TIETOSUOJA- JA TIETOTURVAPOLITIIKKA

Utajärven kunta

Kunnanhallitus 4.9.2023 § 164

Sisällys

1. Tietosuoja- ja tietoturvapolitiikka 2
1.1 Tietoturva 2
1.2 Tietosuoja 3
2. Tietosuoja- ja tietoturvatyön tavoitteet ja periaatteet 3
2.1 Tietosuojavastaavan asema 4
3. Tietoturvan ja tietosuojan varmistaminen hankinnoissa 4
4. Seuranta, arviointi ja riskienhallinta 5
4.1 Riskienhallinta 5
4.2 Lokitietojen kerääminen ja hallinta 6
4.3 Käyttöoikeuksien hallinta 7
5. Menettely tietosuojan tai tietoturvallisuuden vaarantuessa 8
6. Varautuminen 8
6.1 Viestintä häiriötilanteessa 9
7. Tietosuoja- ja tietoturvarikkomukset 9
8. Organisointi ja vastuut 9
8.1 Kunnanhallitus 10
8.2 Kunnanjohtaja 10
8.3 Toimialajohtaja 10
8.4 Tietohallintopäällikkö 11
8.5 Esihenkilö 11
8.6 Tietosuoja- ja tietoturvaryhmä 12
8.7 Tietosuojavastaava 12
8.8 Tietojärjestelmän ja tietovarannon omistaja 12
8.9 Tietojärjestelmän pääkäyttäjä 13
8.10 Asiakirjahallinnosta vastaava viranhaltija 13
8.11 Työntekijät ja viranhaltijat 13
8.12 Luottamushenkilöt 13
8.13 Tytäryhtiöt 13
8.14 Ulkoiset palveluntuottajat 14

1. Tietosuoja- ja tietoturvapolitiikka

Tietosuoja- ja tietoturvapolitiikka on Utajärven kunnanhallituksen hyväksymä strateginen asiakirja ja kannanotto tietosuojan ja tietoturvallisuuden toteuttamiseen Utajärven kunnassa. Politiikka määrittää tietosuojan ja tietoturvallisuuden periaatteet ja tavoitteet, sekä organisoinnin ja vastuut. Utajärven kunta on sitoutunut kaikessa toiminnassaan lainsäädäntöön perustuvaan tietosuojan ja tietoturvallisuuden toteuttamiseen, ylläpitoon sekä jatkuvaan kehittämiseen. Politiikan avulla vahvistetaan yhdenmukaisia toimintaperiaatteita ja käytäntöjä Utajärven kunnassa hyvän tietosuojan ja tietoturvatason saavuttamiseksi. Politiikka on myös osa kunnan riskienhallintaa. Tietotekniikan hyödyntäminen sekä tietotekniikkaan ja tietoturvallisuuteen panostaminen ovat johdon strategisia päätöksiä, joilla vaikutetaan kunnan toimintakykyyn.

Tietojenkäsittely eli tietojen kerääminen, säilyttäminen, käyttö, siirtäminen ja luovuttaminen on edellytys kunnan toiminnalle ja palveluiden tuottamiselle. Tietojenkäsittelyn toimivuus, tehokkuus ja virheettömyys ovat keskeisiä tekijöitä kunnan palveluita tuotettaessa. Kunnan toiminnassa käytettävät tietojärjestelmät ja tietoaineistot sisältävät usein asiakkaisiin, työntekijöihin ja toimintaan liittyvää tietoa, joka on lainsäädännön perusteella suojattava. Hyvä tietosuojan ja tietoturvallisuuden hallinta edellyttää toiminnan jatkuvaa arviointia, seurantaa, pitkäjänteistä suunnittelua sekä riittävää resursointia erilaisten poikkeusolojen ja uhkatilanteiden varalle. Tietosuojan ja tietoturvallisuuden toteuttaminen vaatii sovittujen ohjeiden ja toimintatapojen noudattamista, koulutusta sekä viestintää.

Tämä tietosuoja- ja tietoturvapolitiikka kattaa Utajärven kunnan kaikkeen toimintaan liittyvät tietojenkäsittelyn tehtävät. Jokaisen Utajärven kunnan viranhaltijan, työntekijän ja luottamushenkilön on tunnettava tietosuoja- ja tietoturvapolitiikka sekä noudatettava siinä määritettyjä periaatteita ja sen perusteella annettuja ohjeistuksia. Organisaation ulkopuolisten toimijoiden tulee myös sitoutua noudattamaan tätä politiikkaa, kansallisia normeja sekä ohjeita ehtona pääsylle kunnan tietojärjestelmiin ja tietoaineistoihin. Politiikkaa täydentävät ja täsmentävät kunnan sisäiset tietosuojaa ja tietoturvallisuuttaa koskevat ohjeet ja määräykset.

1.1 Tietoturva

Tietoturva eli tietoturvallisuus on osa organisaation kokonaisturvallisuutta. Tietoturvalla tarkoitetaan hallinnollisia, toiminnallisia ja teknisiä toimia, joilla varmistetaan eri muodossa olevan tiedon luottamuksellisuus, eheys ja käytettävyys sen koko tiedon elinkaaren ajan. Tietoturvallisuuden osa-alueita ovat;

- Hallinnollinen turvallisuus (mm. organisointi, resurssit ja osaaminen)
- Fyysinen turvallisuus (mm. säilytys, käsittely ja tilojen suojaaminen)
- Tekninen turvallisuus (mm. laitteistot, tietoliikenne, tietojärjestelmät ja ohjelmistot)

Hyvä tietoturvataso tukee kunnan palvelujen tuottamista. Tietoturvallisuuden varmistamisen tarkoituksena on taata kunnan toiminnan jatkuminen ja minimoida toiminnalle aiheutuvat riskit ja vahingot. Kunnan tulee varmistaa, että tiedot ovat vain niiden tahojen käytettävissä, joilla käyttöön on asianmukainen oikeus. Tiedon oikeellisuus ja muuttumattomuus on myös suojattava. Lisäksi tiedon ja kriittisten palveluiden käytettävyys on varmistettava. Vastuu tietoturvallisuuden

toteutumisesta kuuluu jokaiselle tietojärjestelmien ja tietoaineistojen kanssa työskentelevälle. Tietoturvallisuuden toteuttaminen ja hallinta vaatii kouluttautumista, ohjeistuksen seuraamista ja perehtymistä. Tietoturva on yksi tietosuojan toteuttamisen keino.

1.2 Tietosuoja

Henkilötietojen suoja on jokaiselle rekisteröidylle kuuluva perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä. Henkilötietojen käsittelyn on oltava asian- ja tarkoituksenmukaista. Henkilötietojen keräämiselle, tallentamiselle ja säilyttämiselle täytyy olla tietosuoja-asetuksen mukainen peruste. Kunnan tulee varmistua siitä, että kunnan tehtävien hoito ja palveluiden tuottaminen toteutetaan kuntalaisten, kunnan asiakkaiden ja muiden rekisteröityjen yksityisyyttä kunnioittaen.

2. Tietosuoja- ja tietoturvatyön tavoitteet ja periaatteet

Tietosuoja- ja tietoturvatyön tavoitteena on ylläpitää, kehittää ja parantaa kunnan toiminnan luotettavuutta, jatkuvuutta laatua, sekä riskienhallintaa ja varautumista. Tietosuoja- ja tietoturvatyö on kiinteä osa kunnan johtamista, riskien- ja laadunhallintaa sekä palvelutoimintaa. Utajärven kunta toteuttaa sisäänrakennetun ja oletusarvoisen tietosuojan ja tietoturvallisuuden periaatteita. Tämä tarkoittaa, että tietosuoja ja tietoturvallisuus huomioidaan mahdollisimman varhaisessa vaiheessa toiminnan tai siihen kohdistuvien muutosten suunnittelua. Tavoitteiden ja periaatteiden toteutumista arvioidaan vuosittain laadittavassa tietotilinpäätöksessä.

Utajärven kunnan tietosuoja- ja tietoturvatyön tavoitteet ja periaatteet ovat:

- Varaudumme kunnan tuottamien palveluiden jatkuvuuteen tunnistamalla ja hallitsemalla tietojärjestelmiin, tietovarantoihin ja tietoliikenteeseen kohdistuvat riskitekijät.
- Kehitämme aktiivisesti henkilöstön tietosuoja- ja tietoturvaosaamista sekä tietoisuutta.
- Varmistamme tietosuojan ja tietoturvallisuuden toteutumisen läpi toiminta- ja hankintaketjujen.
- Mitoitamme ja järjestämme kunnan toimintaympäristön siten, että toiminta on tehokasta ja se edistää tietosuojan ja tietoturvallisuuden toteutumista kunnan eri toiminnoissa.
- Varmistamme että kunnan tietojärjestelmiä ja tietovarantoja käyttävät vain henkilöt, joilla on niihin asianmukainen oikeus, sekä käyttöoikeudet on määritetty vähimpien oikeuksien periaatteiden mukaisesti.
- Valvomme järjestelmällisesti tietosuojan ja tietoturvallisuuden toteutumista toimintaympäristössä.
- Noudatamme henkilötietojen käsittelyssä tietosuoja-asetuksen mukaisia periaatteita, joita ovat lainmukaisuus, kohtuullisuus ja avoimuus, täsmällisyys, eheys ja luottamuksellisuus, käyttötarkoitussidonnaisuus, sekä tietojen minimointi ja säilytyksen rajoittaminen.
- Varmistamme että toiminnassa käytettävä tieto on oikeaa, ajantasaista, luotettavaa ja sitä käsitellään lainmukaisesti, ja että julkinen tieto on helposti löydettävissä ja käytettävissä.
- Varmistamme että tietosuoja-asetuksen mukaiset rekisteröityjen oikeudet toteutuvat kunnan toiminnassa.

2.1 Tietosuojavastaavan asema

EU:n yleisen tietosuoja-asetuksen mukaan kunnan tulee nimittää tietosuojavastaava. Kunnan tulee määritellä tietosuojavastaavan asema organisaatiossa, resurssit ja valtuudet siten, että hänellä on edellytykset hoitaa tietosuojavastaavalle kuuluvat tehtävät organisaatiossa. Tietosuoja-asetus sisältää yksityiskohtaiset säännökset tietosuojavastaavan asemasta ja tehtävistä.

Tietosuojavastaava on tehtävässään riippumaton eikä hän saa ottaa vastaan ohjeita asetuksen mukaisten tehtävien hoitamisen yhteydessä. Tietosuojavastaava raportoi suoraan rekisterinpitäjän tai henkilötietojen käsittelijän ylimmälle johdolle. Tehtäviään suorittaessa tietosuojavastaavaa sitoo salassapitovelvollisuus Euroopan unionin lainsäädännön tai kansallisen lainsäädännön mukaisesti.

Tietosuojavastaava on otettava asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn ja kehittämiseen, esimerkiksi, kun suunnitellaan tai kehitetään tietojärjestelmiä ja tietovarantoja. Hänelle on asetuksen mukaan annettava riittävät resurssit sekä pääsy henkilötietoihin ja käsittelytoimiin. Tietosuojavastaavalle on varattava riittävä perehdytys ja koulutus asiantuntemuksen ylläpitämiseksi.

Rekisterinpitäjä tai henkilötietojen käsittelijä ei saa erottaa tai rangaista tietosuojavastaavaa sen vuoksi, että hän on hoitanut tehtäviään tietosuojavastaavana. Tietosuojavastaava voi tehtävänsä ohella suorittaa muita tehtäviä, mutta ne eivät saa aiheuttaa eturistiriitoja.

3. Tietoturvan ja tietosuojan varmistaminen hankinnoissa

Utajärven kunta voi ulkoistaa osan toimintaansa liittyvästä tietojenkäsittelystä tai ICT-palvelutuotannosta sopimusperusteisesti, esimerkiksi hankkimalla kunnan toiminnassa tarvittavan tietojärjestelmän kunnan käyttöön toimittajalta palveluna. Kunta valitsee sopimuskumppanikseen vain sellaisia toimijoita, jotka noudattavat voimassa olevaa lainsäädäntöä ja hyvää henkilötietojen käsittelytapaa.

Hankinnan vastuutahon tulee huolehtia, että hankinnan suunnittelussa tunnistetaan vaikutukset kunnan tiedonhallintaan ja henkilötietojen käsittelyyn, sekä vaatiiko hankinnan kohde erityisiä tietoturvamenettelyitä. Jos hankinnasta seuraa toimintaympäristöön merkittäviä muutoksia, muutoksesta vastaava taho laatii tiedonhallinnan muutosvaikutusten arvioinnin, jonka laatimiseen tiedonhallintalaki (Laki julkisen hallinnon tiedonhallinnasta 906/2019) velvoittaa. Arvioinnilla varmistetaan muutosten hallinnolliset, taloudelliset, toiminnalliset ja riskeihin perustuvat vaikutukset, millä pyritään varmistamaan järjestelmien yhteentoimivuus, tietoturvallisuus ja tietoaineistojen lainmukainen käsittely. Utajärven kunnan tietohallinto ja tietosuojavastaava osallistuvat hankinnan suunnitteluun ja vaikutustenarvioinnin laatimiseen tietosuojan ja tietoturvan varmistamiseksi.

Tietoturvallisen toimintaympäristön hallinta varmistetaan palveluntuottajien, yhteistyökumppanien ja alihankintaketjujen sitouttamisella ja velvoittamisella sopimusteknisesti. Sopimuksissa tulee huomioida toiminnallinen vastuunjako tietoturvan, tietosuojan, palveluiden jatkuvuuden ja varautumisen osalta, esimerkiksi RACI-mallilla. Säännöllinen raportointi palvelutason toteutumisesta,

häiriötilanteiden hallinnasta ja tietoturvapoikkeamista sekä rikkomuksiin liittyvistä käytänteistä ja sanktioista on myös tarpeen määritellä sopimuksiin.

4. Seuranta, arviointi ja riskienhallinta

Tietosuojan ja tietoturvallisuuden ylläpito ja kehittäminen vaativat jatkuvaa seurantaa ja arviointia. Tietoturvallisuuden osalta lähtökohtana on seurata ja arvioida toteutuuko eri muodoissa olevan tiedon saatavuus, eheys ja luottamuksellisuus koko tiedon elinkaaren ajan. Tietosuojan näkökulmasta arvioidaan sitä, toteutuuko rekisteröityjen oikeudet, rekisterinpitäjän velvollisuudet ja tietosuojaperiaatteet henkilötietoja käsiteltäessä ja yleisesti kunnan toiminnassa. Tavoite on tunnistaa tietoon, tietosuojaan ja tietoturvallisuuteen kohdistuvia riskejä ja kehittämiskohteita. Seuranta ja arviointi voi kohdistua kunnan oman toiminnan lisäksi sen sidosryhmien ja palveluntuottajien toimintaan. Arviointia voidaan toteuttaa tarvittaessa itsearvioinnin lisäksi ulkoista auditointia hankkimalla.

Tietosuojan ja tietoturvallisuuden jatkuva seuranta, arviointi ja riskienhallinta on osa kunnan sisäistä valvontaa. Havaitut puutteet tai laiminlyönnit raportoidaan kunnan tietosuoja- ja tietoturvatyöryhmälle, joka käsittelee ilmoitetut epäkohdat ja määrittää tilanteeseen korjaavat toimenpiteet. Lisäksi arviointia, valvontaa ja tarkastusta voidaan tehdä organisaation henkilöstöltä tai ulkopuoliselta taholta tulleen ilmoituksen perusteella tai rekisteröidyn pyynnöstä.

Tietosuojan ja tietoturvallisuuden tilaa sekä määritettyjen tavoitteiden ja periaatteiden toteutumista seurataan säännöllisesti vuosittain laadittavan tietotilinpäätöksen yhteydessä. Kunnanhallitus käsittelee tietotilinpäätöksen, ja tarvittaessa ohjaa tavoitteiden ja periaatteiden toteuttamista. Tietosuoja- ja tietoturvapolitiikan ajantasaisuus katselmoidaan vuosittain, ja politiikkaa päivitetään tarvittaessa. Päivityksen valmistelee tietohallintopäällikkö yhdessä tietosuoja- ja tietoturvaryhmän kanssa. Sisällölliset muutokset hyväksyy kunnanhallitus.

Kunnan sisäisten tietosuoja- ja tietoturvallisuutta koskevien ohjeiden ajantasaisuutta ja riittävyyttä tarkastellaan jatkuvan seurannan ja arvioinnin yhteydessä. Jokaisella työntekijällä ja viranhaltijalla on oikeus ja velvollisuus ilmoittaa tietosuoja- ja tietoturvaohjeistuksissa havaitsemistaan puutteista tai sen riittämättömyydestä.

4.1 Riskienhallinta

Tietosuojan ja tietoturvallisuuden toteutumista arvioidaan aina riskilähtöisesti. Tietosuojaan ja tietoturvallisuuteen kohdistuvien riskien arviointia ja hallintaa toteutetaan Utajärven kunnassa jatkuvana ja ennakoivana toimintana, ja sitä tehdään etenkin merkittävien organisaatioon tai toimintaympäristöön kohdistuvien muutoksien yhteydessä. Riskienhallinta on osa kunnan johtamista ja varautumista sekä kunnan tuottamien palveluiden laadunhallintaa.

Riskienhallinnan keskeisenä tavoitteena on tunnistaa tietosuojaan ja tietoturvallisuuteen kohdistuvat riskit, arvioida ne ja päättää tarvittavista toimenpiteistä. Riskienhallinnalla on selkeät päävaiheet. Aluksi riskit tunnistetaan ja niiden merkitys arvioidaan. Seuraavaksi suunnitellaan riskien torjunta ja toimenpiteet, joilla riski poistetaan tai pienennetään sen todennäköisyys tai vaikutus hyväksyttävälle

tasolle. Tämän jälkeen tilannetta seurataan. Mahdolliset toteutuneet riskit analysoidaan ja kehitetään toimintaa siten, ettei riski toteudu jatkossa.

Tietoturvallisuuden riskienhallintaan velvoittaa tiedonhallintalaki. Kunnan on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava toimenpiteet riskiarvioinnin mukaisesti (TihL 13 §). Riskejä on arvioitava kokonaisvaltaisesti, arvioitaessa on huomioitava hallinnolliseen, fyysiseen ja tekniseen turvallisuuteen sekä kunnan toiminnan jatkuvuuteen ja tietosuojaan kohdistuvat riskit.

Tietosuojan näkökulmasta arviointiin ja riskienhallintaan velvoittaa EU:n yleinen tietotuoja-asetus. Tietosuoja-asetuksen lähtökohtana on sisäänrakennettu ja oletusarvoinen tietosuoja sekä riskiperusteinen lähestymistapa. Utajärven kunta on rekisterinpitäjänä vastuussa siitä, että se toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla varmistetaan ja käytännössä myös osoitetaan, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen vaatimuksia. Tietosuojaan kohdistuvia riskejä on arvioitava rekisteröidyn näkökulmasta; mitä rekisteröidyn vapauksia ja oikeuksia käsittely voi vaarantaa, ja mitä vahinkoja (aineelliset, aineettomat ja fyysiset) rekisteröidylle voi aiheutua henkilötietojen käsittelystä.

Tietosuojan suunnitteluun ja arviointiin sekä riskienhallintaan velvoittaa myös tietosuoja-asetuksen 35 artiklassa säädetty tietosuojan vaikutusten arviointi. Tietosuojaa koskeva vaikutusten arviointi on tehtävä silloin, kun suunnitellaan henkilötietojen käsittelyä, joka todennäköisesti aiheuttaa korkean riskin rekisteröidyn oikeuksille ja vapauksille. Korkean riskin kriteerejä ovat mm. rekisteröityjen järjestelmällinen valvonta, tietojen laajamittainen käsittely, tietokokonaisuuksien yhdistäminen ja heikossa asemassa olevien henkilötietojen käsittely. Vaikutustenarvioinnin tarkoituksena on auttaa tunnistamaan, arvioimaan ja hallitsemaan henkilötietojen käsittelyyn sisältyviä riskejä. Se on tarkoitettu jatkuvaksi riskien tunnistamisen ja hallitsemisen prosessiksi.

4.2 Lokitietojen kerääminen ja hallinta

Lokitiedoilla valvotaan tietosuojan ja tietoturvallisuuden toteutumista ja jäljitettävyyttä, ennaltaehkäisten tai todentaen poikkeavia tapahtumia tai väärinkäytöksiä. Lokitietojen avulla voidaan selvittää mitä, miksi ja milloin jotakin on tapahtunut tai on todennäköisesti tapahtumassa. Lokitiedoilla tarkoitetaan tietojenkäsittelystä (mm. tietojärjestelmät, sovellukset, palvelimet, päätelaitteet, tietoliikenne) kerättävää käyttäjä- ja tapahtumakohtaista tietoa. Lokitietojen keräämisellä ja käsittelyllä voidaan nopeuttaa erilaisten tapahtumien tai poikkeamien selvittämistä ja niistä toipumista sekä parantaa vaatimustenmukaisuuden todentamista.

Lokitietojen keräämisen perusteena kunnan toiminnassa on Tiedonhallintalain 17 §:n velvoite lokitietojen keräämisestä, jonka mukaan lokitietoja on kerättävä, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista.

Lokitietojen keräämisen ja käsittelyn tulee olla suunniteltua ja perusteltua. Lokitietojen kerääminen ja hallinta määritellään osana tietojärjestelmän hankinnan suunnittelua. Lokitietojen keräämistä suunniteltaessa arvioidaan tietojärjestelmän ja sen sisältämän tiedon kriittisyys huomioiden, mitä lokitietoja tietojärjestelmästä on tarpeen kerätä ja miten niitä hallitaan. Suunnittelussa on huomioitava kriittisyyden lisäksi riskienhallinta, varautuminen, lainsäädännön velvoitteet sekä

erityisesti tietosuojan toteutuminen. Tietojärjestelmän omistaja on vastuussa lokitietojen asianmukaisesta toteutuksesta. Lokitietojen hallinnassa noudatetaan seuraavia periaatteita:

- Lokitietoja ei kerätä tai käytetä yleistä valvontaa varten, vaan niiden keräämiselle määritellään peruste lokilähdekohtaisesti, ja tietojen käsittelyn lainmukaisuus varmistetaan koko elinkaaren ajan.
- Pääsyoikeus lokitietoihin myönnetään vain tarveperusteisesti, ja tiedot ovat suojattuja siten, ettei niitä pääse katselemaan muut kuin siihen oikeutetut henkilöt. Lokitietojen käsittelystä tulee myös kerätä lokitietoja, jotta voidaan tarvittaessa selvittää, kuka lokitietoja on käsitellyt.
- Lokitiedot suojataan niin, ettei niitä voi muuttaa.
- Jokaiseen tuotettuun lokimerkintään tallennetaan ainoastaan minimimäärä tietoja, jolla voidaan toteuttaa lokin käyttötarkoitus.
- Lokitietoa saa käyttää vain teknisen ympäristön, tietojärjestelmän, sovelluksen tai käyttäjän suojaamiseen, tietoturvapoikkeamien ja loukkausten selvittämiseen sekä teknisen ympäristön, järjestelmän tai sovelluksen kehittämiseen.

4.3 Käyttöoikeuksien hallinta

Asianmukaisen ja ajantasaisen käyttöoikeuksien hallinnan ja valvonnan avulla mahdollistetaan tietojärjestelmien ja niissä olevan tiedon luvallinen käyttö ja estetään luvatonta käyttöä. Tiedonhallintalain 16 § velvoittaa tietojärjestelmästä vastuussa olevan viranomaisen määrittelemään tietojärjestelmiensä käyttöoikeudet. Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan sekä pidettävä ajantasaisena. Tietojärjestelmien käyttöoikeuksista on vastuussa kunkin tietojärjestelmän omistaja. Käyttöoikeuksien hallinnan tulee olla suunniteltua ja hallittua, ja niissä noudatetaan seuraavia periaatteita:

- Tietojärjestelmälle nimetään omistajan toimesta pääkäyttäjä, joka toteuttaa käyttöoikeuksien hallintaa tietojärjestelmässä omistajan määrittelyn mukaisesti. Erityisesti kriittisille järjestelmille nimetään myös pääkäyttäjän varahenkilö.
- Tietojärjestelmien käyttäjätunnukset ja käyttöoikeudet myönnetään henkilökohtaisina, ja tietojärjestelmiä ei käytetä yhteistunnuksilla.
- Käyttöoikeuksien hallinnassa noudatetaan vähimpien oikeuksien periaatetta, ja hallinta kattaa tietojärjestelmien koko elinkaaren. Vähimpien oikeuksien periaate tarkoittaa, että käyttäjälle annetaan tietojärjestelmiin vain sellaiset käyttöoikeudet ja -valtuudet, jotka ovat työn suorittamiseksi välttämättömiä.
- Käyttöoikeuksien myöntämisen yhteydessä tarkistetaan, että käyttöoikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu saamaan käyttöoikeudet. Lisäksi varmistetaan, että henkilöllä on riittävä koulutus tietojärjestelmän käyttöön.
- Tarpeettomat käyttäjätunnukset sekä käyttöoikeudet poistetaan viipymättä, kun niitä ei enää tarvita. Käyttöoikeudet katselmoidaan säännöllisesti.
- Tietojärjestelmän käyttäjistä ylläpidetään ajantasaista luetteloa. Käyttöoikeuksien muutoksista tulee jäädä merkintä sähköisesti lokitietoihin tai muutokset on kirjattava muilla tavoin ylläpidettävään rekisteriin.
- Organisaation ulkoiset ja sisäiset käyttäjät erotellaan käyttäjätunnuksen muodon perusteella.

5. Menettely tietosuojan tai tietoturvallisuuden vaarantuessa

Kun kunnan toiminnan tietoturvallisuuteen kohdistuu häiriö- tai uhkatilanne, jonka seurauksena kunnan toimintaan ja sen jatkuvuuteen, tai henkilötietojen tietosuojaan kohdistuu poikkeama tai loukkaus, tilanteiden tunnistaminen ja niihin reagointi on ensisijaisen tärkeää. Toiminta näissä tilanteissa tulee olla ennalta suunniteltua ja organisoitua.

Jokaisella kunnan tietojärjestelmiä käyttävällä ja tietoja käsittelevällä on velvollisuus ilmoittaa toiminnassa havaitsemistaan tietosuojaan tai tietoturvallisuuteen kohdistuvista häiriö- tai uhkatilanteista sekä poikkeamista ja loukkauksista viipymättä. Ilmoitus tehdään toimialajohtajalle sekä tietohallintopäällikölle ja tietosuojavastaavalle. Henkilöstöä kannustetaan ilmoittamaan havainnoistaan matalalla kynnyksellä, jo pelkät epäilyt on syytä ilmoittaa, sillä vaikka kyseessä ei olisi häiriö- tai uhkatilanne, poikkeama tai loukkaus, voi ilmoituksen perusteella olla tarpeen toteuttaa kunnan tietosuojaan tai tietoturvallisuuteen kohdistuvia kehitystoimenpiteitä.

Niiltä osin, kun kunta ulkoistaa tietojenkäsittelyä ja ICT-palveluntuotantoa sopimusperusteisesti, sopimusehdoissa velvoitetaan toimijoita ilmoittamaan kunnalle viipymättä toimittajan havaitsemista tai toimittajan toimintaan kohdistuvista tietosuojan tai tietoturvallisuuden uhka- ja häiriötilanteista, poikkeamista sekä loukkauksista, jotka koskevat kunnan asiakkuutta. Sopimusehdoissa on sovittava myös toimittajan avustamisvelvollisuudesta poikkeamien ja loukkausten käsittelyssä. Toimittajan kanssa sovitaan myös ilmoitusten tekemisestä, kenelle toimittaja ilmoitukset tekee. Tyypillisesti ilmoitusten vastaanottaja on kunnassa tietosuojavastaava, sopimukseen merkitty vastuuhenkilö tai pääkäyttäjä.

Tietosuojaa tai tietoturvallisuutta koskevien häiriö- ja uhkatilanteiden sekä poikkeamien ja loukkausten toimintaprosessi on Utajärven kunnassa ennalta määritetty. Ilmoitukset ohjataan viipymättä kunnan toimialajohtajalle sekä tietohallintopäällikölle ja tietosuojavastaavalle, jotka koostavat alustavan tilannekuvan, arvioivat tilanteen vakavuuden, ja tapahtuman ollessa vakava, raportoivat tapahtuneesta kunnan tietosuoja- ja tietoturvaryhmälle. Ryhmä päättää jatkotoimenpiteistä, mm. mahdollisesta siirtymisestä normaaliolojen häiriötilanteen tai poikkeusolojen mukaiseen toimintaan, jolloin johtovastuu siirtyy kunnanjohtajalle ja kunnan johtoryhmälle. Toimintaprosessi, organisointi ja vastuut määritellään tarkemmin kunnan ICT-valmiussuunnittelussa.

6. Varautuminen

Utajärven kunta varautuu ensisijaisesti kriittisten toimintojensa ja palveluidensa jatkuvuuden turvaamiseen normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Varautumista toteutetaan ylläpitämällä valmiussuunnitelmia ja harjoittelemalla säännöllisesti. Tavoitteena on varautua toiminnan häiriöitilanteisiin ja keskeytyksiin niin, että toimintaa voidaan jatkaa mahdollisimman normaalisti rajoittamalla haittavaikutuksia ja toipua tilanteesta mahdollisimman nopeasti. Toimenpiteiden priorisointi normaaliolojen häiriötilanteissa ja poikkeusoloissa on:

1. Hengen tai terveyden turvaaminen.
2. Arkaluonteisen tai muuten salassa pidettävän tai erittäin merkittävän tiedon turvaaminen.
3. Tietojärjestelmien ja henkilörekistereiden eheyden turvaaminen.

4. Käyttö- ja toimintaympäristön saatavuuden turvaaminen

6.1 Viestintä häiriötilanteessa

Normaaliolojen häiriötilanne tai poikkeusolot vaativat usein viestintää kunnan asiakkaille ja muille sidosryhmille. Viestinnässä noudatetaan Utajärven kunnan kriisiviestinnän ohjeistuksia ja vastuita. kriisiviestintää johtaa kunnanjohtaja yhdessä kunnan johtoryhmän kanssa.

7. Tietosuoja- ja tietoturvarikkomukset

Tietosuojan tai tietoturvallisuuden laiminlyönti voi aiheuttaa vakavaa haittaa tai vahinkoa kunnalle, sen asiakkaille ja muille rekisteröidyille, sekä kunnan sidosryhmille ja palveluntuottajille.

Havaitusta lainsäädännön vastaisesta toiminnasta, kunnan tietosuoja- ja tietoturvapolitiikan tai sen perusteella annettujen tietoturva- ja tietosuojaohjeiden noudattamatta jättämisestä, tai niiden vastaisesta toiminnasta tulee aina tehdä ilmoitus. Ilmoitus tehdään toimialajohtajalle sekä tietohallintopäällikölle ja tietosuojavastaavalle. Ilmoituksen perusteella toteutettava selvitysprosessi etenee toimialajohtajan johtovastuulla yhteistyössä tietohallintopäällikön ja tietosuojavastaavan kanssa. Selvityksen suorittamiseksi edellä mainituille henkilöille tulee mahdollistaa pääsy selvitystyön edellyttämään tietoon. Tietosuoja- ja tietoturvarikkomusten selvitysprosessi on kuvattu liitteessä 2.

Palvelussuhteeseen vaikuttavista seuraamuksista on säädetty ensi sijassa työsopimuslaissa ja viranhaltijalaissa. Sovellettavaksi voivat tulla myös rikos- ja vahingonkorvauslainsäädäntö. Tietosuoja- ja tietoturvarikkomukset käsitellään tapauskohtaisesti. Kunnan tietosuoja- ja tietoturvapolitiikan sekä sen perusteella annettujen tietoturva- ja tietosuojaohjeiden noudattamatta jättäminen tai niiden vastainen toiminta voi olla peruste käyttöoikeuksien rajoittamiselle tai menettämiselle, huomautukselle, varoitukselle, työ- tai virkasuhteen irtisanomiselle, tai rikoslain mukaisille rikosoikeudellisille seuraamuksille. Mikäli rikkomuksesta aiheutuu välittömästi tai välillisesti taloudellisia menetyksiä, voidaan päätyä vahingonkorvausvaatimuksiin. Salassapitovelvollisuuden rikkominen on asianomistajarikos, jolloin asianomainen henkilö voi tehdä asiasta rikosilmoituksen. Tietosuoja- ja tietoturvarikkomusten seuraamustaulukko on esitetty liitteessä 3. Seuraamuksista päättää toimialajohtaja.

Sopimuskumppaneiden kuten palveluntuottajien tietosuoja- ja tietoturvarikkomusten ilmetessä kunta pyytää toimittajalta kirjallisen vastineen tapahtuneesta. Väärinkäytökset tai sopimuksen vastainen toiminta voivat johtaa sopimuksen purkamiseen ja/tai vahingonkorvausvastuuseen.

8. Organisointi ja vastuut

Utajärven kunnan tietosuoja ja tietoturvatyön toteuttamisen perustana on kunnanhallituksen hyväksymä tietosuoja- ja tietoturvapolitiikka ja sen pohjalta laaditut ohjeistukset. Tietosuojan ja tietoturvallisuuden toteuttaminen kunnan toiminnassa on jatkuvaa ja kuuluu kaikille, jotka tietoja käsittelevät. Toteuttamiseen osallistuvat kunnan ja sidosryhmien henkilöstö, osana omaa yleistä toimintavastuutaan.

8.1 Kunnanhallitus

- Vastaa kunnan hallintosäännön 75 §:n mukaisesti kokonaisvaltaisen sisäisen valvonnan ja riskienhallinnan järjestämisestä.
- Vastaa kunnan hallintosäännön 54 §:n mukaisesti siitä, että tiedonhallintalain 4.2 §:n vastuut, käytännöt ja valvonta on määritelty kunnassa.
- Sitoutuu kunnan tietosuojan ja tietoturvallisuuden ylläpitämiseen ja kehittämiseen sekä huolehtii siihen kohdennettavasta riittävästä resursoinnista.
- Varmistaa, että organisaatiolla on edellytykset toimia poikkeus-, erityis- ja kriisitilanteissa.
- Hyväksyy päätöksellään tietosuoja- ja tietoturvapolitiikan kunnan toimintaa ohjaavaksi asiakirjaksi.

8.2 Kunnanjohtaja

- Luo johtamisellaan toiminnalliset edellytykset tietosuojan ja tietoturvallisuuden asianmukaiselle ylläpidolle, kehittämiselle, seurannalle sekä arvioinnille ja riskienhallinnalle organisaatiossa.
- Johtaa kunnan varautumista ja jatkuvuudenhallintaa, normaaliolojen häiriötilanteiden sekä poikkeusolojen toimintaa ja siihen liittyvää viestintää yhdessä kunnan johtoryhmän kanssa.
- Hyväksyy päätöksillään koko organisaation toimintaa ohjaavat tietosuojaa ja tietoturvallisuuttaa koskevat ohjeistukset.
- Nimeää kunnan tietosuoja- ja tietoturvaryhmän jäsenet.

8.3 Toimialajohtaja

- Vastaa yleisten sekä toimialaansa erityisesti koskevien lakisääteisten tietosuoja- ja tietoturvallisuusvelvoitteiden noudattamisesta johtamallaan toimialalla.
- Johtaa toimialansa toiminnan, tietojärjestelmien ja tietovarantojen tietosuojan ja tietoturvallisuuden ylläpitoa, seurantaa, arviointia, kehittämistä sekä riskienhallintaa ja varautumista.
- Varmistaa tietosuoja- ja tietoturvapolitiikan sekä tietosuojaan ja tietoturvallisuuteen liittyvien ohjeistusten ja koulutusten toteuttamisen johtamallaan toimialalla yhdessä toimialansa esihenkilöiden kanssa.
- Toimii toimialansa tietojärjestelmien ja tietovarantojen ensisijaisena omistajana sekä nimeää tietojärjestelmien pääkäyttäjät.
- Vastaa ja valvoo tietosuojaa ja tietoturvallisuutta koskevien sopimusehtojen riittävyyttä ja noudattamista siltä osin, kun tietojenkäsittelyä tai palvelutuotantoa on ulkoistettu sopimusperusteisesti.
- Vastaa toimialansa osalta kunnan tiedonhallintamallin laatimisesta ja tietojen ajantasaisuudesta.
- Vastaa toimialallaan toteutettavien tiedonhallintaan kohdistuvien muutosten yhteydessä tiedonhallinnan muutosvaikutusten arvioinnin tekemisestä.
- Toimii toimialansa osalta rekisterinpitäjän henkilörekisterien vastaavana viranhaltijana, vastaten henkilötietojen käsittelyn lainmukaisuudesta, henkilötietojen käsittelyn tarkoitusten

ja keinojen määrittelystä, henkilötietojen käsittelylle asetetut vaatimukset toteuttamisesta, sekä rekisteröidyn oikeuksien toteutumisesta ja informoinnista.

- Vastaa tietosuoja-asetuksen mukaisen tietosuojaa koskevan vaikutusten arvioinnin tekemisestä sisältä osin, kun toimialalla suunnitellaan tai toteutetaan henkilötietojen käsittelyä, joka todennäköisesti aiheuttaa korkean riskin rekisteröidyn oikeuksille ja vapauksille.

8.4 Tietohallintopäällikkö

- Toimii tietoturvavastaavana vastaten tietoturvallisuuden seuraamisesta, kehittämisestä ja koordinoinnista sekä tietosuoja- ja tietoturvatietouden edistämisestä.
- Vastaa kunnan tietohallinnon asiantuntijayksikön toiminnasta ja kehittämisestä.
- Vastaa kunnan ICT-palveluiden ja tietoliikenteen tietosuojan ja tietoturvallisuuden ylläpidosta ja kehittämistä sekä riskienhallinnasta.
- Kehittää ja koordinoi kunnan ICT-varautumista ja toiminnan jatkuvuuden hallintaa.
- Vastaa kunnan kokonaisarkkitehtuurin hallinnasta sekä tiedonhallintamallin ylläpidosta ja kehittämisestä.
- On valtuutettu sulkemaan, tai määräämään suljettavaksi tietojärjestelmä, tietovaranto, tietoliikenneyhteys, käyttäjätunnus tai laite uhka- tai väärinkäytöstilanteen vahinkojen minimoimiseksi.

8.5 Esihenkilö

- Vastaa yksikkönsä osalta, että kuntaa ja toimialaa koskevia lakisääteisiä tietosuoja- ja tietoturvavelvoitteita, tietosuoja- ja tietoturvapolitiikkaa sekä tietosuojaan ja tietoturvallisuuteen liittyviä ohjeistuksia noudatetaan yksikön toiminnassa.
- Vastaa että yksikkönsä työntekijöillä on käyttöoikeudet tarvittaviin tietojärjestelmiin ja tietovarantoihin työtehtävien edellyttämässä laajuudessa huomioiden vähimpien oikeuksien periaatteen toteutuminen.
- Vastaa että yksikön työntekijät saavat riittävän perehdytyksen ja koulutuksen tietosuojaan ja tietoturvallisuuteen sekä ymmärtävät näiden merkityksen toiminnassaan.
- Vastaa että yksikön työntekijät ovat allekirjoittaneet salassapito- ja käyttäjäsitoumuksen sekä suorittaneet tietosuojaan ja tietoturvaan liittyvät pakolliset koulutukset.
- Vastaa että muutokset yksikön työntekijöiden työtehtävissä huomioidaan tietojärjestelmien käyttöoikeuksissa, ja työsuhteen päättyessä työntekijät palauttavat kaiken kunnalle kuuluvan omaisuuden sekä käyttöoikeudet tietojärjestelmistä poistetaan.
- On velvoitettu raportoimaan tietosuojaan tai tietoturvallisuuteen kohdistuvista häiriö- tai uhkatilanteista, poikkeamista ja loukkauksista sekä kehittämistarpeista toimialajohtajalle, tietohallintopäällikölle ja tietosuojavastaavalle.

8.6 Tietosuoja- ja tietoturvaryhmä

- Valvoo, arvioi ja kehittää kunnan tietosuojan ja tietoturvallisuuden toteutumista kokonaisuutena.
- Seuraa tietosuojan ja tietoturvallisuuden yleistä kehitystä, toimintaympäristön ja lainsäädännön muutoksia, sekä arvioi kokonaisvaltaisesti organisaatioon kohdistuvia muutostarpeita ja havaittuja tietosuoja- ja tietoturvariskejä.
- Valmistelee kunnan toimintaa ohjaavat tietosuojaan ja tietoturvallisuuteen liittyvät ohjeet.
- Käsittelee havaitut tietosuojaa tai tietoturvallisuutta koskevat laajat poikkeamat ja loukkaukset.
- Valmistelee vuosittain tehtävän tietotilinpäätöksen, johon kootaan tiedot kunnan tietojenkäsittelyn nykytilasta sekä arvio tietosuojan ja tietoturvallisuuden toteutumisesta.
- Valmistelee tietosuojan ja tietoturvallisuuden kehittämiskohteet talousarviota varten sekä raportoi toteumasta tietotilinpäätöksen yhteydessä.

8.7 Tietosuojavastaava

- Toimii organisaation sisäisenä tietosuojan asiantuntijana, joka seuraa henkilötietojen käsittelyä ja auttaa tietosuojasäännösten noudattamisessa.
- Seuraa tietosuojalainsäädännön ja kunnan omien ohjeiden, määräysten ja sääntöjen noudattamista, tuo esiin havaitsemiaan puutteita sekä antaa kehitysehdotuksia tietosuojan toteuttamisesta.
- Antaa tietoja ja neuvoja tietosuojalainsäädännön mukaisista velvollisuuksista johdolle ja henkilötietoja käsitteleville työntekijöille.
- Antaa pyydettäessä neuvoja tietosuojan vaikutustenarvioinnin tekemisestä ja valvoo vaikutustenarvioinnin toteutusta.
- Toimii rekisteröityjen yhteyshenkilönä henkilötietojen käsittelyyn liittyvissä asioissa.
- Toimii tietosuojavaltuutetun toimiston yhteyshenkilönä ja tekee yhteistyötä tietosuojavaltuutetun toimiston kanssa.
- Raportoi havaitsemistaan tietosuojaan liittyvistä epäkohdista toimialajohtajille, tietohallintopäällikölle, tietosuoja- ja tietoturvaryhmälle sekä tarvittaessa kunnanjohtajalle ja kunnanhallitukselle.

8.8 Tietojärjestelmän ja tietovarannon omistaja

- Vastaa tietojärjestelmän tai tietovarannon elinkaaren hallinnasta, tietosuojan ja tietoturvallisuuden toteuttamisesta, sekä lokitietojen keräämisen ja hallinnan määrittelystä.
- Vastaa tietojärjestelmän tai tietovarannon käyttöoikeuksien määrittelystä.
- Vastaa tietojärjestelmän tai tietovarannon toimintaan ja turvallisuuteen liittyvien asetusten ja vaatimusten määrittelystä yhdessä pääkäyttäjän kanssa.
- Vastaa tietojärjestelmän tai tietovarannon dokumentaation laadinnasta ja ylläpidosta tietohallinnon ylläpitämään tietojärjestelmäluetteloon sekä Utajärven kunnan tiedonhallintamalliin.
- Vastaa tietojärjestelmään tai tietovarantoon kohdistuvien muutosten tiedottamisesta kunnan tietohallinnolle, tietosuojavastaavalle ja käyttäjille.

8.9 Tietojärjestelmän pääkäyttäjä

- Toteuttaa tietojärjestelmän käyttöoikeuksien hallintaa ja ylläpitoa tietojärjestelmän omistajan määrittelyn mukaisesti.
- Neuvoo ja opastaa käyttäjiä tietojärjestelmän käytössä.

8.10 Asiakirjahallinnosta vastaava viranhaltija

- Ohjaa ja kehittää asiakirjahallintoa osana kunnan tiedonhallintaa.
- Ohjaa toimialoja asiakirjahallinnon hoidossa, jotta arkistolain 7 §:n vaatimukset toteutuvat kunnan toiminnassa oikeusturva, tietosuoja ja tietoturvallisuus huomioiden.
- Laatii ja ylläpitää kunnan arkistonmuodostussuunnitelmaa ja tiedonohjaussuunnitelmaa, sekä hyväksyy sen päätöksellään käyttöön.

8.11 Työntekijät ja viranhaltijat

- Vastaavat tietosuojan ja tietoturvallisuuden toteuttamisesta omassa toiminnassaan, sekä kunnan tietosuoja- ja tietoturvapolitiikan sekä tietosuojaan ja tietoturvallisuuteen liittyvien ohjeistuksien noudattamisesta.
- Suorittavat pakolliset, säännöllisesti järjestettävät tietosuoja- ja tietoturvaosaamista ylläpitävät koulutukset.
- Allekirjoittavat salassapito- ja käyttäjäsitoumuksen, joka on edellytyksenä Utajärven kunnan päätelaitteiden, tietojärjestelmien, tietovarantojen ja tietoliikenneyhteyksien käyttöoikeuksien myöntämiselle.
- Ovat velvoitettuja ilmoittamaan viipymättä havaitsemistaan tietosuojaan tai tietoturvallisuuteen kohdistuvista häiriö- tai uhkatilanteista, poikkeamista, loukkauksista, puutteista, virheellistä menettelyistä tai riskeistä toimialajohtajalle, tietohallintopäällikölle ja tietosuojavastaavalle.
- Ovat oikeutettuja ja velvoitettuja ilmoittamaan tietosuoja- ja tietoturvaohjeistuksissa havaitsemistaan puutteista tai sen riittämättömyydestä.

8.12 Luottamushenkilöt

- Vastaavat tietosuojan ja tietoturvallisuuden toteutumisesta luottamustehtävissään.
- Suorittavat kunnan järjestämän, luottamushenkilöille suunnatun tietosuoja- ja tietoturvakoulutuksen säännöllisesti.
- Allekirjoittavat luottamushenkilöitä koskevan salassapito- ja käyttäjäsitoumuksen.

8.13 Tytäryhtiöt

- Kuntakonserniin kuuluvien tytäryhtiöiden toimitusjohtajat vastaavat tämän tietosuoja- ja tietoturvapolitiikan sekä kunnan ohjeiden ja määräysten noudattamisesta tytäryhtiön toiminnassa.
- Kuntakonserniin kuuluvien tytäryhtiöiden toimitusjohtajien vastuulla on tuntea toimialansa erityispiirteet ja lainsäädäntö, seurata niiden kehittymistä ja kommunikoida niistä kunnan tietohallinnolle ja tietosuojavastaavalle.
- Kuntakonserniin kuuluvien tytäryhtiöiden toimitusjohtajien tehtävänä on valvoa tietosuojan ja tietoturvallisuuden toteutumista ja ohjeistuksen noudattamista tytäryhtiön toiminnassa

sekä raportoida mahdollisista häiriö- ja uhkatilanteista, poikkeamista, loukkauksista ja kehittämistarpeista kunnan tietohallintopäällikölle ja tietosuojavastaavalle.

8.14 Ulkoiset palveluntuottajat

- Palveluntuottajien vastuut ja velvollisuudet tietosuojaan ja tietoturvallisuuteen liittyen sovitaan palveluntuottajan ja kunnan välille solmittavissa sopimuksissa, jonka ehtojen mukaisesti palveluntuottaja on velvoitettu tuottamaan palvelua.

Liitteet:

Liite 1 Työntekijöiden ja viranhaltijoiden salassapito- ja käyttäjäsitoumus

Liite 2 Luottamushenkilöiden salassapito- ja käyttäjäsitoumus

Liite 3 Tietosuojan tai tietoturvallisuuden vaarantumisepäilyn selvitysprosessi

Liite 4 Tietosuoja- ja tietoturvarikkomusten seuraamustaulukko