Tietosuojaa koskevan vaikutustenarvioinnin ja riskianalyysin tekeminen

Ohje
Tietosuoja-asiantuntija Sari Lehtonen,
Helsingin kaupunki

Tämä ohje on tehty Helsingin kaupungin käyttöön, muut organisaatiot voivat hyödyntää sitä soveltuvin osin.

Helsinki

Mitä henkilötiedot ovat ja mitä niiden käsittelyllä tarkoitetaan?

Helsinki

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

Helsinki

Mikä on tietosuojaa koskeva vaikutustenarviointi?

Helsinki

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, eli Helsingin kaupungin, tulee etukäteen, jo käsittelyä suunnitellessaan, arvioida ja dokumentoida, millaiset riskit henkilötietojen käsittelystä ihmisille aiheutuu.

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

Helsinki

Milloin vaikutustenarviointi tulee tehdä?

Helsinki

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 kaupungin omin voimin

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

Helsinki

Henkilötietojen käyttö tutkimustarkoituksiin

- Kun käsitellään erityisiä henkilötietoryhmiä (esim. rotu tai etninen alkuperä, poliittiset mielipiteet, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys, geneettiset tai biometriset tiedot, terveystiedot, seksuaalinen käyttäytyminen ja suuntautuminen) tutkimustarkoituksiin, ja rekisteröidyn oikeuksien (esim. oikeus saada pääsy tietoon, oikeus tulla unohdetuksi) toteuttamisesta halutaan poiketa, tulee vaikutustenarviointi tehdä aina.

- Tutkimustarkoituksiin on tehty oma vaikutustenarvioinnin lomakkeensa, joka löytyy intrasta.

- Tutkimusluvasta päättävä taho arvioi vaikutustenarvioinnin perusteella, millaisia riskejä tutkimus aiheuttaa henkilötietojen käsittelylle ja päättää riskiarvion perusteella, voidaanko tutkimuslupa myöntää.

- Tutkimuslupaa haettaessa vaikutustenarviointi tulee toimittaa kirjallisesti tiedoksi kansallisen tietosuojavaltuutetun toimistoon ennen käsittelyyn ryhtymistä. Tietosuojavaltuutettu on ohjeistanut tarkemmin, mitä vaikutustenarvioinnin lisäksi tulee toimittaa: https://tietosuoja.fi/rekisteroidyn-oikeuksista-poikkeaminen

Helsinki

Kuka vastaa vaikutustenarvioinnin tekemisestä?

Helsinki

Vastuu tekemisestä ja säilytyksestä

- Vaikutustenarvioinnin tekeminen on sen **hankkeen vastuulla, jonka yhteydessä järjestelmää tai prosessia suunnitellaan**. Jos erillistä hanketta ei ole, vaikutustenarvioinnin tekee se organisaation osa, jonka vastuulle järjestelmän tai prosessin käyttö kuuluu.

- Tehdyt arvioinnit tallennetaan kussakin organisaatiossa **omiin työtiloihin tai muuhun soveltuvaan tallennuspaikkaan.**

- Vaikutustenarvioinnin **eteneminen ja tulokset käsitellään osana hankkeen ohjausryhmän toimintaa tai viedään hankkeesta vastaavan viranhaltijan tietoon päätöksenteon tueksi**. Jos hanketta ei ole, päätökset tekee se viranhaltija, jonka vastuulle järjestelmän tai prosessin käyttö kuuluu.

Helsinki

Mistä apua?

- Oman organisaation **tietosuojan vastuuhenkilö** neuvoo vaikutustenarvioinnin tekemisessä ja tietosuojakysymyksissä.
    - **Huom!** Tietosuojan vastuuhenkilö ei kuitenkaan toimi vaikutustenarvioinnin työryhmän puheenjohtajana eikä hänen vastuullaan ole vaikutustenarvioinnin eteneminen.
- **Tietoturvan vastuuhenkilöllä** on tärkeä rooli avustaa vaikutustenarviointiin liittyvissä tietoturvakysymyksissä, esimerkiksi asianmukaisen tietojen suojaustason määrittelyssä.
- Muita asiantuntijoita otetaan mukaan vaikutustenarvioinnin tekemiseen tarpeen mukaan.

Helsinki

Vaikutustenarvioinnin työkalut

Helsinki

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 ja vaikutustenarvioinnin työkalu. Työkalujen käyttö aloitetaan aina alkukartoituksella, joka ohjaa eteenpäin tarvittaviin muihin työkaluihin.

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

- Tehdyt arvioinnit tallennetaan kullakin toimialalla/virastossa/liikelaitoksessa omiin työtiloihin tai muuhun soveltuvaan tallennuspaikkaan.

- Kukin toimiala/virasto/liikelaitos raportoi vaikutustenarviointien tilanteesta vuosittain tietotilinpäätökseen. Kaupungin tietosuojavastaavalle raportoidaan pyynnöstä tilanne vaikutustenarviointien suhteen.

Helsinki

Alkukartoituksen tekeminen

Helsinki

Milloin alkukartoitus tehdään

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

Helsinki

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 kaupungilla 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?

Helsinki

Varsinaisen vaikutustenarvioinnin tekeminen

Helsinki

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.

- Ennen ensimmäistä työpajaa osallistujien kannattaa katsoa tietoisku intrasta.

Helsinki

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

Helsinki

Alkukokous / agenda

- Hankkeen yhteenveto, mitä ollaan tekemässä (puheenjohtaja)
- Vaikutustenarviointi:
  - Tarkoitus (tietosuojan vastuuhenkilö)
  - Työkalun esittely (tietosuojan vastuuhenkilö)
    - Käydään vaatimukset läpi (2. sarake, ”Vaatimus”), käydään riskianalyysiin liittyvät välilehdet läpi
- 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

Helsinki

Vaikutustenarvioinnin työpaja 1

- Huom. Alla olevat ovat esimerkkejä, ryhmässä voidaan sopia myös muunlaisesta toimintatavasta.

- Ennen työpajaa:
  - Kukin vastuuhenkilö täyttää työkaluun omat rivinsä, myös tunnistetut riskit / työkalua täytetään pienryhmissä
  - Kukin vie riskit riskianalyysiin alustavalla tasolla

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

  - Päätetään, mitkä riskit viedään riskianalyysi-välilehdelle
  - Ryhmä luokittelee riskit
  - Ryhmä täyttää riskianalyysiin riskienhallinnan toimenpiteet

Helsinki

- Aikataulu: Sari Lehtonen
  - Seuraavasta työpajasta sopiminen

Vaikutustenarvioinnin lopputoimet

- Yhteenveto-välilehden täyttäminen, vaikutustenarvioinnin lopputuloksen arviointi (aina)
- Loppuraportin laatiminen päätöksentekoa varten (tarvittaessa). Pohja tähän löytyy intran tietosuojasivulta.
- Tietosuojavastaavan loppuarvion pyytäminen (tarvittaessa, jos riskit ovat korkeat), ohje tähän löytyy intran tietosuojasivulta.
- Tietosuojaviranomaisen ennakkokuuleminen, jos riskit ovat suuria eikä niitä itse saada pienennettyä (tarvittaessa)

Helsinki

Tietosuojavastaavan loppuarvio

- Jos vaikutustenarviointi osoittaa, että henkilötietojen käsittely kyseisessä tapauksessa aiheuttaisi korkean riskin, tulee olla yhteydessä kaupungin tietosuojavastaavaan loppuarvion pyytämistä varten.

- Tietosuojavastaavalta voi myös tiedustella mielipidettä ennen varsinaisen loppuarvion pyytämistä ja pyytää häneltä toimintaohjeita.

- Korkeita riskejä ovat esimerkiksi, että **tietojen käsittelyperusteesta on epäselvyyttä, käsittelystä ei jää tarvittavia lokitietoja, käsittelyssä profiloidaan rekisteröityjä, käsittelyssä hyödynnetään tekoälyä, rekisteröidyillä voi olla vaikeuksia käyttää oikeuksiaan tai tietoihin saattaa olla pääsy tahoilla, joille ne eivät kuulu.**

Tietosuojavaltuutetun ennakkokuuleminen 1/2

- Ennakkokuuleminen on toteutettava, kun vaikutustenarviointi osoittaa, että henkilötietojen käsittely aiheuttaisi korkean riskin rekisteröidylle, eikä rekisterinpitäjä ole omilla toimenpiteillään saanut riskiä alhaisemmaksi.

- Ennakkokuuleminen tulee siis tehdä, kun rekisteröidylle aiheutuvat riskit jäävät korkeiksi, mutta suunniteltua toimintaa haluttaisiin silti tehdä. Ennakkokuulemisessa kansallinen tietosuojavaltuutettu antaa kirjalliset ohjeet niistä toimenpiteistä, joihin on ryhdyttävä riskin alentamiseksi. Tarvittaessa tietosuojavaltuutettu voi ennakkokuulemisen yhteydessä käyttää myös sille tietosuoja-asetuksessa annettuja toimivaltuuksia, kuten varoitusta.

- Kun ennakkokuulemiseen on päädytty ja kaikki materiaali on lähetetty kaupungin tietosuojavastaavalle, tietosuojavastaava kaupungin yhteyspisteenä tietosuojavaltuutettuun päin lähettää tehdyn vaikutustenarvioinnin tietosuojavaltuutetulle.

Helsinki

Tietosuojavaltuutetun ennakkokuuleminen 2/2

- Tietosuojavaltuutettu toimittaa vastauksensa kaupungin tietosuojavastaavalle, joka toimittaa sen vaikutustenarvioinnin tehneelle organisaatiolle.

- Tietosuojavaltuutetun antamaan vastaukseen on perehdyttävä organisaatiossa huolellisesti. Ennen kuin henkilötietojen käsittely voidaan aloittaa, tietosuojavaltuutetun vastauksessaan määräämät toimenpiteet on toteutettava. Jos tietosuojavaltuutettu vastauksessaan kieltää käsittelyn, sitä ei saa aloittaa. Mikäli organisaatio on eri mieltä tietosuojavaltuutetun kanssa, on päätöksestä oikeus valittaa Helsingin hallinto-oikeuteen.

- Asiassa on usein tarpeen pyytää ohjeistusta kaupungin tietosuojavastaavalta.

Helsinki

Vaikutustenarvioinnin työkalun välilehdet

Helsinki

Taustatiedot-välilehti

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

Lyhyt selostus siitä, millaista henkilötietojen käsittelyä suunnitellaan:	
Toimiala / Virasto / Liikelaitos:	
Yksikkö:	
Laatijat:	
Laatimispäivämäärä:	
Hyväksyjä (viranhaltija, ohjausryhmä tms.):	
Edellinen vaikutustenarviointi laadittu:	
Muut aiheeseen liittyvät arvioinnit ja suunnitelmat, jos on:	

Helsinki

Vaikutustenarviointitaulukko-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.

Helsinki

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 käsitellä
- Järjestelmässä olevien tieto
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?

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.

Tietoja käsitellään EU/ETA-alueen ulkopuolella vain tietosuojalinjauksissa (LINKKI) mainituin perustein.

EU/ETA-alueen ulkopuolella tietoa saa käsitellä tarkan harkinnan tuloksena.

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.

Rekisteröidyllä on mahdollisuus saada pääsy omiin henkilötietoihinsa.

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

Helsinki

Ohje vaatimuksen toteutumisen arviointiin-sarake

- Tässä sarakkeessa on tarkentavaa ohjeistusta vaatimuksen toteutumisen arvioimiseksi.

- Ohjeistus koskee mm. sitä, mitä kaupungin linjauksia/ohjeita vasten vaatimuksen toteutumista tulee arvioida.

- Ohjeistuksen tarkoituksena on helpottaa vaatimusten toteutumisen arviointia ja varmistaa arviointikriteerien yhdenmukaisuus.

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.

Helsinki

Listaus tarkemmasta dokumentaatiosta

- Tähän sarakkeeseen voi listata, mistä dokumentaatiosta löytyy lisätietoa ja mistä dokumentaatio löytyy. Suoria linkkejä kannattaa välttää niiden vanhentumisen vuoksi.

Helsinki

Huomioitavaa-sarake

- Tähän kirjataan tarpeelliset lisätiedot ja huomiot.

Helsinki

Tiedonsiirtoja koskeva arvio-välilehti

- Tällä välilehdellä tehdään tiedonsiirtoja koskeva arvio, jos tietoja siirretään sellaisiin maihin EU/ETA-alueen ulkopuolelle, joiden osalta Euroopan komissio ei ole tehnyt päätöstä tietosuojan riittävyydestä.

- Arvion tekemisen tarve ilmenee Vaikutustenarviointitaulukko-välilehteä täytettäessä.

Helsinki

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.

Helsinki

Vaikuttavuus ja todennäköisyys-välilehti

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

Vaikuttavuus:

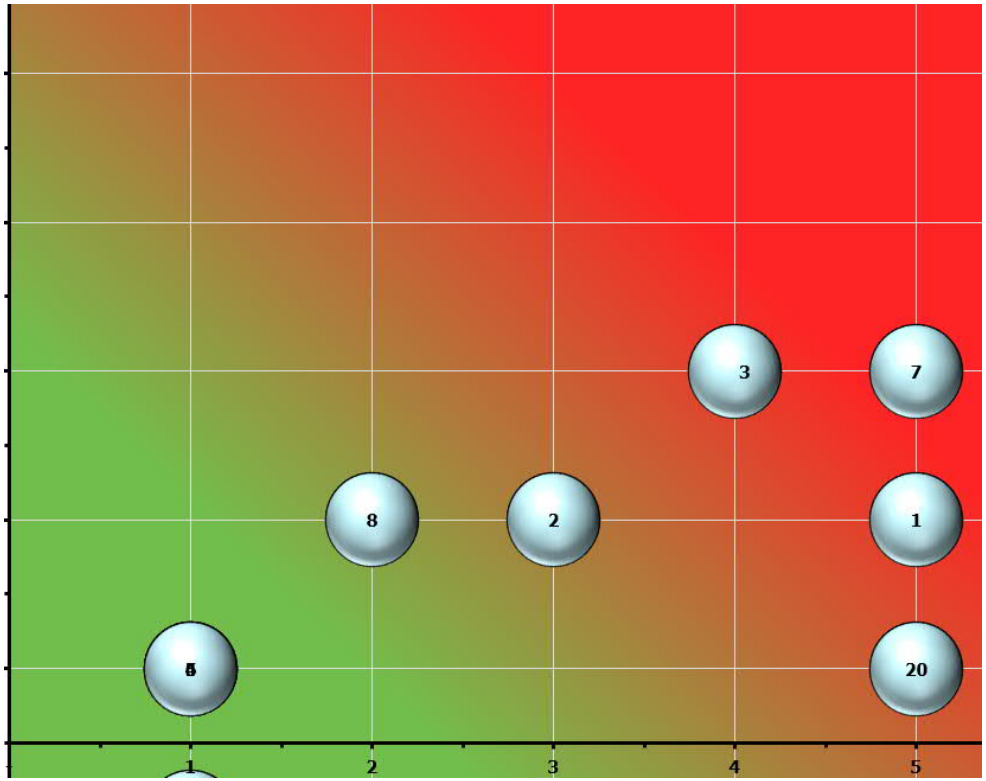
Arvo	Seurauksen vakavuus
5 Merkittävä	• Riskin toteutuminen koskee erityisiä henkilötietoryhmiä, salassa pidettäviä henkilötietoja, henkilötunnuksia tai hyvin suurta määrää henkilötietoja (satoja). o Riskin toteutuessa henkilötietoja pääsee käsittelemään ulkopuolinen taho. Ulkopuolinen taho voi olla myös kaupungin toimija, jolla ei ole oikeutta näihin tietoihin. o Tietoja käsitellään alkuperäisen käyttötarkoituksen kanssa yhteensopimattomalla tavalla • Riskin toteutuminen voi johtaa esimerkiksi identiteettivarkauteen, kiristykseen, merkittävään taloudelliseen vahinkoon, henkilötietojen paljastumiseen julkisuuteen tai merkittävään mainehaittaan • Riskin toteutuessa kriittisen tietojärjestelmän (esim. terveystietoja sisältävän järjestelmän) käyttö estyy, josta voi aiheutua henkeen ja tervevteen liittvvää vahinkoa. • 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 tietoturvaloukkauksesta • 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, jo o Tietoja käsitellään alkuperäisen käyttötarkoituksen kanssa yhteensopimattomalla tavalla • Riskin toteutuminen voi johtaa esimerkiksi identiteettivarkauteen, kiristykseen, korkeaan taloudelliseen vahinkoon, henkilötietojen paljas • Riskin toteutuessa kriittisen tietojärjestelmän (esim. terveystietoja sisältävän järjestelmän) käyttö vaikeutuu, josta voi aiheutua henkeen • Riskin toteutuminen edellyttää nopeaa reagointia • Suunniteltu henkilötietojen käsittely on kaupungin ohjeistuksen vastaista • Rekisteröidyn oikeuksien toteuttaminen on vaikeaa • Riskin toteutuminen aiheuttaa väliaikaisen luottamuksen menetyksen • Riskin toteutuminen velvoittaa ilmoittamaan tietosuojavaltuutetulle ja rekisteröidylle tietoturvaloukkauksesta • Suunnitellaan uudenlaista toimintaa, jonka riskit ovat vaikeasti hahmotettavissa • Seuraukset rekisteröidylle ovat pitkäaikaisia (useita kuukausia tai jopa vuosia)
3 Kohtalainen	• Riskin toteutuminen koskee vähäriskisiä henkilötietoja, eli muita kuin erityisiä henkilötietoryhmiä tai salassa pidettäviä henkilötietoja tai henkilötunnuksia. o Riskin toteutuessa henkilötietoja pääsee käsittelemään ulkopuolinen taho. Ulkopuolinen taho voi olla myös kaupungin toimija, jolla ei ole oikeutta näihin tietoihin. o Tietoja käsitellään alkuperäisen käyttötarkoituksen kanssa yhteensopimattomalla tavalla • Riskin toteutuminen voi johtaa lievään taloudelliseen vahinkoon, henkilötietojen kiusalliseen paljastumiseen julkisuuteen sekä lievään mainehaittaan • Riskin toteutuessa ei-kriittisen tietojärjestelmän (esim. kirjaston asiakkaiden tietoja sisältävän järjestelmän) käyttö estyy, mistä ei kuitenkaan voi aiheutua henkeen ja terveyteen liittyvää vahinkoa. • Riskin toteutuminen edellyttää reagointia

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

Riskikuvaaja-välilehti

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



Helsinki

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).

Helsinki

Yhteenveto päätöksentekoon-välilehti

- Tähän kootaan vaikutustenarvioinnin keskeisimmät havainnot, merkittävimmät riskit ja vaikutustenarvioinnin tekijöiden loppuarvio ja johtopäätökset.

- Tarkoituksena on tuottaa yhteenveto, josta saa käsityksen vaikutustenarvioinnin tuloksista ja jatkotoimista päätöksentekoa varten.

- Erillisen loppuraporttipohjan mukainen loppuraportti on hyvä laatia päätöksenteon tueksi. Silloin, jos kyse on hyvin merkittävästä ja riskialttiista käsittelystä, loppuraportti on laadittava, mutta muulloinkin se on hyödyllinen.

Helsinki

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

Helsinki

Tietosuojan tarkistuslistan käyttäminen

Helsinki

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.

Helsinki

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?

Helsinki


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