

Tietotilinpäätös 2024



Uusikaupunki

Sisällys

1. Tietotilinpäättöksen tarkoitus	1
2. Tietosuoja-asioiden vastuunjako Uudenkaupungin kaupungilla	1
2.1 Kaupunginhallitus	1
2.2 Tietosuojavastaava	1
2.3 Tietoturvavastaava	2
2.4 Tietoturva- ja tietosuojaryhmä.....	2
2.5 Palvelualojen vastuut	2
3. Tietosuoja ja tietoturvallisuuden toteuttaminen.....	2
3.1 Tietosuojan periaatteet.....	2
3.2 Henkilöstön koulutus ja ohjeet.....	3
3.3 Tietoturvapolitiikka.....	3
3.4 Tietosuojaloukkaukset.....	3
3.4 Väärinkäytösten ilmoituskanava.....	4
3.5 Tietopyynnöt.....	4
3.6 Tietoturva- ja tietosuojaryhmä.....	5
4. Tietoturva	5
5. Tiedon hallinta	5
5.1 Tiedonhallintamalli	6
5.2 Asiakirjajulkisuuskuvaukset	6
6. Tietosuojan kehittämistarpeet	6

Julkaisija:

Uudenkaupungin kaupunki, 2025

Tietoturva- ja tietosuojaryhmä

Hyväksytty kaupunginhallituksessa xx.x.xxxx

1. Tietotilinpäätöksen tarkoitus

Tietotilinpäätös kuvaa tietovarantoihin, tietojenkäsittelyyn ja tietoturvallisuuteen liittyviä toimintaperiaatteita sekä arvioi tietosuoja- ja tietoturvan toteutumista Uudenkaupungin kaupungissa. Tietotilinpäätöksellä vastataan EU:n yleisen tietosuoja-asetuksen osoitusvelvollisuuteen. Osoitusvelvollisuus tarkoittaa sitä, että organisaation pitää pystyä osoittamaan noudattavansa tietosuoja-asetusta henkilötietojen käsittelyssä ja toteuttavansa tietosuojaperiaatteita myös käytännössä.

Osoitusvelvollisuuden toteuttaminen edellyttää, että henkilötietojen käsittelyyn liittyvät prosessit ja tietosuojaperiaatteiden käytännön toteuttaminen dokumentoidaan. Tietotilinpäätös on osa tätä dokumentointia.

Tietosuoja ja tietoturva ovat kaupungin yhteinen asia, joka vaatii johdon, henkilöstön, luottamushenkilöiden ja tytäryhtiöiden sitoutumista tietoturva- ja tietosuojatyöhön. Tässä tietotilinpäätöksessä kuvataan keskeisiä toimenpiteitä, kuinka Uudenkaupungin kaupunki huolehtii asiakkaiden, henkilöstön ja sidosryhmien henkilötiedoista ja yksityisyydestä.

Tietotilinpäätöksen koonnista vastaa tietosuojavastaava yhdessä tietoturva ja tietosuojaryhmän kanssa. Tietotilinpäätöksen hyväksyy kaupunginhallitus.

2. Tietosuoja-asioiden vastuunjako Uudenkaupungin kaupungilla

2.1 Kaupunginhallitus

Hallintosäännön mukaisesti kaupunginhallitus vastaa siitä, että kaupunki täyttää tietosuojalainsäädännön velvoitteet ja valvoo niiden toteutumista. Kaupunginhallitus hyväksyy tietoturva- ja tietosuojapolitiikan ja siihen ehdotetut muutokset, seuraa tietoturvallisuuden sekä tietosuoja- ja tietoturvan toteutumista ja vastaa kaupungin sisäisen valvonnan ja riskienhallinnan järjestämisestä.

2.2 Tietosuojavastaava

Tietosuojavastaavan tehtäviin kuuluu organisaation neuvonta ja ohjaus tietosuojakysymyksissä, tietosuoja-asetuksen noudattamisen valvonta, yhteistyö valvontaviranomaisen (tietosuojavaltuutettu) kanssa ja rekisteröityjen oikeuksien toteuttamisen tukeminen. Tietosuojavastaava raportoi tietosuoja- ja tietoturvan toteutumisesta kaupunginjohtajalle ja tietoturva- ja tietosuojaryhmälle.

2.3 Tietoturvavastaava

Uudenkaupungin kaupungin ICT-päällikön tehtäviin kuuluu vastata kaupungin tietoturvallisuusjärjestelyistä, tietoturvallisuuden kehittämisestä, tietoturvallisuusohjeiden ylläpitämisestä, tietoturvallisuusvaatimusten toteuttamisesta sekä tietoturvallisuuden tilan seuraamisesta sekä poikkeusoloihin varautumisesta tietojärjestelmien ja tietoaineistojen osalta.

2.4 Tietoturva- ja tietosuojaryhmä

Tietoturva ja tietosuojaryhmä on nimetty tietosuojan ja tietoturvan toiminnan kehittämiseksi ja seuraamiseksi sekä omalta osaltaan jalkauttamaan kaupungin yhteisiä toimintatapoja toimialoille. Ryhmän tavoitteena on seurata ja valvoa tietoturvan ja tietosuojan tilaa sekä linjata kehittämistä. Ryhmä avustaa myös tietojen, tietojärjestelmien ja prosessien omistajia ylläpitämään ja kehittämään tietoturva- ja tietosuoja-asioita heidän päivittäisessä toiminnassaan.

Ryhmään kuuluu tiedonhallintapäällikkö, joka toimii myös tietosuojavastaavana, tiedonhallintasihteeri, ICT-päällikkö, joka toimii myös tietoturvapäällikkönä, kasvun ja oppimisen palveluiden ICT-pedagogi, viestintä- ja palvelusuunnittelija, paikkatietoinsinööri, maanmittausinsinööri, aineopettaja ja kirjastonhoitaja. Insinöörit toimivat Trimble-järjestelmän pääkäyttäjinä ja aineopettaja Google-oppimisympäristön pääkäyttäjänä.

2.5 Palvelualojen vastuut

Palvelualojen johdolla on vastuu toiminnan lainmukaisuudesta henkilötietojen käsittelyssä. Palvelualojen johto vastaa palvelukeskuksen tietojenkäsittelyn riskienhallinnasta, varautumisesta tietojenkäsittelyn häiriötilanteisiin sekä tietoturvallisuuden ja tietosuojan toteutumisesta ja kehittämisestä.

3. Tietosuoja ja tietoturvallisuuden toteuttaminen

3.1 Tietosuojan periaatteet

Uudenkaupungin kaupunki pyrkii toiminnassaan noudattamaan EU:n tietosuoja-asetuksen ja tietosuojalain mukaisia tietosuojaperiaatteita, jonka mukaan henkilötietoja on:

- käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi

- käsiteltävä luottamuksellisesti ja turvallisesti
- kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten
- kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden
- päivitettävä aina tarvittaessa – epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä
- säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteutumista varten.

3.2 Henkilöstön koulutus ja ohjeet

Tietoturvallisuus tulee olla sisällytettyinä perehdytysprosessiin. Tietojärjestelmien käyttäjiltä edellytetään käyttö- ja salassapitositoumuksen hyväksymistä.

Henkilökunnalle on pidetty lyhyitä tietoturva- ja tietosuojakoulutuksia automaattisesti. Lisäksi käyttäjille on lähetetty simuloituja organisaatiokohtaisia hyökkäyksiä ja mikrokoulutuksia. Koulutuksilla nostetaan käyttäjien valmiutta varautua sähköpostikalasteluihin ja -hyökkäyksiin.

Esihenkilöt varmistavat, että henkilöstö hallitsee tietoturvan ja tietosuojan perusteet.

Kaupunki osallistui TAISTO24- tietoturva ja tietosuojaharjoitukseen marraskuussa. Harjoitus simuloi varautumista organisaation toiminnan keskeytyessä ulkoisista syistä, myös tietojärjestelmien toiminta- ja palautumisvalmiuksien selvittämiseksi. Digi- ja väestötietoviraston vuosittain järjestämässä Taisto-harjoituksessa yritykset ja organisaatiot harjoittelevat toimintaa tietoturvan ja tietosuojan poikkeamatilanteissa.

3.3 Tietoturvapolitiikka

Tietojen suojaamisen ja turvaamisen periaatteet, tavoitteet, vastuut ja yleiset toteutuskeinot määrittelee kaupungin tietoturva- ja tietosuojapolitiikka, joka on hyväksytty kaupunginhallituksessa 20.12.2021 ja astunut voimaan 1.1.2022.

Tietojärjestelmien yleisetkäytösäännöt tulivat voimaan 2.1.2024. Käytösäännöt on tarkoitettu osaltaan varmistamaan se, että kaupungin työntekijät ja sidosryhmät tietävät, mitä tietojärjestelmien tietoturvasta ja tietosuojasta huolehtiminen käytännössä merkitsee.

3.4 Tietosuojaloukkaukset

Henkilötietojen tietosuojaloukkaus on tapahtuma, jossa henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee taho, jolla ei ole käsittelyoikeutta. Tietosuojaloukkaus voi tapahtua vahingossa tai tahallisesti.

Henkilötietojen tietosuojaloukkauksia ovat esimerkiksi tietojen lähettäminen väärälle henkilölle, kadonnut henkilötietoja sisältävä paperi, omaan työhön kuulumattomien henkilötietojen katselu, kadonnut muistitikku, varastettu tietokone tai murtautuminen henkilötietoja sisältävään tietojärjestelmään.

Tietosuojaloukkausten varalta kaupungilla on menettelyohjeistus, ja käytössä on lomake tietosuojaloukkausten ilmoittamiseksi.

Vuoden 2024 aikana ei tapahtunut yhtään tietosuojaloukkausta, joka olisi vaatinut raportointia tietosuojavaltuutetun toimistolle.

Vuoden 2024 aikana tapahtui yksi tietosuoja-rikkomus, josta on laadittu sisäinen tietosuoja-rikkomus dokumentti.

3.4 Väärinkäytösten ilmoituskanava

Sisäinen väärinkäytösten ilmoituskanava otettiin käyttöön vuonna 2023.

Ilmoituskanavan soveltamispiiriin kuuluvat lain laiminlyönnit mm. Julkisista hankinnoista, rahanpesusta, liikenneturvallisuudesta, ympäristönsuojelusta, elintarviketurvallisuudesta, kuluttajansuojasta ja yksityisyyden ja henkilötietojen suojasta sekä verkko- ja tietojärjestelmien turvallisuudesta

Väärinkäytös ja muu moitittava tai epäeettinen toiminta voi olla huolimattomuudesta tai osaamattomuudesta johtuvaa, tahallista tai jopa rikokseksi katsottavia tekoja tai laiminlyöntejä. Väärinkäytösepäily voi kohdistua yksittäiseen viranhaltijaan, työntekijään tai luottamushenkilöön tai esimerkiksi kaupungin palveluiden tuottamiseen, työyhteisön toimintaan, hankintoihin, sopimuksiin tai päätöksentekoon.

Kaupungin työntekijä voi jättää ilmoituksen joko omalla nimellä tai anonyymisti. Kaikki ilmoitukset käsitellään luottamuksellisesti eikä ilmoituksen tekijää voi jäljittää. Kaupungin ilmoituskanavaan tulleet ilmoitukset tulevat tietosuojavastaavalle sekä hallinnonsuunnittelijalle. Vuoden 2024 aikana ilmoituskanavaan tuli yksi ilmoitus, joka ei kuulunut ilmoituskanavan soveltamispiiriin, mutta ilmoitus on käsitelty.

3.5 Tietopyynnöt

Rekisteröidyllä on oikeus tietää, mitä tietoja hänestä on tallennettu ja miten tietoja on käytetty.

Vuonna 2024 kaikki omien tietojen tietopyynnöt (2 kpl) ovat koskeneet koulutodistuksia.

Julkiisuuslain mukaisia tietopyyntöjä on tullut 45 kpl.

3.6 Tietoturva- ja tietosuojaryhmä

Tietoturva- ja tietosuojaryhmä kokoontui vuoden 2024 aikana kahdeksan kertaa.

Tietoturva- ja tietosuojaryhmä seuraa tietoturvallisuuden ja tietosuojan yleistä kehittymistä, uhkia ja riskejä sekä tietoturvallisuuden ja tietosuojan toteutumista kaupungissa. Se myös tekee kehitysehdotuksia tietoturvallisuuden ja tietosuojan parantamiseksi sekä avustaa tietojen, tietojärjestelmien ja prosessien omistajia ylläpitämään ja kehittämään tietoturva- ja tietosuoja-asioita.

4. Tietoturva

Tietoturva liittyy läheisesti tietosuojaan. Rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetusta. Tietoturvatoinenpiteet, kuten käyttöoikeuksien hallinta ja käyttöoikeusrajaukset, järjestelmälokitukset, auditoinnit sekä kyky taata järjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyyys ja vikasietoisuus sekä kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa, ovat teknisiä toimenpiteitä, joilla pyritään varmistamaan tietosuojan toteutuminen.

5. Tiedon hallinta

Organisaation tulee suunnitella ja kuvata tiedonhallinnan, tietovarantojen ja tietovirtojen kokonaistilanteensa. Tarkoituksena on selventää sitä, miten tietoa hallitaan sen koko elinkaaren ajan, tiedon vireille tulosta hävittämiseen tai arkistointiin saakka. Lisäksi kuvaukset toimivat ja toteuttavat julkisuusperiaatetta sekä toimivat omien tietojen pyyntöön liittyvinä apuvälineinä.

Uudenkaupungin kaupungin asiakirjojen hallintaa ohjaa tiedonohjaussuunnitelma, joka on asiakirjojen rekisteröinnin, käsittelyn ja säilyttämisen ohjeisto.

Tiedonohjaussuunnitelmassa kuvataan kaupungin tehtävät ja käsittelyprosessit, tehtävien hoidossa syntyvän asiakirjallisen tiedon ohjaus- ja hallintaperiaatteet sekä tietojen säilytysajat.

Kaupungilla on käytössä Innofactorin Dynasty 10.3 -asianhallintajärjestelmä. Järjestelmä toimii kaupungin hallinnon ja toimielinten hallinnollisten asioiden asiarekisterinä. Tämän lisäksi tietoja käsitellään ja säilytetään muissa operatiivisissa järjestelmissä.

Vuoden 2025 aikana otetaan käyttöön sähköinen arkisto Kirstu. Sähköinen arkisto otetaan käyttöön asteittain niin, että ensimmäisenä arkistoidaan Dynasty-asianhallintajärjestelmän asiat, migroidaan Dynasty 6.4 vanhat kannat ja Softcon arkistosta siirretään arkistoitava aineisto, Populus ja Unit4.

Kaupungin palkanlaskenta siirtyi vuoden 2024 huhtikuussa Tilikunnan hoidettavaksi.

5.1 Tiedonhallintamalli

Kunnassa on ylläpidettävä sen toimintaympäristön tiedonhallintaa määrittelevää ja kuvaavaa tiedonhallintamallia. Tiedonhallintamallia ylläpidetään palvelujen, asiankäsittelyn ja tietoaineistojen hallinnan suunnittelemiseksi ja toteuttamiseksi, tiedonsaantia koskevien oikeuksien ja rajoitusten toteuttamiseksi, moninkertaisen tietojen keruun vähentämiseksi, tietojärjestelmien ja tietovarantojen yhteentoimivuuden toteuttamiseksi sekä tietoturvallisuuden ylläpitämiseksi.

Uudenkaupungin kaupungin tiedonhallintamalli on laadittu Digiturvamalli-työkaluun tallennettavien tietojen pohjalta.

5.2 Asiakirjajulkisuuskuvauk

Asiakirjajulkisuuskuvauk antaa yleiskuvan tiedonhallinnasta ja siitä, miten ja missä laajuudessa keräämme ja käsittelemme tietoj

Asiakirjajulkisuuskuvauk toteuttaa julkisuusperiaatetta. Tavoitteena on auttaa asiakasta kohdistamaan tietopyyntönsä ja yksilöimään tietopyynnön oikein.

Tiedonhallintalain edellyttämä asiakirjajulkisuuskuvauk on laadittu Digiturvamalli-työkaluun tallennettavien tietojen pohjalta ja se on julkaistu kaupungin verkkosivuilla.

6. Tietosuoja

Yksi tietotilinpää

Esiin nousseet kehittämiskohteet ja tehdyt toimenpiteet:

- Vaikuttavuusarviointien tekeminen niiden tietojärjestelmien ja henkilörekisterien osalta, jotka hyvinvointialueuudistuksen jälkeen jäivät kaupungille.
 - Tällä hetkellä tehtyinä on tietosuoja

toiminnanohjausjärjestelmän Daisyn DPIA sekä Google Workspace for Education -oppimisympäristön DPIA.

- Vuosittainen tietoturva- ja -suojakoulutuksen tarjoaminen kaupungin henkilöstölle sekä uuden työntekijän perehdytyksessä
 - Perusopetuksen digitutoreiden tehtävänä on ollut lukuvuonna 2024–2025 antaa tietoiskuja tietoturvaan ja tietoturvaan liittyen omissa yksiköissään. Digitutoreiden kanssa on kuukausittain sovittu, mikä on seuraava asia, josta he tiedottavat omien yksiköidensä opettajia esimerkiksi opettajankokousten yhteydessä. Perusopetuksessa monialaisena oppimiskokonaisuutena oli myös ”Turvallisuus, tietosuoja ja tietoturva”, johon tehtiin oma sites-sivustonsa opettajien käyttöön. Lisäksi perusopetuksen digitutorit ovat saaneet koulutusta tekoälystä, tiedottaneet yksiköissään tekoälyn käytöstä opetuksessa ja jakaneet opettajille tehdyt päivittyvät ohjeistukset tekoälyn käyttöön liittyen. Lukuvuoden 2025–2026 koulutusteemana tulee olemaan muun muassa tekoäly.
- Keskeisten ja kriittisten tietojärjestelmien ja sovellusympäristöjen varautumis- ja palautumissuunnitelmien tekeminen
 - tekemättä mm. prosessit ja kattavat suunnitelmat. Tällä hetkellä asiaa on tarkasteltu sekä teknisen palautumisen että toiminnan jatkumisen näkökulmasta mutta ei toiminnan palautumisen näkökulmasta.