Rauman kaupunki

Tietosuojapolitiikka ja tietoturva

Rauman kaupungin tieto- ja asianhallinnan poikkihallinnollinen tiimi

Kaupunginvaltuusto hyväksynyt 18.6.2018 § 56, RAU/475/07.01.01/2018
Päivitetty 1.8.2019

Sisällys

1. Johdanto

Rauman kaupungin tietosuojapolitiikka tukee Rauman kaupungin strategian, Rauma Tarinan mukaisesti palvelujen tuottamista asukaslähtöisesti, tehokkaasti ja turvallisesti. Politiikka on laadittu EU:n yleisen tietosuoja-asetuksen, tietosuojalain (1050/2018) ja muun noudatettavan keskeisen lainsäädännön mukaisesti ja se pitää sisällään myös tietoturvan.

Raumalla tuotetaan palvelut monikanavaisesti uusia teknologioita hyödyntäen, jolloin ICT-palvelujen on oltava mahdollisimman tehokkaita, virheettömiä ja luotettavia. Palveluiden tuottaminen ja kehittäminen perustuvat luotettavaan, ajantasaiseen ja keskeytyksettömään tietotuotantoon.

Politiikka koskee kaikkea Rauman kaupungin käyttämää, omistamaa ja hallinnoimaa **tietoa** riippumatta tiedon esitystavasta tai tiedon elinkaaren vaiheesta, jossa Rauman kaupunki toimii rekisterinpitäjänä. Valtaisan sähköisen tietomäärän lisäksi Rauman kaupungin hallussa on myös mittavasti muissa muodoissa olevaa tietoa. Kaikki nämä asiakirjat, sopimukset, lomakkeet ja ohjeet tulee turvata asianmukaisesti ja yhtenäisten käsittelysääntöjen mukaisesti.

Tietosuojapolitiikka koskee jokaista Rauman kaupungin kanssa palvelussuhteessa olevaa työntekijää, viranhaltijaa ja määräaikaista henkilöä sekä luottamushenkilöä ja yhteistyökumppania. Rauman kaupungin henkilöstön ja sen luottamushenkilöiden sekä muiden ulkopuolisten tahojen tulee sitoutua noudattamaan tietosuojapolitiikkaa, niihin sisältyviä ohjeita sekä kansallisia normeja ja ohjeita.

Tärkeää tietosuojassa on koko henkilöstön asennoituminen ja käytännön toiminta. Vain tällä tavoin turvallisuuskulttuuri saadaan sisäänrakennetuksi osaksi kaupungin **toimintakulttuuria**. Tietojenkäsittelyyn liittyy aina inhimillisenä toimintana riskejä, joita minimoidaan mm. ohjeistuksilla, teknisillä ratkaisuilla ja koulutuksella. Tärkeintä ovat jokaisen henkilön päivittäisessä tietojen käsittelyssä tekemät ratkaisut ja toimenpiteet, jotka pohjautuvat lainsäädännön ja ohjeiden noudattamiseen.

Politiikka on koko henkilöstön saatavilla intranetissä ja se on osa henkilöstön perehdytysohjelmaa. Lisäksi palveluiden käyttäjiä ohjeistetaan tarpeen mukaan.

Yhteistyökumppanien ohjeistamisesta vastaa tilaaja. Periaatteena on, että kaikki jotka käsittelevät kaupungin tietoa, ovat saaneet riittävän perehdytyksen tiedon turvalliseen ja asianmukaiseen käsittelyyn.

2. Tietosuojapolitiikan tarkoitus

Tämä tietosuojapolitiikka osanaan tietoturva määrittelee ne **tavoitteet, tietosuojaperiaatteet, toimintatavat, vastuut, valvonnan ja seuraamusjärjestelmän,** joita noudatetaan Rauman kaupungin tietosuojan toteuttamisessa ja kehittämisessä. Tarkoituksena on varmistaa, että ihmisten oikeus **henkilötietojen suojaan** ja sitä kautta yksityisyyteen toteutuu myös digitaaliaikana. Sääntely pyrkii vastaamaan teknologian nopean kehityksen haasteisiin ja vahvistamaan ihmisten oikeutta valvoa henkilötietojaan.

Rauman kaupungin tietosuojapolitiikka **toimii perustana sitä täydentäville periaatteille ja ohjeille**, jotka voivat tarkentaa yksityiskohtaisemmin tässä politiikassa annettuja tietosuojaa tai tietoturvaa koskevia periaatteita ja määräyksiä.

Tietoturvatyö tarkoittaa halutun tietoturvallisuuden ja -suojan tason saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja niiden käytännön toteuttamista. Tämä työ kattaa kaikki tietojen turvaamisen menetelmät, välineet, toimenpiteet, määräykset, ohjeistuksen, koulutuksen ja viestinnän. Lisäksi se tarkoittaa varautumista erilaisiin uhkatilanteisiin sekä sovittujen toimintatapojen noudattamista. Rauman kaupunki osoittaa tarvittavat resurssit turvallisuuden varmistamiseksi.

3. Määritelmät

Tietosuojan, tietoturvan ja yksityisyyden toteutuminen tehokkaasti käytännössä vaatii tiedon luottamuksellisuuden, eheyden, saatavuuden ja tarvittaessa myös kiistämättömyyden toteutumista. Tässä kappaleen määritysten lisäksi tietosuojaan liittyviä keskeisiä käsitteitä on määritelty liitteessä 1. (Liite 1. Keskeiset käsitteet ja sanastoa.)

Tietosuoja

Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä. Tietosuoja tulisi aina ottaa huomioon silloin kun käsitellään henkilötietoja. Tietosuojaan kuuluvat ihmisten yksityiselämän suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä.

Henkilötietojen käsittelyn on aina perustuttava lakiin. Riippumaton viranomainen valvoo henkilötietojen suojaa koskevien säännösten noudattamista. (https://tietosuoja.fi/tietosuoja, luettu 1.8.2019.)

Tietosuojaseloste

Seloste on rekisterinpitäjän antama informaatio siitä, miten se menettelee haltuunsa saamiensa henkilötietojen käsittelyssä, mitkä ovat rekisteröidyn oikeudet ja miten oikeudet toteutetaan (vrt. HetiL 24 §).

Rekisterinpitäjä

Rekisterinpitäjä on se valiokunta, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä.

Tietoturva

Tietoturvalla tarkoitetaan niitä hallinnollisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus, eheys ja tietoresurssien käytettävyys sekä saatavuus.

Tietoturvallisuudella Rauman kaupungissa tarkoitetaan tiedon, tietojärjestelmien, tietoliikenteen ja palveluiden, sekä niiden käyttöympäristöjen turvaamista siten, että niihin kohdistuvat uhat eivät aiheuta merkittävää riskiä tiedon elinkaaren missään vaiheessa.

Luottamuksellisuus
- Tieto on vain tietoon oikeutettujen käyttäjien ja tietojärjestelmien käytettävissä sovituilla tavoilla ja sovittuun aikaan
- Tietoa ei paljasteta tai muutoin saateta sivullisten tietoon

Eheys
- Tieto on koko elinkaaren ajan luotettavaa, oikeellista ja ajantasaista
- Tieto ei pääse muuttamaan tahallisesti tai tahattomasti, eikä se voi muuttua laitteistosta tai ohjelmistosta johtuvan vian tai teknisen häiriön seurauksena

Saatavuus
- Tiedon, tietojärjestelmän tai palvelun tulee olla siihen oikeutettujen henkilöiden ja tietojärjestelmien saatavilla sekä käytettävissä silloin kun sitä tarvitaan

Kiistämättömyys
- Tietoon kohdistuvat käsittelytoimenpiteet suoritetaan siten, että käsittelyn osapuolet voidaan aina yksiselitteisesti tunnistaa sekä toimenpiteiden aikana että jälkikäteen koko tiedon elinkaaren aikana

4. Tavoitteet

Rauman kaupungin tavoitteena on saavuttaa luottamuksellinen toimintakulttuuri, jossa EU:n yleistä tietosuoja-asetusta **ja tietosuojaperiaatteita noudatetaan** kaikissa henkilötietojen käsittelyvaiheissa.
Tavoitteena on myös saavuttaa tietoturvallisuusasetuksen (681/2010) kuvaaman **tietoturvallisuuden perustason** vaatimukset kaupungin laajuisesti. Lisäksi tavoitteena on **turvata palveluiden jatkuvuus** varautumalla erilaisiin riskeihin. Organisaatio kykenee osoittamaan noudattavansa asetusta. Tavoitteeseen pyritään seuraavilla toteutuksilla:

- Toteutettu henkilötietovarantojen kuvaus, ylläpito ja informaatio, sisältäen henkilötietovirrat
- Organisoitu tietosuojatyö, jossa resurssit ja vastuunjako ovat selkeät, toimintakulttuuri sisältää tietosuojariskien hallinnoinnin
- Koko Rauman kaupungin henkilökunnalla on ajan tasalla oleva ja riittävä tietoturvallisuus- ja tietosuojaosaaminen tehtäviensä suorittamiseksi
- Tekniset ja hallinnolliset tietoturvajärjestelyt ovat ajan tasalla ja täyttävät keskeisiltä osin perustason vaatimukset
- Tietoturvapoikkeamia kyetään seuraamaan ja hallitsemaan

- Tavoitteena on kuvatut tietosuoja- ja tietoturvaprosessit, sisältäen seuraamuskäytännöt tietoturva- ja tietosuojarikkomuksissa
- Tavoitteena on tietosuojan seuranta, valvonta ja jatkuva kehittäminen, sisältäen tietotilinpäätöksen

5. Tietosuojan periaatteet ja toteuttaminen

Sisäänrakennettu ja oletusarvoinen tietosuoja

Tietosuoja on kiinteä osa Rauman kaupungin palveluita ja toimintaa, sekä jokaisen käyttäjän työtapoja. Henkilötietojen käsittelyä koskevat periaatteet toimivat ohjenuorana kaikissa henkilötietojen käsittelyvaiheissa. Sisäänrakennetun ja oletusarvoisen tietosuojan periaatteiden mukaisesti tietosuojaa koskevat kysymykset tunnistetaan ja otetaan huomioon johtamisessa, hankinnoissa/sopimuksissa, toimintaprosesseissa sekä kehittämistyössä. Tietosuoja ja sen osa-alue tietoturva ovat kiinteä osa Rauman kaupungin kokonaisturvallisuutta sekä riskien hallintaa.

Riskienhallinta

Riskienhallinnan avulla palveluihin, toimintaan ja tietoon kohdistuvia riskejä hallitaan järjestelmällisesti ja ennakoivasti. Riskienhallintakäytäntöjen tavoitteena on riskien rajoittaminen hyväksyttävälle tasolle niin, että käytetyt keinot ovat suhteessa palvelun ja toiminnan kriittisyyteen ja arvioidun riskin suuruuteen. Palveluiden kriittisyyden luokittelu auttaa jatkuvuuden hallinnassa ja auttaa kohdentamaan poikkeusolojen toimenpiteet palveluiden kriittisyyden mukaan. Riskienhallinta kuuluu jokaisen kaupungin työntekijän vastuulle.

Rauman kaupunki rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. EU:n yleinen tietosuoja-asetus korostaa erityisesti suuririskisessä henkilötietojen käsittelyssä riskien ja niiden vaikutusten arviointia.

Rauman kaupunki toteuttaa riskilähtöisen toimintaperiaatteen varmistamiseksi tietosuojan vaikutustenarvioinnin sekä tarvittaessa ennakkokuulemisen sellaisten henkilötietojen käsittelytoimille, joiden suunnitteluvaiheessa on todennäköistä, että käsittelytoimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä.

Henkilötiedon elinkaari

Tietosuojan toteuttamisessa Rauman kaupunki haluaa varmistaa tietosuojalainsäädännön vaatimusten toteutumisen koko henkilötietojen elinkaaren ajan. Tietosuoja tulee huomioida tiedon keruun, käytön, säilytyksen/arkistoinnin, luovutuksen, tiedonsiirron, hävittämisen ja anonymisoinnin vaiheissa. Oletusarvoisen tietosuojaperiaatteen mukaisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja.

Rauman kaupunki edellyttää sopimuskumppaneiltaan hyvää, asetuksen mukaista henkilötietojen käsittelytapaa. Tietosuoja huomioidaan jo tarjouspyyntö- ja hankintavaiheessa.

Suostumuskäytäntö

Henkilötietojen käsittelylle on oltava aina laissa säädetty oikeusperuste. Erityisiin henkilötietoryhmiin kuuluvien arkaluonteisten henkilötietojen käsittely on lähtökohtaisesti kiellетty. Tietojen käsittelyn oikeusperusteet on määritelty tietosuojaselosteissa. Henkilötietoja voidaan käsitellä myös, jos asianomainen henkilö on antanut suostumuksensa häntä koskevien tietojen käsittelyyn. Suostumuksella tarkoitetaan kaikenlaista vapaaehtoista, yksilöityä, tietoista tahdonilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn.

Tietosuoja-asetuksessa suostumuskäytäntö jaetaan edelleen suostumukseen ja nimenomaiseen suostumukseen erityisiin henkilötietoryhmiin kuuluvien osalta. Erityisten henkilötietoryhmien osalta suostumuksen on oltava nimenomainen, millä tarkoitetaan mm. korostettua yksilöintivaatimusta sekä pääsääntöistä tarvetta saada suostumus kirjallisesti.

Rekisteröityjen oikeudet

Rekisteröidyllä on oikeus saada tietoa hänen henkilötietojensa keräämisestä sekä käsittelystä. Rekisteröityä informoidaan muun muassa henkilötietojen käsittelyn käyttötarkoituksesta, rekisterien tietosisällöstä sekä siitä, mihin tietoja luovutetaan.

Rauman kaupungissa on määritetty toimintaprosessi, ohjeet ja asiakirjapyyntölomakkeet liittyen rekisteröityjen käyttäessä oikeuttaan saada tietoa rekistereissä olevista henkilötiedoistaan sekä toimintaan tietosuoja- ja tietoturvaloukkausten tapahtuessa. Prosessit, ohjeet ja lomakkeet löytyvät Jemman Tietosuojasivustolta ja nettisivuilta.

6. Tietosuojan organisointi, roolit ja vastuut

Tietosuojan toteuttaminen on jatkuvaa, laaja-alaista ja koskettaa koko henkilöstöä ja kaikkia rekisteröityjä. Tietosuojan organisoinnilla pyritään riskien pienentämiseen sekä muodostamaan toimintakulttuurista sellainen, että tietoja ja tietojärjestelmiä osataan käsitellä oikeaoppisesti. Tietosuojan vastuut ja roolit on kuvattu liitteessä 2. (Liite 2, Tietosuojan organisointi, roolit ja vastuut.)

7. Tietojärjestelmien käyttöperiaatteet

Kaikki Rauman kaupungissa käytössä olevat ICT -palvelut, -sovellukset, -järjestelmät ja -laitteet, mukaan lukien mobiililaitteet, on tarkoitettu työtehtävien hoitamista varten.

Kaupungin tietojärjestelmiä ja laitteistoa ei saa käyttää sellaiseen toimintaan, mikä voi välittömästi tai välillisesti vaarantaa kaupungin vastuulla olevan tiedon ja/tai järjestelmien tai laitteiden turvallisuuden ja aiheuttaa näin haittaa kaupungille tai sen toiminnalle.

Tietojärjestelmiä, laitteita ja ohjelmistoja Rauman kaupungin tietoverkkoon saa liittää ja asentaa vain kaupungin tietotekniikka tai sen valtuuttama taho.

Tietoturvallisuuteen liittyviin väärinkäytöksiin puututaan viipymättä kaupungin normaalein kurinpitomenettelyin.

Henkilö syyllistyy tietoturvarikkomukseen, jos hän rikkoo tietoturvaohjeistusta työssään tai syyllistyy tiedon käsittelyn suhteen laissa määriteltyyn rikokseen. Jokainen Rauman kaupungin työntekijä on vastuussa työtehtäviinsä liittyvästä tietoturvallisuudesta ja myös sen rikkomisen ilmoittamisesta.

Tietotekniikka toteuttaa tietoturvallisuuden teknistä valvontaa kaupungin tietojärjestelmäympäristössä yhteistoimintaneuvotteluissa sovituin menetelmin.

8. Toiminta tietosuoja- ja tietoturvapoikkeamatilanteissa sekä ilmoitusvelvollisuus

Rauman kaupungissa on määritetty toimintaprosessi ja ohje liittyen toimintaan tietosuoja- ja tietoturvaloukkausten tapahtuessa (Liite 3, Tietoturvapoikkeamien käsittelyprosessi). Ilmoituskäytäntö (HaiPro) ja ohjeet löytyvät Jemman Tietosuojasivustolta.

Henkilötietojen tietoturvaloukkauksen sattuessa Rauman kaupungilla on rekisterinpitäjänä ilmoitusvelvollisuus valvontaviranomaiselle sekä rekisteröidylle. Ilmoituksen valvontaviranomaiselle tekee tietosuojavastaava tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturvaloukkaus on tullut ilmi. Rekisteröidylle henkilötietojen tietoturvaloukkaus ilmoitetaan ilman aiheetonta viivytystä. Tietoturvapoikkeamasta ilmoitetaan tarvittaessa myös kyberturvakeskukselle.

9. Tietosuojarikkomukset ja seuraamukset

Rauman kaupungin tietosuojarikkomukset käsitellään tapauskohtaisesti ja mahdollisiin seuraamuksiin sovelletaan erikseen kuvattua ja liitteenä olevaa tietosuojarikkomusten seuraamustaulukkoa (Liite 4, Tietosuojarikkomusten seuraamustaulukko ja vastuut).

10. Tietosuojan seuranta, arviointi ja kehittäminen

Tietosuojavastaavan ja tietosuojatyöryhmän tehtävänä on seurata ja arvioida tietosuojan tilannetta Rauman kaupungilla. Kehittämistoimenpiteistä sovitaan tieto- ja asianhallinnan poikkihallinnollisessa tiimissä ja esitetään kaupungin johtoryhmälle päätettäväksi.

Tietotilinpäätös laaditaan osana talousarvioprosessia.

LIITTEET

Liite 1. Keskeiset käsitteet ja sanastoa
Liite 2. Tietosuojan organisointi, roolit ja vastuut
Liite 3. Tietoturvapoikkeamien käsittelyprosessi
Liite 4. Tietosuoja- ja tietoturvarikkomusten seuraamustaulukko

MUUTOSHISTORIA		
Pvm	**Asia**	**Laatija**
12.4.2018	LUONNOS Käsittely Tietosuojaprojektin johtoryhmä	Kristiina Kuusio
3.5.2018	LUONNOS Käsittely Tietosuojaprojektin johtoryhmä	K. Kuusio
14.5.2018	LUONNOS Käsittely YT toimikunta	K. Kuusio
15.5.2018	LUONNOS Käsittely Rauman kaupungin johtoryhmä	K. Kuusio
21.5.2018	LUONNOS Esittely Rauman tekninen valiokunta	K. Kuusio
22.5.2018	LUONNOS Käsittely Sivistysvaliokunta	K. Kuusio
29.5.2018	LUONNOS Käsittely Sosiaali- ja terveysvaliokunta	K. Kuusio
5.6.2018	LUONNOS Käsittely Rauman kaupungin johtoryhmä	K. Kuusio
5.6.2018	LUONNOS Käsittely Rauman tekninen valiokunta	K. Kuusio
11.6.2018	Käsittely Rauman kaupunginhallitus	Minna Liikanen / Kuusio
18.6.2018	Hyväksyminen Rauman kaupunginvaltuusto	M. Liikanen / Kuusio
1.8.2019	Päivitetty; Sharepoint vaihdettu Jemmaksi Työryhmä kirjattu tieto- ja asianhallinnan poikkihallinnolliseksi tiimiksi s. 4 Tietosuojan määritelmää tarkennettu. s. 8 HaiPro ilmoituskäytäntö ja kyberturvakeskus lisätty. Liitteet 3 ja 4 päivitetty. Liite 5 poistettu, koska tietotilinpäätös on toimitettu erikseen.	K. Kuusio