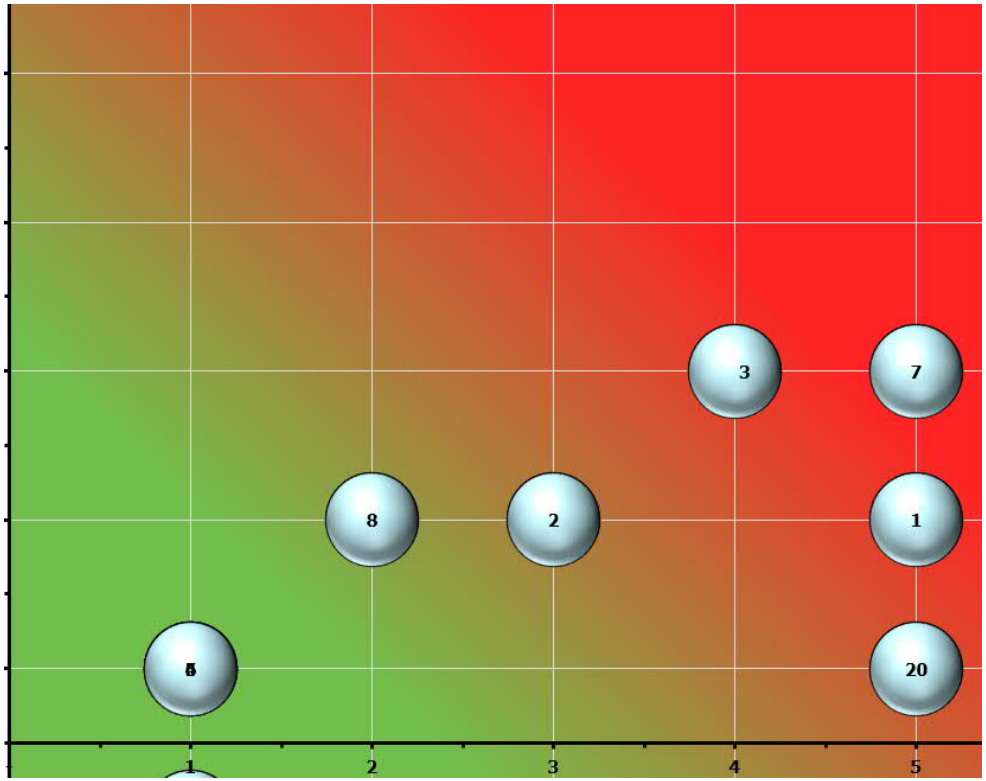
- Riskianalyysi-välilehdelle kirjataan tunnistetut riskit riskiluokittain, näiden todennäköisimmät seuraukset riskin toteutuessa sekä arvio riskin seurausten vakavuudesta ja toteutumisen todennäköisyydestä.

- Riskianalyysissä on keskeistä tunnistaa riskin toteutumiseen johtavat tekijät tai tapahtumaketjut, joihin hallintatoimenpiteillä pyritään vaikuttamaan.

- Jo aiemmin tunnistettujen riskien kohdalla täytetään myös taulukon sarakkeet "Edellinen riskiluku" sekä "Muutos". Näiden kautta seurataan riskienhallintatoimenpiteiden tarkoituksenmukaista kohdentumista.

Riskikuvaaja-välilehti

- Tälle välilehdelle piirtyy koonti kirjatuista riskeistä niiden merkittävyyden mukaisesti. Kuvioon riskit on numeroitu samalla numeroinnilla, jolla ne ovat "Riskianalyysi"-välilehdelläkin.



Riskien hallintatoimenpiteet-välilehti

- Tällä välilehdellä määritellään riskiä pienentävät tai ehkäisevät hallintatoimenpiteet vähintään niille riskeille, joiden riskiluku on 8 tai enemmän tai, jotka muutoin katsotaan sellaisiksi riskeiksi, että niihin tulee kohdentaa toimenpiteitä. Tällä välilehdellä riskit suodatetaan automaattisesti riskiluvun mukaiseen järjestykseen (suurin riskiluku ylimmäisenä).

- Hallintatoimenpiteille tulee määrittää vastuuhenkilö, joka on vastuussa toimenpiteiden toteuttamisesta sekä aikataulu, jonka mukaisesti hallintatoimenpiteet pyritään toteuttamaan. Aikatauluun on syytä kirjata myös sovittu raportointikäytänne toimenpiteiden etenemisestä.

- Kohdassa "Valmiusaste" seurataan määritettyjen hallintatoimenpiteiden toteuttamisen kulloistakin valmiusastetta (Aloittamatta - 25% - 50% - 75% - Valmis).

Miten vaikutustenarvioinnin ja riskianalyysin tuloksia hyödynnetään?

- Tietosuojariskien hallitsemiseksi on useita mahdollisuuksia:
  - Muutokset suunnitteilla olevaan prosessiin tai järjestelmään
  - Organisatoriset hallintakeinot
    - Koulutukset, ohjeet, sopimukset
  - Ennakkokuuleminen
    - Pyydetään kansallista tietosuojavaltuutettua ottamaan asiaan kantaa
  - Hankkeesta luopuminen
    - Jos riskejä ei yllä mainituilla keinoilla saada hallintaan, täytyy hanke joko lakkauttaa tai suunnitella uudelleen

Tietosuojan tarkistuslistan käyttäminen

Helsinki

Tietosuojatiimi

Tarkistuslistan käyttö

- Jos alkukartoitus on osoittanut, että henkilötietoja käsitellään, mutta varsinaista vaikutustenarviointia ei tarvitse tehdä, tulee käyttöön tietosuojan tarkistuslista

- Tietosuojan tarkistuslistalta löytyvät ne asiat, jotka on aina otettava huomioon kehittämisen aikana, vaikka ei käsiteltäisi erityisen arkaluonteista tai muutoin riskialtista henkilötietoa.

Esimerkkejä tarkistuslistan vaatimuksista

Tunnistetaan, mitä henkilörekisteriä tai rekistereitä järjestelmällä ylläpidetään. Tunnistetaan myös tarvitaanko uusi rekisteriseloste tai aiempaan rekisteriselosteeseen päivitystä ja huolehditaan, että tarvittavat muutokset tehdään.

Rekisteriselosteet hel.fi:ssä: https://www.hel.fi/helsinki/fi/kaupunki-ja-hallinto/hallinto/organisaatio/rekisteriselosteet

Käsittelylle on olemassa lainmukainen peruste.

Mahdolliset käsittelyperusteet:
a) rekisteröidyn suostumus yhtä tai useampaa erityistä tarkoitusta varten;
b) käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä;
c) käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi;
d) käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi;
e) käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi; tai
f) käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi)

Seuraavat rekisteröidyn oikeudet tulevat huomioiduksi:

1. Rekisteröidyllä on mahdollisuus saada pääsy omiin henkilötietoihinsa. *Henkilöllä on oikeus tarkastaa, mitä henkilötietoja kaupungilla hänestä on käsiteltävänä, sisältäen myös tallennetun tiedon.*

2. Rekisteröidyllä on mahdollisuus omien henkilötietojensa oikaisemiseen ja poistamiseen. *Henkilöllä on oikeus pyytää poistamaan henkilötietojaan. Tämä oikeus toteutuu, jos kaupungilla ei enää ole perustetta käsitellä tietoja tai jos henkilö peruuttaa aiemmin antamansa suostumuksen käsittelylle.*

3. Rekisteröidyllä on tietyissä tilanteissa oikeus vastustaa ja rajoittaa henkilötietojensa käsittelyä.

Jos henkilö kiistää kaupungilla olevien tietojensa paikkansapitävyyden tai käsittelyn lainmukaisuudesta on epäselvyyttä, käsittelyä voidaan rajoittaa asian selvittelyn ajaksi

Käsittelytoimen kuvaukseen tai muuhun dokumentaatioon (esim. arkkitehtuurikuvaus) sisältyy tietovirtojen kuvaus, josta selviää:

- Missä kaikkialla tietoja säilytetään ja käsitellään?
- Käsitelläänkö EU/ETA-alueen ulkopuolella vain tietosuojalinjauksissa (LINKKI) mainituin perustein?
- Millaisia rajapintoja ja käyttöliittymiä käytetään?
- Missä maissa tietoja käsitellään?
- Missä palvelimet ovat?
- Peilataanko tiedot johonkin muuhun konesaliin?
- Missä varmuuskopiot ovat?
- Pääseekö tietoihin etäyhteydellä tai muuten ja jos niin
  - kuka?
  - mistä?
  - missä tapauksissa?

Tietosuojavaltuutetun ennakkokuuleminen korkeariskisessä käsittelyssä

Helsinki

Tietosuojatiimi

Milloin tarvitaan ennakkokuuleminen?

- Rekisterinpitäjän on ennen käsittelyä kuultava valvontaviranomaista, jos tietosuojaa koskeva vaikutustenarviointi osoittaa, että käsittely aiheuttaisi korkean riskin, jos rekisterinpitäjä ei ole toteuttanut toimenpiteitä riskin pienentämiseksi.

- Jos siis vaikutustenarvioinnissa esiin tulleisiin riskeihin ei omilla riskienhallinnan toimenpiteillä pystytä vaikuttamaan, mutta käsittelyä haluttaisiin silti alkaa tekemään, on kansallisen tietosuojavaltuutetun ennakkokuuleminen pakollinen.

- Käsittelyä ei saa aloittaa ennen tietosuojavaltuutetun lausuntoa ennakkokuulemisesta.

Miten ennakkokuuleminen tehdään?

- Ennakkokuulemista varten tietosuojavaltuutetun toimistoon on toimitettava:

  a) rekisterinpitäjän, yhteisrekisterinpitäjien ja käsittelyyn osallistuneiden henkilötietojen käsittelijöiden vastuualueet erityisesti konsernin sisällä suoritettavaa käsittelyä varten;
  b) suunnitellun käsittelyn tarkoitus ja keinot;
  c) toimenpiteet ja toteutetut suojatoimet rekisteröidyille kuuluvien oikeuksien ja vapauksien suojaamiseksi tämän asetuksen nojalla;
  d) tapauksen mukaan tietosuojavastaavan yhteystiedot;
  e) edellä artiklassa 35 säädetty tietosuojaa koskeva vaikutustenarviointi; ja
  f) muut valvontaviranomaisen pyytämät tiedot

- Tietosuojavaltuutettu on ohjeistanut ennakkokuulemisesta seuraavasti: https://tietosuoja.fi/ennakkokuuleminen.


“The processing of personal data should be designed to serve mankind.”
(Recital 4 GDPR)