

TORNION KAUPUNGIN KUNNALLINEN SÄÄNTÖKOKOELMA

Tornion hallintopalvelut



Tornio

TORNION KAUPUNGIN TIETOTURVA- JA TIETOSUOJAHOHJE

Hyväksytty

Kaupunginhallitus 18.11.2019 § 364

Päivitetty

Kaupunginhallitus 19.6.2023 § 198

Tietoturva- ja tietosuojatyöryhmä 5.12.2023

Tietoturva- ja tietosuojatyöryhmä 26.2.2025

Kaupunginhallitus 4.5.2026

Sisällys

TORNION KAUPUNGIN TIETOTURVA-JA TIETOSUOJAOHJE	1
1 Johdanto	3
2 Käsitteitä ja määritelmiä	3
OSA 1 TIETOSUOJAOHJE	5
3 Tietosuojaperiaatteet	5
4 Kaupungin eri toimijoiden vastuut	5
5 Tietosuojan toteutuminen	6
OSA 2 TIETOSUOJA JA HENKILÖTIETOJEN KÄSITTELY	8
6 Henkilötietojen käsittelyn periaatteet	8
7 Rekisteröidyn oikeudet	10
8 Henkilötietojen tietoturvaloukkauksista ilmoittaminen ja niiden käsittely	10
OSA 3 TIETOTURVAOHJE	13
9 Mitä on tietoturvallisuus?	13
10 Käyttöoikeuksien hakeminen	14
11 Tietojenkäsittely	15
12 Tietokoneen ja mobiililaitteiden käyttö	15
13 Internet, pilvipalvelut, sosiaalinen media ja sähköposti	16
14 Etäkäyttö ja etätyö	17
15 Omat tiedot ja yksityisyys	18
16 Ilmoitusvelvollisuus	18
17 Salassapitovelvollisuus	19
18 Tietoturva- ja tietosujoahjeen soveltaminen, ylläpito ja uusiminen	19
LIITTEET	23

1 Johdanto

Henkilötietojen käsittely on Tornion kaupungin perustehtävän mukaista toimintaa, jota ohjaavat kaupunkistrategiassa 2026-2029 mainitut toimintaperiaatteet:

- turvallinen
- kestävä
- rohkea

Tietoturva- ja tietosuojahjeella määritetään tietosuojan ja tietoturvan periaatteet, vastuut, toimintatavat, valvonta ja seuraamukset, joilla ohjataan tietoturvan ja tietosuojan kehittämistä. Tavoitteena on luoda yhdenmukaiset toimintaperiaatteet ja käytännöt. Ohjeen osat 1 ja 2 käsittelevät tietosuojaa ja osa 3 tietoturvaa. Ohjetta tarkennetaan tarvittaessa toimialakohtaisilla käytännönohjeistuksilla.

Yleisperiaatteena

- käsittelemme henkilötietoja asianmukaisesti ja lainsäädännön vaatimalla tavalla
- ohjeistamme käsittelemään henkilötietoja läpinäkyvästi
- minimoimme kerättävien henkilötietojen määrää ja painotamme virheettömyyttä
- ohjeistamme informoimaan avoimesti ja selkeästi
- tiedotamme, että yksityishenkilöillä (rekisteröidyillä) on tietosuojasetuksen mukaisesti oikeuksia, joiden avulla he voivat ymmärtää ja seurata, miten heidän tietojensa käsitellään ja käytetään eri tarkoituksiin.

Uudet lainsäädäntömuutokset, erityisesti 25.5.2018 sovellettavaksi tullut EU:n yleinen tietosuojasetus (GDPR), vahvistavat luonnollisten henkilöiden oikeutta henkilötietojen suojaan. Tietosuojalaki ja EU:n saavutettavuusdirektiivi tähtäävät tietoturvan, tietosuojan, riskienarvioinnin, kokonaisarkkitehtuurin ja yhteen toimivuuden huomioimiseen suunnittelussa ja sen kautta saatavaan kustannustehokkuuteen ja tietojen käytettävyyteen.

Tietoturvallisuuden ja tietosuojan toteutumiseksi kaupungin tulee tunnistaa sen toiminnan kannalta elintärkeät palvelutehtävät ja määritellä niiden turvaamiseksi riittävät tietoturvaperiaatteet.

Jokaisen viranhaltijan, työntekijän ja kaupungin luottamushenkilön sekä muiden tietojärjestelmien käyttäjien on tunnettava tämä organisaation tietoturva- ja tietosuojahje ja noudatettava siinä annettuja ohjeita ja määräyksiä. Myös palveluntarjoajien, järjestelmätoimittajien ja muiden ulkopuolisten tahojen tulee sitoutua noudattamaan tätä ohjetta, kansallisia sekä kansainvälisiä säädöksiä sekä ohjeita ehtona tehtäviensä mukaiselle pääsyyllä organisaation tietojärjestelmiin ja niiden sisältämiin tietoihin.

2 Käsitteitä ja määritelmiä

Sisäistääksesi tämän tietoturva- ja tietosuojahjeen sisällön, sinun on tunnettava ainakin seuraavat käsitteet ja määritelmät.

Tietoturva ja tietosuojaja

Tietoturva on yksi tietosuojan toteuttamisen keino. Sen tarkoitus on suojata tietoaineisto ja tietojärjestelmät. Tietoturva tarkoittaa muun muassa organisatorisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon saatavuus, luottamuksellisuus ja eheys, järjestelmien käytettävyyttä sekä rekisteröidyn oikeuksien toteutuminen.

Tietosuojaja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.

Henkilötieto

Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön (rekisteröityyn) liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

Tällaisia henkilön tunnistettavuustietoja ovat esimerkiksi:

- nimi
- henkilötunnus (hetu)
- sähköpostiosoite
- työntekijä-/opiskelijanumero
- sijaintitieto (esim. kotiosoite tai paikkannustieto)
- verkkotunnistetiedot (esim. ip-osoite)
- yksi tai useampi henkilöä koskeva tunnusomainen fyysinen, geneettinen, psyykinen, taloudellinen, kulttuurinen tai sosiaalinen tekijä (esim. valokuva, sormenjälki, hiusten-, silmien- ja ihonväri)

Henkilörekisteri

Henkilörekisterillä tarkoitetaan mitä tahansa jäseneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot on saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu.

Rekisterinpitäjä

Rekisterinpitäjä on se taho, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjä voi olla luonnollinen henkilö tai oikeushenkilö, viranomainen tai toimielin, jonka käyttöä varten rekisteri perustetaan ja jolla on oikeus määrätä rekisterin käytöstä.

Henkilötietojen käsittelijä

Henkilötietojen käsittelijä on se henkilö, viranomainen, virasto, alihankkija tai muu taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Henkilötietojen käsittely

Henkilötietojen käsittelyllä tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietokäsittelyä käyttäen tai manuaalisesti, *kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.*

Tietosuojavastaava

Rekisterinpitäjän ja henkilötietojen käsittelijän on nimitettävä tietosuojavastaava tietosuojasäädösten mukaisesti. Tietosuojavastaavan tehtävinä on mm. osallistua organisaation henkilötietojen käsittelyä koskevaan suunnittelu-toimintaan, ohjeistaa henkilötietojen käsittelyä ja niiden suojausmenetelmiä, tukea henkilökuntaa tietosuoja-asioissa (mm. koulutus ja ohjeistus), toimia yhdysiteenä valvontaviranomaisiin ja vastata organisaation johdon osoittamista muista tietosuojaa tukevista tehtävistä.

OSA 1 TIETOSUOJAOHJE

3 Tietosuojaperiaatteet

3.1 Tietosuojan tavoite, rekisterinpitäjä ja henkilötietojen käsittelyn periaatteet

Tietosuojan tavoite on suojata henkilön perusoikeuksia ja –vapauksia, erityisesti henkilön ja hänen perheensä yksityisyyden suojaa. Tietosuojalla turvataan henkilötietojen asianmukainen käsittely koko kaupungin organisaation toiminnassa, varmistetaan tietojen oikeellisuus ja ennalta ehkäistään henkilötietojen käyttöön liittyviä loukkauksia. Tornion kaupungissa noudatetaan asiakkaiden, kaupunkilaisten, kaupungin henkilöstön ja muiden sidosryhmien henkilötietojen käsittelyssä voimassa olevia tietosuojasäädöksiä. Toukokuusta 2018 lähtien EU:n yleinen tietosuoja-asetus on velvoittanut suunnittelemaan ja dokumenteina osoittamaan, että henkilötietojen käsittelyssä noudatetaan lakia ja kaupungin ohjeita.

Rekisterinpitäjänä on Tornion kaupunki, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. *Nämä määritykset ovat luettavissa Rekisteröidyn informointi-ilmoituksista/tietosuojaselosteista, jotka löytyvät kaupungin verkkosivuilta ja asiakaspalvelupiste Kompassista.*

Tornion kaupungin tietosuojaohjeessa määritetään linjaukset, periaatteet ja vastuut tietosuojan hallinnoinnissa ja henkilötietojen käsittelyssä. Hyvän tietosuojatason saavuttamiseksi jokaisen henkilön tulee ymmärtää tietojen käsittelyn periaatteet: *mitä tietoa saa käsitellä, missä tarkoituksessa ja milloin saa käsitellä sekä mitkä ovat rekisteröidyn oikeudet.*

4 Kaupungin eri toimijoiden vastuut

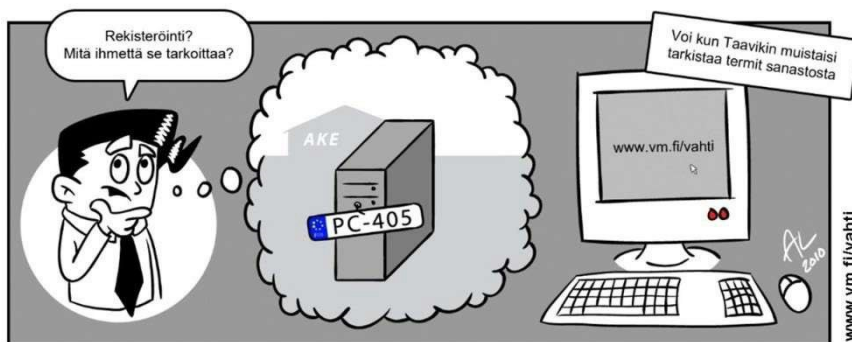
Kaupunginjohtajan ja toimialajohtajien rooli tietosuojan toteutumisessa on merkittävin. Tornion kaupungin ja sen toimialojen johtamisjärjestelmästä on säädetty hallintosäännössä ja sen perusteella annetuin delegointipäätöksin. Tietosuojan johtaminen, vastuu ja organisointi noudattavat samaa johtamisjärjestelmää. Johto, mukaan lukien toimielimet ja esihenkilöt tekevät niitä päätöksiä, joilla johdetaan ja vaikutetaan siihen, miten tietosuoja Tornion kaupungilla toteutuu. Kukin toimialajohtaja vastaa omalla toimialallaan tietosuojan lainmukaisuudesta. Heidän vastuullaan on huolehtia mm. riittävästä resursoinnista ja siitä, että tietosuoja otetaan huomioon kaikissa toiminnoissa.

Digitryöryhmä valmistelee tietosuojalainsäädännön käytännön toteutusta; ohjaa ja koordinoi sitä yhteistyössä palvelualueiden johdon ja esihenkilötason kanssa ja mm. valmistelee tietoturva- ja tietosuojaohjeen sekä muut käytännön ohjeet Tornion kaupungille ja suorittaa osaltaan tietoturvan ja –suojan toteutumisen seurantaa, arvioi tietoturvariskejä sekä raportoi tietoturvallisuuden tilasta kaupungin johdolle.

Tietosuojavastaava antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle sekä henkilötietoja käsitteleville työntekijöille tietoja ja neuvoja, dokumentoi sekä mm. seuraa, että tietosuoja-asetusta ja muita tietosuojamääräyksiä noudatetaan. Tietosuojavastaava tekee myös yhteistyötä valvontaviranomaisen kanssa.

Tietohallinto vastaa tietoturvan kehittämisestä ja teknisestä järjestämisestä siten, että tietosuoja toteutuu. Se vastaa tietojärjestelmien häiriöttömästä toiminnasta ja turvallisuudesta saamiensa resurssien ja toimintavaltuuksien puitteissa.

Jokaisella, joka käsittelee Tornion kaupungin toiminnan tuloksena syntyvää tietoa, on vastuu kokonaisturvallisuudesta. Henkilötietoja saavat käsitellä vain ne henkilöt, joilla on siihen tehtäviensä vuoksi oikeus.



Käyttöoikeudet rajataan henkilön työtehtävien mukaisesti. Jokainen tietoja ja tietojärjestelmiä käyttävä henkilö on velvollinen ilmoittamaan havaitsemistaan tietoturvaloukkauksista ja tietoturvallisuuden/tietosuojan puutteista tässä ohjeessa mainitulla tavalla.

5 Tietosuojan toteutuminen

5.1 Tietosuoja on koko organisaation asia

Hyvän tietosuojatason saavuttaminen ja ylläpitäminen vaatii koko henkilöstöltä tietosuojakäytäntöjen merkityksen ymmärtämisen sekä niihin sitoutumisen, jotta taataan koko Tornion kaupungin organisaatiossa häiriötön toiminta sekä normaali- että poikkeusoloissa. Tietosuoja tulee huomioida niin manuaalisessa kuin sähköisessä henkilötietojen käsittelyssä ja niin puhutussa kuin kirjoitetussa tiedossa.

5.2 Tietosuojan vaikutustenarviointi (DPIA)

Kun Tornion kaupunki rekisterinpitäjänä ottaa käyttöön uuden järjestelmän tai palvelun, jossa käsitellään henkilötietoja, on arvioitava tietosuojan vaikutustenarvioinnin tarve. Jos käsittely todennäköisesti aiheuttaa luonnollisen henkilön oikeuksien kannalta korkean riskin, on vaikutustenarviointi tehtävä **ennen käsittelyn aloittamista**.

Tietosuojan vaikutustenarviointi on tietosuoja-asetuksen mukainen tehtävä, jonka dokumentointi kuuluu myös rekisterinpitäjän osoitusvelvollisuuteen. Osoitusvelvollisuus tarkoittaa, että rekisterinpitäjän on pystyttävä osoittamaan noudattavansa tietosuojalainsäädäntöä.

Ohje tietosuojan vaikutustenarvioinnin tekemiseen löytyy Tornion kaupungin intranetistä. Lomakkeet ja ohjeistusta saa tietosuojavastaavalta.

5.3 Sopimukset henkilötietojen käsittelyn ulkoistamisessa

Silloin, kun Tornion kaupunki rekisterinpitäjänä ulkoistaa henkilötietoja sisältävien tehtäviensä käsittelyn toimeksisaajalle/palveluntuottajalle (henkilötietojen käsittelijälle), se valitsee sopimus Kumppanikseen vain sellaisia toimijoita, jotka noudattavat hyvää henkilötietojen käsittelytapaa asianmukaisten teknisten ja organisatoristen toimenpiteiden avulla sekä täyttävät tietosuoja-asetuksen vaatimukset ja pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta.

Tornion kaupungin ja erikseen valitun henkilötietojen käsittelijänä toimivan toimeksisaajan/palveluntuottajan välille laaditaan kirjallinen sopimus. Siihen määritellään mahdollisimman tarkasti tietosuoja-asetuksen vaatimukset (mm. henkilötietojen käsittelyn kohde, tarkoitus, kesto ja sovitaan käsiteltävät henkilötiedot).



5.4 Seuraamukset laiminlyöntitilanteissa

Jokainen Tornion kaupungin työntekijä tutustuu perehdyttämistilanteessa esihenkilönsä opastamana kaupungin tietoturva- ja tietosuojaohjeisiin ja on velvollinen noudattamaan niitä. Lisäksi jokainen on velvollinen suorittamaan henkilöstön tietoturva- ja tietosuojakoulutuksen verkko-opiskeluna.

Rikkomustapauksissa työntekijä on tietojen käsittelijänä vastuussa vahingosta. Havaitut rikkomukset raportoidaan kaupungin johdolle ja tietosuojavastaavalle, joka dokumentoi ne asianhallintajärjestelmään. Taulukko rikkomuksen seuraamuskäytännöistä on tämän ohjeen luvussa 8.

OSA 2 TIETOSUOJA JA HENKILÖTIETOJEN KÄSITTELY

6 Henkilötietojen käsittelyn periaatteet

6.1 Miten henkilötietoja käsitellään ja milloin niitä saa käsitellä?

Henkilötietojen käsittelyssä noudatetaan yksityiselämän suojaa ja muita perusoikeuksia sekä hyvää tiedonhallintatapaa varmistavia menetelmiä.

Henkilötietojen käsittelyssä noudatetaan aina tietosuojalainsäädännön mukaisia tietosuojaperiaatteita. Henkilötietoja

- ✓ *käsitellään lainmukaisesti ja asianmukaisesti*
- ✓ *käsitellään rekisteröidyn kannalta läpinäkyvästi*; rekisteröityä informoidaan hänen tietojensa käsittelystä, rekisteröidyn oikeuksia kunnioitetaan ja oikeuksien turvaamiseksi luodaan käytäntöjä ja ohjeita
- ✓ *käsitellään luottamuksellisesti ja turvallisesti*
- ✓ *kerätään ja käsitellään tiettyä, nimenomaista ja laillista tarkoitusta varten*; henkilötietojen käsittely suunnitellaan ja käsittelytoimet määritellään tiedon koko elinkaari huomioiden; henkilötietoja käsitellään vain siinä laajuudessa kuin se on kyseisen palvelun/tehtävän kannalta tarpeellista; tietoja ei käytetä tarkoituksen kannalta yhteensopimattomalla tavalla
- ✓ *kerätään vain tarpeellinen määrä henkilötietoja* käsittelyn tarkoitukseen nähden; henkilötietoja ei voi kerätä esim. ainoastaan siltä varalta, että niiden käyttö voisi myöhemmin osoittautua hyödylliseksi
- ✓ *päivitetään aina tarvittaessa* – epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä
- ✓ *säilytetään muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.*



6.2 Arkaluonteisen ja lasten henkilötietojen käsittely

Henkilötietojen käsittelylle on aina oltava laissa säädetty käsittelyn oikeusperuste. Sellaisten erityisiin henkilötietoryhmiin kuuluvien henkilötietojen käsittely, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettisten tai biometrinen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevien tietojen käsittely on lähtökohtaisesti kiellettyä. Niitä voidaan käsitellä vain

- ✓ rekisteröidyltä tai hänen edunvalvojaltaan saadun suostumuksen perusteella
- ✓ jos käsittely on tarpeen elintärkeiden etujen suojaamiseksi tai
- ✓ jos käsittely on tarpeen lainsäädännön nojalla tärkeää yleistä etua koskevasta syystä

Suuri osa Tornion kaupungin keräämistä henkilötiedoista perustuu lakisääteisten tehtävien hoitamiseen. Mikäli henkilötietojen käsittelylle ei ole erityislain perustetta, rekisteröidyltä pyydetään kirjallinen suostumus (suostumuslomakkeella). Ennen sen antamista on rekisteröityä informoitava suostumuksen merkityksestä. Jotta suostumus on pätevä, se on oltava yksilöity, tietoinen, aidosti vapaaehtoinen ja yksiselitteinen tahdonilmaisuu. Jos henkilötietojen käsittelyn tarkoitus muuttuu, pyydetään rekisteröidyltä uusi suostumus.

Alle 13-vuotias lapsi tarvitsee tietosuojalainsäädännön mukaan huoltajan tai muun vanhempainvastuunkantajan suostumuksen tai valtuutuksen tietoyhteiskunnan palveluiden, esimerkiksi sosiaalisen median ja erilaisten sovellusten käyttöön. Lapsi voi kuitenkin käyttää neuvonta- ja tukipalveluja sekä ennalta ehkäiseviä palveluja ilman huoltajan suostumusta.

6.3 Käyttöoikeudet sekä salassapito ja vaitiolovelvollisuus

Tietojärjestelmien käyttöoikeudet annetaan vain niille henkilöille, joilla siihen on tehtäviensä vuoksi tarve. Käyttöoikeudet hakee esihenkilö täyttämällä ja lähettämällä käyttöoikeuslomakkeen tietohallinnolle (ks. sivu 15, Osa 3, Tietoturvaohje, käyttöoikeuksien hakeminen). Käyttöoikeuksien myöntämisestä ja mahdollisesta muutoksesta tulee jäädä lokimerkintä tai muu dokumentti, jotta käyttöoikeuksia voidaan tarvittaessa selvittää myös jälkikäteen.

Tietovarastojen tietoja, joihin sinulla on käyttöoikeudet, saat käyttää vain omiin työ-/virkatehtäviisi. Henkilörekisterin tietojen käyttötarkoituksen vastainen käyttö on lainvastaista. Pelkkä tietojen katselu on myös henkilötietojen käsittelyä, johon pitää olla aina perusteet. Tämä tarkoittaa käytännössä, ettei asiakirjaa tai asiaa saa pelkästä mielenkiinnosta avata, jollei se liity omaan työtehtävään. Asianhallintajärjestelmään tehdään säännöllisesti tietosuojatarkastuksia ja näistä ilmenee kuka ja milloin on dokumentteja avannut.

Tornion kaupungin palveluksessa olevat henkilöt tai ulkopuoliset toimeksisaajat eivät saa ilmaista sivullisille toisen henkilön terveydentilaa, taloudellista asemaa ja henkilökohtaisia oloja koskevia tietoja, joita ovat saaneet tietoonsa henkilötietojen käsittelyyn liittyviä tehtäviään hoitaessaan tai muutoin. Tähän heitä veloitetaan

työ- tai muilla sopimuksilla. Veloitte on voimassa työ-, sopimus- tai muun toimeksiantosuhteen päätyttyäkin. Veloitteen rikkominen on rangaistava teko.



7 Rekisteröidyn oikeudet

Rekisteröidyn tärkeimpiä oikeuksia ovat:

1. Oikeus saada selkeää informaatiota henkilötietojensa käsittelystä

Henkilörekistereistä laaditaan tietosuoja-asetuksen mukainen informointi-ilmoitus/tietosuojaseloste (liite 1), jossa kerrotaan mm. henkilötietojen käsittelyn tarkoitus ja oikeusperuste; mistä tiedot on saatu ja mahdolliset tietojen vastaanottajat, mitä tietoja kerätään sekä tiedot rekisteröidyn oikeuksista.

Informointi-ilmoitukset/tietosuojaselosteet ovat nähtävillä kaupungin verkkosivuilla ja asiakaspalvelupiste Kompassissa. Rekisterin vastuuhenkilö ja yhteyshenkilö pitävät informointi-ilmoituksen/tietosuojaselosteen jatkuvasti ajan tasalla. Ajantasainen versio toimitetaan aina sähköisessä muodossa kaupungin tietosuojavastaavalle.

2. Oikeus päästä häntä itseään koskeviin henkilötietoihin

Pyyntö käyttää oikeuttaan tehdään kaupungin verkkosivuilla sähköisellä henkilötietojen käsittely/tarkastuspyyntö-lomakkeella.

Lomakkeen voi myös tarvittaessa tulostaa tallentamalla sen ensin pdf-muotoon (lomakkeen alareunasta) ja toimittaa kaupungintalon asiakaspalvelupisteeseen, tai lähettää osoitteeseen Tornion kaupunki / Kirjaamo, Suensaarenkatu 4, 95400 Tornio.

3. Oikeus pyytää henkilötietojen oikaisemista tai poistamista taikka käsittelyn rajoittamista

Pyyntö käyttää oikeuttaan tehdään kaupungin verkkosivuilla [sähköisellä rekisteritietojen korjausvaatimus - lomakkeella](#).

Katso tulostus- ja toimitusohjeet kohdasta 2.

4. Oikeus tehdä valitus valvontaviranomaiselle epäkohdasta henkilötietojen käsittelyssä

Rekisteröity voi tehdä henkilötietojensa käsittelyä koskevan valituksen tietosuojavaltuutetun toimistoon käyttämällä [sähköistä lomaketta](#).

Tietosuojavaltuutetun toimiston yhteystiedot löytyvät [Tietosuojavaltuutetun toimiston verkkosivuilta](#).

8 Henkilötietojen tietoturvaloukkauksista ilmoittaminen ja niiden käsittely

Tornion kaupungilla on laadittu toimintaprosessi henkilötietoihin kohdistuvien tietoturvaloukkausten varalle (**liite 2**). Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvottomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi:

- pääsy henkilötietoihin, joihin ei ole oikeutta
- henkilötietojen postittaminen väärälle henkilölle
- henkilötietoja sisältävä asiakirja tulostuu väärään tulostimeen
- joukkosähköpostiviesti lähetetään vastaanottajille, jolloin kaikki vastaanottajat voivat nähdä muiden vastaan- ottajien yksityiset sähköpostiosoitteet
- hävinnyt tiedonsiirtoväline, esim. USB-muistitikku, joka sisältää henkilötietoja
- haittaohjelmatartunta
- hakkerointi
- kyberhyökkäys
- varastettu tietokone
- varastettu mobiililaitte (älypuhelin tai tablettitietokone)

Jos havaitset tietoturvaloukkauksen, ilmoita siitä välittömästi sähköisellä lomakkeella:

[Ilmoitus tietoturvaloukkauksesta.](#)

Järjestelmän/laitteiston teknisen ongelman aiheuttamasta tietoturvaongelmasta tulee ilmoittaa välittömästi myös tietohallintoon HelpDeskiin, puh. 016 432 400

Tietoturvaloukkaus ilmoituksen saatuaan tietosuojavastaava tekee vakavuuden arvioinnin (tiedon luonne ja määrä) sekä kirjaa ilmoituksen asianhallintajärjestelmään. Ilmoituksen käsittelyä ja tiedottamista varten perustetaan tapauskohtaisesti työryhmä. Työryhmän tehtävänä on päättää yhdessä mihin toimenpiteisiin ryhdytään tietoturvaloukkauksen takia.

Tornion kaupungin velvollisuus on reagoida tietoturvaloukkaukseen nopeasti; 72 tunnin kuluessa siitä, kun on tultu tietoiseksi tietoturvaloukkauksesta. Henkilötietojen tietoturvaloukkauksesta ilmoitetaan tietosuoja-asetuksen mukaisesti valvontaviranomaiselle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille tai vapauksille. Jos se todennäköisesti aiheuttaa korkean riskin henkilön oikeuksille ja vapauksille, tietoturvaloukkauksesta on ilmoitettava tietosuoja-asetuksen mukaisesti myös rekisteröidylle.

Tietosuojavastaava dokumentoi tietosuoja-asetuksen mukaisesti kaikki tietoturvaloukkaukset sekä niiden vaikutukset ja toteutetut korjaavat toimenpiteet riippumatta siitä, mitä toimenpiteitä tietoturvaloukkauksesta lopulta seuraa.

Taulukko rikkomuksen aiheuttamista henkilötietojen tietoturvaloukkauksista ja niiden seuraamus-käytännöistä:

TAHALLISUUDEN ASTE RIKKOMUSTEN VAKAVUUS	Tietämättömyys, osaamattomuus, erehdys, vahinko, huolimattomuus	Piittaamattomuus, tahallisuus, toistuvuus
Vakava rikkomus (lain mukaan rikkomuksena tai rikoksena tuomittava teko)	<ul style="list-style-type: none"> - puheeksi ottaminen ja opastus - suullinen huomautus - kirjallinen varoitus - rikosilmoitusta harkitaan tai tehdään 	<ul style="list-style-type: none"> - tehdään rikosilmoitus - palvelussuhteen päättämismenettelyn käynnistäminen
Rikkomus (vakava väärinkäyttö tai turvallisuuden rikkominen)	<ul style="list-style-type: none"> - puheeksi ottaminen ja opastus - suullinen huomautus - kirjallinen varoitus 	<ul style="list-style-type: none"> - kirjallinen varoitus - rikosilmoitusta harkitaan tai tehdään - palvelussuhteen päättämismenettelyn käynnistys
Lievä rikkomus (asiaton toiminta tai väärinkäytös)	<ul style="list-style-type: none"> - puheeksi ottaminen ja opastus - suullinen huomautus 	<ul style="list-style-type: none"> - suullinen huomautus - kirjallinen varoitus - palvelussuhteen päättämismenettelyn käynnistys

• **Vakava rikkomus (lain mukaan rikkomuksena tai rikoksena tuomittava teko)**

- Salassa pidettävien tietojen oikeudeton käsittely ja luovuttaminen (esim. potilastietojen katsominen ilman oikeudellista perustetta)
- Tietojen luvaton käyttö (esim. tekijänoikeuden loukkaus tai rikoslain alaisen materiaalin oikeudeton käsittely ja hallussapito, kuten mm. rasistinen aineisto tai lapsiporno)
- Hakkerointi ja tunkeutuminen tietojärjestelmiin
- Vahingonteko (esim. virusten tahallinen levittäminen tai palvelun tahallinen estäminen)
- Vakoilu
- Virka-aseman väärinkäyttö
- Hyötymistarkoitus



- **Rikkomus (vakava väärinkäyttö tai turvallisuuden rikkominen)**

- Ohjeiden vastainen laitteistojen tai ohjelmien käyttö
- Tunnuksen luovuttaminen (esim. salasanan kertominen toiselle käyttäjälle tai avoimen työaseman luovuttaminen niin, että toinen pääsee valvomatta käyttämään luovuttajan tunnusta)
- Tiedon luottamuksellisuuden vaarantaminen (esim. työaseman jättäminen auki valvomatta tai poliittiedon luovuttaminen henkilölle, jolla ei ole oikeutta saada sitä)
- Ylläpito-oikeuksien luvaton hallussapito
- Ohjelmien ja pelien luvaton kopiointi
- Luvattomien ohjelmien asentaminen
- Luvattomien laitteiden lisääminen verkkoon

- **Lievä rikkomus (asiaton toiminta tai väärinkäytös)**

- Henkilökohtaisen tietoturvan/tietosuojan laiminlyönti (esim. käyttäjätunnuksen huolimaton käyttö, salasanan jättäminen näkyviin, salassa pidettävien asiakirjojen jättäminen näkyviin)
- Haitan aiheuttaminen (esim. laitteiden/ohjelmien lukitseminen ja toisten oikeutetun pääsyn estäminen)
- Resurssien tuhlaus (esim. työajan väärinkäyttö, kuten asiaton surffailu internetissä/somessa)
- Luvaton kaupallinen tai poliittinen toiminta (esim. sähköpostin käyttäminen henkilökohtaiseen markkinointiin)
- Kulunvalvontaohjeiden rikkominen (esim. avainten luovuttaminen toisen käyttöön)



OSA 3 TIETOTURVAOHJE

9 Mitä on tietoturvaluisuus?

Tietoturvaluisuus on tärkeä osa organisaation kokonaisturvaluisuutta, sisäistä valvontaa ja riskienhallintaa. Tietoturvaluisuus koostuu tietoturvaan ja tietosuojaan liittyvistä vastuista ja käytännöistä, joilla pyritään varmistamaan tietojen, tietojärjestelmien ja palvelujen suojaaminen ja turvaaminen siten, että niiden luottamuksellisuus, eheys ja saatavuus voidaan taata ja osoittaa toteutuneen.

- **Luottamuksellisuus:** Tiedot, tietojärjestelmät ja palvelut ovat vain niihin oikeutettujen saatavilla eikä niitä luvatta paljasteta tai muutoin saateta sivullisten tietoon.

- **Eheys:** Tiedot, tietojärjestelmät ja palvelut ovat oikeita ja eheitä, eivätkä muuttuneet tahallisen tai tahattoman teknisen tai inhimillisen toiminnan seurauksena.

- **Saatavuus:** Tiedot, tietojärjestelmät ja palvelut ovat tarvittaessa niihin oikeutettujen esteettä hyödynnettävissä.

Tietoturva, kuten tietosuojakin on huomioitava organisaation kaikessa toiminnassa jo suunnitteluvaiheessa. Tornion kaupungilla tietoturva on myös osa kaupunkistrategiaa ja kaupungin arvoja.

Työssään tai luottamustehtävissään tietoja tarvitsevilla tulee olla riittävät oikeudet ja tietoja tulee käsitellä salassapitosäännösten mukaisesti. Tietoaineistoja, tietojärjestelmiä ja palveluita pitää suojata kaupungin tietoturva- ja tietosuojajelman mukaisesti ja niihin pääsy tulee varmistaa käyttöoikeuksia hallinnoimalla siten, että myös tietoihin liittyvät riskit tulevat huomioituiksi.

Tietoturvariskien hallinnan on oltava suunnitelmallista ja keskeinen osa jatkuvaa tietoturvatyötä. Riskien arviointi käsittää ne toimenpiteet, joilla pyritään tunnistamaan tietoturva- ja tietosuojariskejä sekä toteutuessaan arvioimaan niiden seurauksia sekä varautumaan vikatilanteisiin ja poikkeusolosuhteisiin.

Tornion kaupungin digityöryhmä kartoittaa tietoturva- ja tietosuojariskejä, seuraa niiden toteutumista ja raportoi niistä vuosittain tilinpäätöksen yhteydessä. Kaikki havaitut tietoturvaloukkaukset kirjataan asianhallintajärjestelmään. Näillä toimenpiteillä pyritään poistamaan jo tiedostetut riskit ja ennakoimaan mahdolliset tulevat riskit sekä ohjaamaan tietoturva- ja tietosuojatyön käytännön toteutumista.



© Grafiant / Antti Laitinen 2011

10 Käyttöoikeuksien hakeminen

Tornion kaupungin ja konserniyhtiöiden työntekijöiden käyttöoikeudet tietojärjestelmiin hakee esihenkilö täyttämällä sähköisen **tunnustilauslomakkeen**. Linkki lomakkeeseen löytyy Väylästä digityökalut-sivulta kohdasta käyttöoikeus- ja laitetilaus.

Tunnustilauslomakkeen pakolliset tiedot:

- Tilaajan nimi ja sähköpostiosoite
- Tilauksen tyyppi
- Käyttäjän kaikki etunimet
- Sukunimi
- Syntymäaika muodossa p.k.vvvv
- Henkilötunnus (vaaditaan vain tietyissä järjestelmissä)
- Toimipiste
- Nimike
- Puhelinnumero
- Työsuhteen kesto
- Käyttöoikeuksien voimassaoloaika (määräaikaisessa työsuhteessa)
- Käyttäjän rooli (esihenkilö / työntekijä)
- Toimiala

Käyttöoikeushakemuksen tekijä sitoutuu aina toimittamaan uudelle käyttäjälle Tornion kaupungin tietosuoja- ja tietoturvaohjeen.

Ulkopuolisten käyttäjien käyttöoikeudet haetaan intranetistä löytyvällä erillisellä, tulostettavalla käyttöoikeushakemuksella, johon vaaditaan sekä esihenkilön että työntekijän allekirjoitus. Allekirjoitettu hakemus toimitetaan tietohallintoon paperisena tai skannattuna pdf-tiedostona sähköpostitse osoitteeseen helpdesk@tornio.fi Mikäli hakemus sisältää henkilötietoja esim. henkilötunnuksen tai muita luottamuksellisia tietoja, on skannaamiseen ja lähettämiseen käytettävä salattua skannausta ja salattua sähköpostia.

Tornion kaupungin luottamushenkilöille on olemassa oma käyttöoikeushakemus. Luottamushenkilöt täyttävät ja allekirjoittavat paperisen käyttöoikeushakemuksen ja toimittavat sen tietohallintoon yhdessä laitteen käyttösopimuksen kanssa.

Tornion kaupungin työntekijät ovat allekirjoittaneet tietosuoja/tietoturvasitoumuksen työsuhteensa, joten heiltä ei tarvita erillistä allekirjoitusta ja oikeudet voi hakea sähköisesti.

10.1 Käyttäjätunnusten luovuttaminen

Tietohallinto vastaanottaa käyttöoikeushakemuksen ja **myöntää tunnukset tietokoneelle kirjautumiseen** (verkkotunnus) ja **sähköpostiin**.

Muiden järjestelmien osalta tietohallinto pyytää sovellusten pääkäyttäjiä tekemään käyttäjätunnukset ja ilmoittamaan niistä suoraan käyttäjille.

Tietohallinto luovuttaa verkkotunnuksen ja sähköpostitunnuksen henkilökohtaisesti tunnusten saajalle. Tunnuksia luovuttaessa tietohallinnolla on velvollisuus tarkistaa tunnusten vastaanottajan henkilöllisyys. Vastaanottaessaan tunnukset, työntekijä sitoutuu noudattamaan Tornion kaupungin tietoturva- ja tietosuojaohjeita.

10.2 Muutokset käyttöoikeuksissa

Sähköistä tunnustilauslomaketta käytetään myös käyttöoikeuksien muuttuessa. **Esihenkilön on ilmoitettava työsuhteissa tapahtuvista muutoksista hyvissä ajoin** (esim. työsuhteen päätyminen, määräaikaisen työsuhteen jatkuminen, eläkkeelle siirtyminen, virkavapaus tai muu pitkä poissaolo), jotta tietojärjestelmien käyttöoikeuksiin ei tulisi

tarpeettomia katkoksia ja tieto aktiivisista käyttäjistä pysyy ajan tasalla. Tietohallinto ilmoittaa muutoksista eteenpäin sovellusten pääkäyttäjille.

11 Tietojenkäsittely

- **Käsittele tietoja huolellisesti välineestä riippumatta.** Tarkista ulkoiset tallennusvälineet esim. usb-tikku tietoturvaohjelmalla ennen käyttöä.
- **Henkilötietojen ja salassa pidettävien tietojen tallentaminen ulkoisiin tallennusvälineisiin on kielletty.**
- **Kun syötät salasanoja, huolehdi, että kukaan ei näe tietokoneesi tai mobiililaitteesi näyttöä tai näppäimistöä.**
- Työtiedostot tallennetaan ensisijaisesti Teamsiin/Sharepointiin, koska Microsoft pilvipalvelut varmistetaan keskitetysti. Lisätietoja tiedostojen käsittelystä ja niiden tallentamisesta löytyy Väylästä Tiedostonhallinnan pelikirjasta.
- **Vältä turhaa tulostamista ja kopiointia,** koska ylimääräiset kopiot lisäävät väärin käsiin joutumisen riskiä.
- **Varmista, mihin tulostimeen tulostat ja missä tulostin sijaitsee.** Hae tulosteesi verkkotulostimesta heti tulostuksen jälkeen ja käytä turvatulostusta aina, mikäli mahdollista.
- Laita hävitettäväksi tarkoitettu salassa pidettävä/arkaluonteinen aineisto lukittuun tietoturvalaatikkoon tai käytä tiedon hävittämiseen suojausvaatimusten mukaista ristiin leikkaavaa silppuria.
- Mikäli joudut lähettämään salassa pidettävää aineistoa sähköpostilla, **käytä lähettämiseen turvapostia (salattua sähköpostia) ja varmistu, että vastaanottaja on oikeutettu vastaanottamaan lähetyksen ja että lähetys on mennyt perille. Henkilötietoja, käyttäjätunnuksia, salasanoja, ip -osoitteita ym. salassa pidettäviä tietoja ei saa lähettää sähköpostitse muutoin kuin turvapostin kautta.** Microsoft Outlookissa oleva sähköpostin salaustoiminnallisuus on riittävä organisaation sisällä lähetettävien viestien osalta, ja osa muistakin organisaatioista hyväksyy Microsoftin salauksen riittävänä tapana salata sähköpostit. Tieran Turvapostin suojausominaisuudet mahdollistavat viestien turvallisen lähettämisen mihin tahansa sähköpostiosoitteeseen sekä vastausviestin vastaanottamisen luottamuksellisesti. Molempien salaustoimintojen käyttämiseen löytyy tarkat ohjeet intranetistä, järjestelmien käyttöohjeista.
- **Huolehdi, että kannettava tietokone tai mobiililaitte ei jää ilman valvontaa.** Säilytä laitteita lukitussa tilassa silloin, kun ne eivät ole mukana. Muista myös tallennusvälineiden, paperitulosteiden ym. asianmukainen säilyttäminen.
- Noudata "Puhtaan pöydän –periaatetta". **Työpöydällä ei saa säilyttää salassa pidettävää tietoa** (koskee myös käyttäjätunnuksia ja salasanoja).
- **Älä jätä vierasta ilman valvontaa työhuoneeseesi tai muihin toimitiloihin.** Asiakaspalvelupisteessä tietokoneen näyttö ei saa näkyä asiakkaalle. Käytä tarvittaessa näytölle asennettavaa tietosuojakalvoa.
- **Tietovarastojen tietoja, joihin sinulla on käyttöoikeudet, saat käyttää vain työ-/virkatehtäviin.** Henkilörekisterin tietojen käyttötarkoituksen vastainen käyttö on lainvastaista.
- **Palvelussuhteen aikana ja sen päätyttyä sivulliselle ei saa ilmaista työn vuoksi tietoon saatuja** (esim. asiakkaita tai muita yhteistyötahoja koskevia) salassa pidettäviä tietoja. Tällaisia ovat myös mm. liike- ja ammattisalaisuudet sekä arkaluonteiset henkilötiedot ellei julkisuuslainsäädännössä toisin määrätä.

12 Tietokoneen ja mobiililaitteiden käyttö

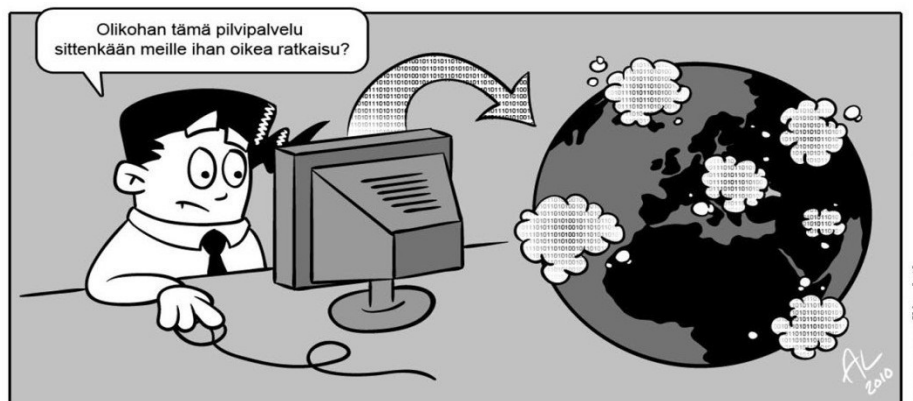
Tietokoneen käyttö sisältää sekä oman työaseman että verkon kautta käytettävien palveluiden käytön. Vastaa käyttäjänä omasta koneestasi. Ole siis huolellinen.

- **Kirjautu tietokoneelle aina omilla käyttäjätunnuksillasi. Käyttäjätunnukset ja salasanat ovat henkilökohtaisia, eikä niitä saa luovuttaa toisen henkilön käyttöön.**
- **Vaihda salasanat riittävän usein ja heti, kun epäilet niiden paljastuneen.**

- Käytä **aina vahvaa salasanaa**. Vahva salasana on riittävän monimutkainen (sisältää vähintään 8 merkkiä, joista vähintään yksi on iso kirjain ja yksi numero). Vältä tuttuja ja jokapäiväisten nimien käyttöä. **Älä käytä samaa salasanaa henkilökohtaiseen ja työkäyttöön.**
- **Työnantajan työntekijälle luovuttama tietokone ja mobiililaitte ovat ensisijaiset sallitut laitteet työkäyttöä varten.**
- **Estä asiaton pääsy tietojärjestelmiin lukitsemalla tietokoneesi aina Ctrl+Alt+Del –näppäinyhdistelmällä, kun poistut työhuoneestasi.**
- **Mobiililaitteiden suojaamiseen tulee käyttää näytön lukitsemiseen tarkoitettua PIN-koodia (eri kuin SIM-kortin PIN-koodi) ja/tai biometristä tunnistetta (kasvokuva ja/tai sormenjälki). Lukitse mobiililaitteesi näyttö aina, kun et käytä laitetta.** SIM-kortin PIN-koodi pitää olla eri kuin oletus-PIN-koodi (0000).
- **Muista kirjautua ulos sekä ohjelmistoista että koneeltasi työskentelyn päätyttyä.** Jos käytät julkisia tietokoneita, yhteiskäytössä olevaa tai toisen henkilön tietokonetta, muista aina uloskirjautuminen sekä ohjelmistoista että koneelta.
- **Jos kiintolevy tai muu tallennusväline rikkoutuu tai poistetaan muuten käytöstä, sitä ei saa laittaa roskakoriin, vaan se täytyy toimittaa tietohallintoon, joka vastaa sen asianmukaisesta hävittämisestä ja huolehtii, että tietoaineisto ei paljastu ulkopuolisille.**
- **Älä käytä tai asenna työ koneellesi ohjelmia, lukuun ottamatta Windows-päivityksiä, selainten- ja niiden lisäosien päivityksiä sekä Adobe Readerin päivityksiä.** Jos olet epävarma päivitysten suhteen, ota yhteys tietohallintoon.
- **Työpaikalla tietokone on työvälineesi. Käytä sitä työtehtävien suorittamiseen. Älä tallenna sinne tarpeettomasti henkilökohtaisia tiedostoja.**

13 Internet, pilvipalvelut, sosiaalinen media ja sähköposti

- **Internet, pilvipalvelut (OneDrive) ja sähköposti on työpaikalla tarkoitettu työkäyttöön.** Suosittelemme käyttämään henkilökohtaiseen viestintään muuta sähköpostia. Työnantaja ei ole vastuussa henkilökohtaisista viesteistä työsähköpostissa.
- **Internetin kautta ei ole luvallista välittää salassa pidettävää tietoa ilman asianmukaista salausta.** Ne on salattava tietohallinnon hyväksymillä tuotteilla ennen niiden lähettämistä julkisen tietoverkon kautta (esim. salattu sähköposti).
- **Älä tallenna tai jaa työtietoja henkilökohtaisessa käytössäsi olevien pilvipalveluiden kautta.** Lue tarkemmat ohjeistukset Tiedostonhallinnan pelikirjasta.
- **Jos käytät muuta kuin omaa työtietokonetta muista tyhjentää Internet-selaimen välimuisti ja evästeet**



© Grafiant / Antti Laitinen 2010

- **Työhön liittyvä sähköposti vastaanotetaan ja ohjataan oman organisaation sähköpostijärjestelmään.** Työsähköpostia ei saa uudelleenohjata organisaation sähköpostijärjestelmän ulkopuolelle, esim. henkilökohtaiselle Gmail-tilille.
- **Muiden kuin työsähköpostin (tornio.fi) käyttö työkäyttöön ei ole sallittua.** Näihin kuuluvat esimerkiksi ilmaissähköpostiohjelmat tai muut henkilökohtaiset sähköpostiohjelmat. Huom, perusopetuksen ja lukiokoulutuksen henkilökunnan käytössä oleva edutornio.net -tunnus ei ole tarkoitettu sähköpostikäyttöön.
- **Huolehdi sähköpostisi käsittelystä poissaolon aikana työtehtäviesi mukaisesti.** Muista laittaa sähköpostiin automaattinen poissaoloilmoitus, jos et poissa ollessasi lue sähköposteja.

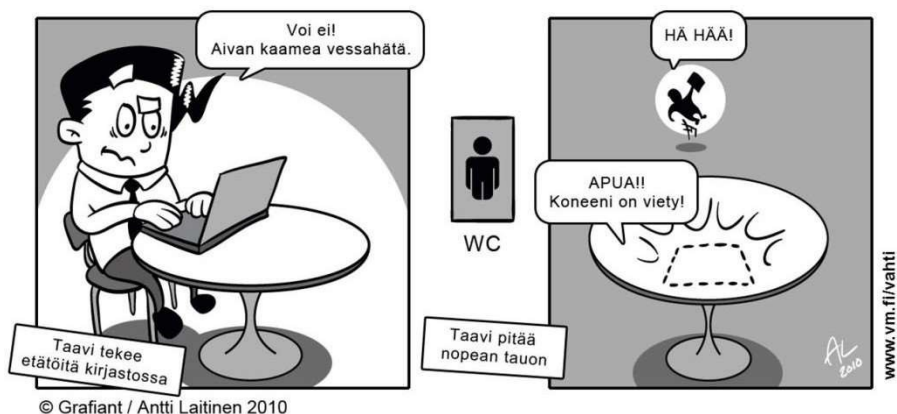
- **Varo kaikkia epätavallisia sähköposteja, erityisesti liitetiedostoja ja älä avaa sähköpostitse tulevia linkkejä ilman tarkistusta** (vie hiiri linkin päälle ja näet linkin osoitteen). Liitetiedostot voivat sisältää haittaohjelmia (viruksia, matoja tai troijalaisia) ja linkit ohjata internetsivuille, josta voi asentua haittaohjelma koneellesi. Älä avaa epäilyttäviä viestejä, vaan ilmoita asiasta tietohallinnolle.
- **Sosiaalisen median** (esim. Facebook, Instagram ja WhatsApp) käyttöönotto tulee tehdä Tornion kaupungin viestintäohjeiden mukaisesti.
- Roskapostia ovat mm. kaikki sähköpostiin tilaamatta tulleet mainokset. **Roskapostiin ei tule kannata vastata, vaan se tulee tuhota heti tai merkitä roskapostiksi sähköpostiohjelmassa olevalla toiminnolla.** Sähköpostin roskapostisuodatin oppii tunnistamaan ei-toivotut lähettäjät ja ohjaa ne jatkossa suoraan Roskaposti -kansioon. Roskapostia voi välttää siten, että ei anna työsähköpostiosoitteaan esim. kyselyihin, uutiskirjeisiin, arvontalomakkeisiin yms.
- **Ole terveen epäluuloinen sähköpostin luotettavuuteen.** Kuka tahansa voi lähettää toisen nimissä sähköpostia. Myös haittaohjelmat voivat lähettää sähköpostia ilman käyttäjän toimenpiteitä.
- **Huolehdi, että lähettämäsi sähköposti on kohdistettu oikeille henkilöille ja oikeisiin osoitteisiin.** Vältä turhien sähköpostien lähettämistä (esim. ketjukirjeet).
- **Mikäli saat vahingossa toiselle henkilölle kuuluvan sähköpostin, ohjaa viesti oikealle vastaanottajalle ja ilmoita lähettäjälle vastaanottajan oikea sähköpostiosoite (työsähköpostiosoite).** Mikäli oikea osoite ei ole tiedossa, ilmoita virheellisestä lähetyksestä lähettäjälle. Muista, että sinulla on vaitiolovelvollisuus saamastasi viestistä. **Mikäli sähköpostiviesti sisältää henkilötietoja, ilmoita asiasta välittömästi tietosuoja- vastaavalle.**
- **Käytä ryhmäviesteissä piilokopiotoimintoa, jos käytät henkilön yksityistä sähköpostiosoitetta eikä sinulla ole lupaa osoitteen julkaisemiseen/luovuttamiseen.** Sähköpostin jakelulista sisältää henkilötietoja, jonka jokainen vastaanottaja saa tietoonsa, mikäli ei käytetä piilokopiotoimintoa. Se voi olla salassa pidettävä tieto, joiden luovuttamisesta on erikseen säädetty.

14 Etäkäyttö ja etätyö

Etäkäytöstä on kysymys silloin, kun käytät organisaation tietoverkkoa tai sen osaa tietoliikenneyhteyden avulla organisaation ulkopuolelta. Etätyöllä tarkoitetaan muualla kuin viraston vakituksessa toimipisteessä tehtävää työtä.

Etä- käyttö ja etätyö on sallittua vain, jos siitä on sovittu erikseen.

- **Muista, että kaikkea toimistossa tehtävää työtä ei voida tehdä tietoturvallisesti etätyönä.**
- Työnantaja hoitaa etäkäytössä vaadittavien laitteiden, ohjelmistojen ja tietoliikenneyhteyksien hankinnan ja asentamisen.
- Käyttäessäsi etäyhteyttä olet osa organisaation tietoverkkoa ja näin ollen tietojen käsittelyssä tulee ottaa samat asiat huomioon kuin ollessasi varsinaisissa toimitiloissa.
- **Huolehdi, että etätyössä käyttämäsi laitteistot, ohjelmistot, tietoliikenneyhteydet ja paperiaineistot ovat vain sinun käytössäsi.**
- **Huolehdi, että käyttämäsi käyttäjätunnukset, salasanat ja mahdolliset toimikortit ja muut todennusvälineet ovat vain sinun hallussasi ja tiedossasi.**



15 Omat tiedot ja yksityisyys

- **Omia henkilökohtaisia tiedostoja ei saa tarpeettomasti tallentaa työasemalle tai pilvipalveluihin. Henkilökohtaisten tiedostojen poistamisesta ja siirtämisestä on työntekijän huolehdittava itse ennen työsuhteen päättymistä.** Työasema on työnantajan omaisuutta ja työsuhteen päättyessä se luovutetaan tietohallinnolle, joka säilyttää sitä yhden kuukauden, ja sen jälkeen kiintolevy tyhjenetään ja/tai tuhotaan.
- **Henkilökohtaisessa OneDrive -tallennustilassa olevien tiedostojen luovuttaminen esim. seuraajan käyttöön edellyttää työntekijän antamaa kirjallista lupaa.** Lupa toimitetaan tietohallinnolle ja siinä täytyy olla työntekijän allekirjoitus. Lupaa ei tarvita, jos on varmistettu, että henkilökohtaiset tiedostot on poistettu tai työtiedostot on siirretty ennen työsuhteen päättymistä palveluyksikön yhteiseen pilvitallennustilaan.
- **Käyttäjä vastaa itse vastaanottamiensa henkilökohtaisten viestien käsittelystä työ sähköpostissa. Siirrä tai poista henkilökohtaiset viestisi sähköpostistasi ennen työsuhteen päättymistä.** Työsuhteen päättyessä sähköposti poistetaan käytöstä välittömästi. Mikäli se joudutaan jostain syystä palauttamaan, se voidaan tehdä tietohallintopalveluiden toimesta.
- Ennen työsuhteen päättymistä, poista SIM-korttien ja mobiililaitteesi PIN-koodit ja palauta laite tehdasasetuksille.
- Järjestelmiin ja tietoverkon laitteisiin tallentuu yksityiskohtaista lokitietoa järjestelmien käytöstä. Tietoja voidaan käyttää ylläpidossa, vianmäärityksessä ja tietoturvallisuuden valvonnassa sekä tietosuoja-asetuksen mukaisten rekisteröidyn oikeuksiin liittyvien tehtävien hoitamisessa.

16 Ilmoitusvelvollisuus

- **Ilmoita aina havaitsemiasi haittaohjelmista (virukset, madot tai troijalaiset) välittömästi tietohallintoon.** Ilmoita aina tietosuojavastaavalle, mikäli havaitset väärinkäytöksiä, laiminlyöntejä tai mitä tahansa puutteita tietosuojaan tai tietoturvaan liittyvissä asioissa.
- **Työsuhteen päättyessä käyttöoikeudet tietojärjestelmiin poistetaan.** Esihenkilön tulee ilmoittaa työsuhteen päättymisestä tietohallinnolle hyvissä ajoin.

17 Salassapitovelvollisuus

- **Keskeiset salassapitoperusteet on lueteltu julkisuuslain 24 §:ssä.** Salassapitosäännöksiä sisältyy kuitenkin myös erityislainsäädäntöön. Esim. asiakkaiden ja yhteistyökumppaneiden henkilötiedot ovat salassa pidettäviä. Salassapitovelvollisuus säilyy työsuhteen päättymisen jälkeenkin.
- **Rekisterien katselu- tai käyttöoikeutta ei ole muihin kuin työtehtävien edellyttämiin tietoihin** esimerkiksi omiin eikä lähiomaisten henkilötietoihin ja lokitietoihin ilman tarvittavaa lupaa.
- **Salassa pidettävästä** viranomaisen asiakirjasta tai sen sisällöstä **saa antaa tiedon vain julkisuuslaissa säädetyin perustein.**



Tietoturvallista työskentelyä edistämässä



© Antti Laitinen / Grafiant 2012 - www.grafiant.com

18 Tietoturva- ja tietosuojaohjeen soveltaminen, ylläpito ja uusiminen

Tietoturva- ja tietosuojaohjeen hyväksyy kaupunginhallitus. Sen soveltamisesta, ylläpitämisestä ja muutoksista vastaa digityöryhmä.

18.1 Tietosuoja- ja tietoturvakoulutus

Vakituisen ja määräaikaisen henkilöstön tulee suorittaa vuosittain kaikille yhteinen Navisec tietoturva- ja tietosuoja-verkkokoulutus. Kaikille yhteinen kurssi koulutuksessa on Henkilöstön tietoturva ja tietosuoja; lisäksi opetustoimen henkilöstö suorittaa kurssin Opetustoimen tietoturva ja tietosuoja; varhaiskasvatuksen henkilöstö suorittaa kurssin Varhaiskasvatuksen tietoturva ja tietosuoja.

Verkkokoulutukseen kirjaudutaan omilla henkilökohtaisilla etunimi.sukunimi@tornio.fi tunnuksilla. Älä käytä työyhteisösi yhteistä sähköpostitunnusta!

18.2 Häiriötilanteissa toimi näin

Tornion kaupunki osallistuu vuosittain Digi- ja väestötietoviraston järjestämiin valtakunnallisiin TAISTO-harjoituksiin, joista saatujen oppien pohjalta on muotoiltu käytännön toimintaohje häiriötilanteiden hallintaa varten.



TAISTO-harjoituksesta laadittu ohje

Tietosuoja ja tietoturva

28.2.2023

Muokattu 20.10.2023

Toimintaohjeet erilaisissa häiriötilanteissa

Tapahtuma	Toimenpide
Kyberturvallisuusrikos esim. epäily sähköpostitilin kaappauksesta tai muu tietoverkkoihin tai järjestelmiin kohdistuva rikos	Ilmoita välittömästi Helpdeskiin numeroon 016 432 400
Palvelunestohyökkäys esim. jokin Tornion kaupungin verkkosivu tai muu kaupungin käytössä oleva järjestelmä (esim. Wilma) ei toimi tai se on poikkeuksellisen hidas	Ilmoita häiriöstä Helpdeskiin numeroon 016 432 400
Sähkökatkos, ennakoimaton	Ilmoita sähkökatkosta omalle esihenkilöllesi. Sopikaa yhdessä toimenpiteistä.
Sähköpostihijaus tai tietojenkalastelu esim. epäilyttävä sähköpostiviesti, joka sisältää liitetiedoston, linkin tai kehotuksen kirjautua M365-tunnuksilla	-Älä avaa liitetiedostoa tai linkkiä -Ilmoita epäilystäsi Helpdeskiin osoitteeseen helpdesk@tornio.fi -Jos ehdit antaa M365-tunnuksesi vaihda salasanasasi välittömästi (Paina näppäinyhdistelmää CTRL+ALT+DEL ja valitse valikosta vaihda salasana) -Jos avasit linkin tai liitetiedoston, soita välittömästi numeroon 016 432 400
Tietoturvaloukkaus esim. epäily henkilötietojen kuten henkilötunnuksen joutumisesta väärin käsiin	Ilmoita välittömästi osoitteeseen tietoturva@tornio.fi tai sähköisellä lomakkeella: Ilmoitus tietoturvaloukkauksesta
Tietovuoto, julkinen esim. asiakkaiden tai henkilöstön henkilötietoja tai muita salassa pidettäviä tietoja on julkisesti saatavilla internetissä	Ilmoita välittömästi osoitteeseen tietoturva@tornio.fi tai sähköisellä lomakkeella: Ilmoitus tietoturvaloukkauksesta
Tietovuoto, sisäinen esim. salassa pidettäviä tietoja liikkuu sähköpostitse salaamattomana tai väärälle vastaanottajalle tai niitä on julkaistu intranetissä	Ilmoita välittömästi osoitteeseen tietoturva@tornio.fi tai sähköisellä lomakkeella: Ilmoitus tietoturvaloukkauksesta
Uhkaus esim. kasvatusten, sähköpostitse, puhelimitse tai muuta kautta	Tilanteen kiireellisyydestä ja vakavuudesta riippuen 1. Jos on hätä, soita hätänumeroon 112. 2. Muussa tapauksessa ilmoita esihenkilöllesi ja sopikaa yhdessä toimenpiteistä.

Lainsäädäntöä ja ohjeistuksia

Navisec tietoturva ja tietosuojakoulutus:

<https://luotsi.navisec.fi/tornio/>

Tietosuoja-asetus:

<https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016R0679>

Tietosuojalaki:

<https://www.finlex.fi/fi/laki/alkup/2018/20181050>

IT-hankintojen sopimusehdot:

<https://julkaisut.valtioneuvosto.fi/items/8bb627f5-37d8-4bff-bdd3-2d84114f5096>

Kuntaliiton ohjeistus tietosuoja-asetuksen huomioimisesta julkisten hankintojen kilpailutuksessa:

https://www.hansel.fi/media/filer_public/1d/2c/1d2c32ab-bb9a-49c0-b75c-da64871d1df9/tietosuojaohje.pdf

Laki sähköisen viestinnän palveluista:

<https://www.finlex.fi/fi/laki/ajantasa/2014/20140917>

Laki yksityisyyden suojasta työelämässä:

<https://www.finlex.fi/fi/laki/ajantasa/2004/20040759>

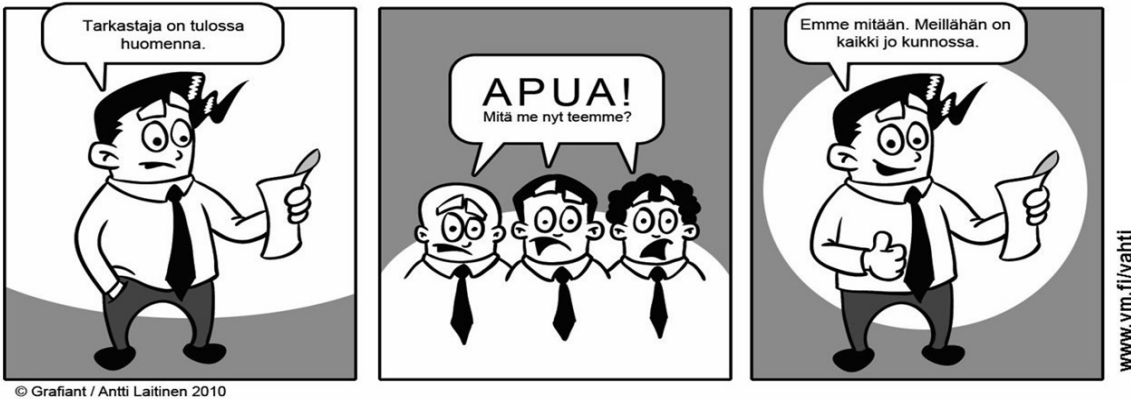
Viranomaistoiminnan julkisuudesta annettu laki ja asetus:

www.finlex.fi/fi/laki/ajantasa/1999/19990621

www.finlex.fi/fi/laki/ajantasa/1999/19991030

Laki julkisen hallinnon tiedonhallinnasta:

<https://www.finlex.fi/fi/laki/alkup/2019/20190906>



Liitteet

LIITE 1

Miten käsittelemme henkilötietojasi Tornion kaupunginrekisterissä? (*rekisterin nimi*)

Toimimme kaikessa henkilötietojen käsittelyssä EU:n yleisen tietosuoja-asetuksen (GDPR) mukaisesti.

1. **Rekisterinpitäjä (nimi, osoite, puhelinnumero, sähköpostiosoite)**
2. **Rekisterin vastuuhenkilö (nimike)**
3. **Yhteyshenkilö rekisteriä koskevissa asioissa (nimike, osoite, puhelinnumero, sähköposti-osoitteeksi kirjaamo@tornio.fi)**
4. **Tietosuoja-asetuksen mukainen tietosuojavastaava ja yhteystiedot**

Kaupungin tietosuojavastaava
Suensaarenkatu 4, 95400 Tornio
+358 (0)40 523 1179
tietoturva@tornio.fi

5. **Henkilötietojen käsittelyn tarkoitus ja käsittelyn oikeusperuste**
6. **Rekisterin tietosisältö (Henkilötietoryhmät art. 14)**
7. **Mistä henkilötiedot on saatu? (Art. 14)**
8. **Henkilötietojen säilytysajan määrittämiskriteerit**
Tietojen säilyttämisessä ja poistamisessa noudatetaan kunnan arkistonmuodostussuunnitelmaa / tiedonohjaussuunnitelmaa, lainsäädännön velvoittamia tietojen säilytysaikoja sekä kansallisarkiston määräyksiä ja kuntaliiton suosituksia.
9. **Henkilötietojen vastaanottajat tai vastaanottajaryhmät (esim. viranomaiset, erilaiset alihankkijat, tietojärjestelmän ylläpitäjät ym. rekisterinpitäjän lukuun henkilötietoja käsittelevä)**
10. **Henkilötietojen luovutukset ja siirrot Euroopan Unionin tai Euroopan Talousalueen ulko- puolelle ja tiedot käytettävistä suojaustoimista.**
11. **Rekisteröidyn oikeudet**

Rekisteröidyllä on oikeus saada tarkistaa rekisterissä olevat tietonsa sekä oikeus pyytää kyseisten tietojen oikaisemista tai poistamista taikka käsittelyn rajoittamista tai vastustaa käsittelyä sekä oikeutta siirtää tiedot järjestelmästä toiseen. Näistä ja muista rekisteröidyn oikeuksista on säädetty tietosuoja-asetuksen artikloissa 13-22 ja 34. Tietojen poistamisoikeutta ei kuitenkaan ole niissä tapauksissa, kun henkilötietojen käsittely on tarpeellista lakisääteisen veloitteen noudattamiseksi tai kunnalle kuuluvan julkisen vallan käyttämistä varten.

Pyyntö käyttää oikeutta tehdään rekisteriasioita hoitavalle yhteyshenkilölle tai tietosuojavastaavalle kaupungin kotisivuilta löytyvällä lomakkeella tai täyttämällä lomake rekisteriasioita hoitavan yhteys-henkilön, tai tietosuojavastaavan luona.

Rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle, jos rekisterinpitäjä kieltäytyy pyynnöstä, eikä kieltäytymiselle ole rekisteröidyn mielestä perusteita.

Tietosuoja-asetuksen mukaisista suoritteista ja niihin liittyvistä toimenpiteistä ei peritä maksua. Maksu voidaan kuitenkin periä edellä mainituissa tilanteissa, mikäli rekisteröidyn pyynnössä esitetyt vaatimukset ovat ilmeisen perusteettomia tai kohtuuttomia, ja erityisesti jos pyyntöjä esitetään toistuvasti. Tällaisissa tilanteissa rekisterinpitäjä voi myös kieltäytyä suorittamasta pyydettyjä toimenpiteitä. Mikäli pyydetty toimenpiteet päätetään suorittaa, peritään niistä maksua Tornion kaupungin asiakirjahinnaston mukaisesti.

Euroopan unionin yleisen tietosuoja-asetuksen 15 artiklan 3 kohdan mukaisesti rekisteröidyllä on oikeus saada rekisterinpitäjältä maksutta jäljennös käsitellyistä rekisteröidyn henkilötiedoista. Mikäli rekisteröity kuitenkin pyytää useampaa tällaista jäljennöstä, voi rekisterinpitäjä periä niistä hallinnollisiin kustannuksiin perustuvan maksun.

