KUSTAVIN KUNNAN
TIETOTILINPÄÄTÖS
2022

Sisällys

1 Johdanto

Tämä on Kustavin kunnan ensimmäinen tietotilinpäätös. Kunnan tietopääoman hyödyntäminen on koko ajan tärkeämpää, jotta voidaan tuottaa kansalaisille palvelut turvallisesti ja oikea-aikaisesti. Palvelut pitää pystyä toteuttamaan entistä kustannustehokkaammin ja nopeammin, mutta asioinnin turvallisuudesta ei saa tinkiä. Kansalaisten tulee voida luottaa siihen, että heidän henkilötietojaan käsitellään luottamuksellisesti ja digitaalinen turvallisuus oletusarvoisesti huomioiden.

Tietotilinpäätöksen tavoitteena on lisätä avoimuutta ja luottamusta siihen, että organisaatiossa noudatetaan organisaation luomia tietoturva- ja tietosuojaperiaatteita ja käsitellään henkilötietoja niiden mukaisesti.

Tietotilinpäätös kuvaa tietojen käsittelyn nykytilaa sekä arvioi tietosuojan ja tietoturvan toteutumista. Lisäksi se sisältää tietosuojaan ja tietoturvaan liittyviä kehittämistarpeita ja toimenpiteitä.

Tietotilinpäätöksen koonnista vastaa kunnan tietosuojavastaava yhdessä kunnanjohtajan kanssa.

Kunta julkaisee vuosittain tietotilinpäätöksen, jonka kunnanhallitus hyväksyy.

Tietosuojasääntely koostuu tietosuoja-asetuksesta, kansallisesta tietosuojalaista sekä erityislainsäädännöstä. Suomessa tietosuojavaltuutetun toimisto valvoo tietosuojalainsäädännön noudattamista. Tietosuoja-asetuksessa (GDPR) on keskeisenä teemana tietosuojariskien hallinta ja rekisterinpitäjän tilintekokykyisyys-periaate. Osoitusvelvollisuuteen kuuluu mm. se, että organisaation sopimuksissa ja alihankinnoissa on huomioitu tietosuojan ja -turvan vaatimukset. Lisäksi rekisterinpitäjän tulee huomioida rekisteröidyn henkilötietojen käsittelyyn kohdistuvat riskit.

Tietotilinpäätös esitellään kunnanhallitukselle 27.3.2023.

Tietosuojapolitiikan soveltaminen ja tavoitteet

Tietosuojaan kuuluvat henkilöiden yksityiselämän suoja ja yksityisyyden suojaa turvaavat muut oikeudet henkilötietoja käsiteltäessä.

Suojaamistoimet koskevat kaikkien sähköisessä, kirjallisessa tai muussa muodossa olevien henkilötietojen käsittelyä, siirtoa ja säilytystä riippumatta siitä, onko tietoihin kohdistuva uhka tahallinen tai tahaton, esimerkiksi järjestelmän vikaantuminen, tapaturma tai luonnonkatastrofi.

Kunnan luottamushenkilöt ja henkilökunta ovat sitoutuneet tietosuojan huomioivaan toimintaan ja toimivat tässä asiakirjassa julkaistujen periaatteiden mukaisesti.

Tietosuojapolitiikan avulla pyritään turvaamaan kunnan toiminta lainsäädännön mukaisesti. Tähän kuuluu olennaisesti henkilötietojen käyttöön liittyvät asiakkaiden, työntekijöiden ja muihin sidosryhmiin kuuluvien henkilöiden oikeudet sekä tietojen käsittelijän oikeuksien ja velvollisuuksien varmistaminen ja noudattaminen henkilötietoja käsiteltäessä.

Tietosuojaa toteutettaessa kiinnitetään erityistä huomiota henkilötietojen salassapitoon ja siihen, ettei asiattomilla ole pääsyä tietoihin ja ettei tietoja käytetä henkilöä vahingoittavasti.

Tietosuojalla on kiinteä yhteys tietoturvaan. Kunnan tietoturvapolitiikka määrittelee, mitä tarkoitetaan tietoturvalla ja kuinka sitä ylläpidetään.

2 Tietojen käsittelyyn vaikuttava lainsäädäntö

2.1 Tietosuojaa määritelevä keskeinen lainsäädäntö

- Kuntalaki (410/2015)
- Hallintolaki (434/2003)
- EU:n yleinen tietosuoja-asetus EU 679/2016
- Tietosuojalaki 5.12.2018/1050
- Tiedonhallintalaki (906/2019)
- Arkistolaki (831/1994)
- Laki digitaalisten palvelujen tarjoamisesta 306/2019
- Laki sähköisestä asioinnista viranomaistoiminnassa 24.1.2003/13
- Euroopan parlamentin ja neuvoston verkko- ja tietoturvadirektiivi
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621
- Toimialakohtaiset erityislait

2.2 Tietosuojaan liittyvän lainsäädännön keskeiset muutokset

Laki julkisen hallinnon tiedonhallinnasta (906/2019) astui voimaan 1.1.2020.
Yleislakina tiedonhallintalaki sisältää koko julkista hallintoa koskevat säännökset tiedonhallinnan järjestämisestä ja kuvaamisesta, tietovarantojen yhteen toimivuudesta, teknisten rajapintojen ja katseluyhteyksien toteuttamisesta sekä tietoturvallisuuden toteuttamisesta.
Tiedonhallintalain siirtymäsäännösten mukaan kolmas siirtymäaika päättyy 1.1.2023 seuraaville lain kohdille:

- Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen (12§)
- Tietoaineistojen ja tietojärjestelmien tietoturvallisuus (13§)
- Tietojen siirtäminen tietoverkossa (14§)
- Tietoaineistojen turvallisuuden varmistaminen (15§)
- Tietojärjestelmien käyttöoikeuksien hallinta (16§)

3 Keskeiset toimenpiteet ja muutokset 2022

1. Vastuu sosiaali- ja terveydenhuollon ja pelastustoimen järjestämisestä siirtyi 1.1.2023 Varsinais-Suomen hyvinvointialueelle (Varha). Siirron myötä Kustavin kunnalta poistui 11 henkilörekisteriä. Tietosuojakäsikirja, tiedonhallintamalli, asiakirjajulkisuuskuvaus ja kunnan kotisivut päivitettiin näiden osalta.

2. Ei muita keskeisiä muutoksia tietoturvan tai tietosuojan osalta 2022.

4 Rekisteröityjen oikeuksien toteutuminen

Rekisteröityjä informoidaan henkilötietojen käsittelystä kunnan internet sivuilla olevilla tietosuojaselosteilla.
Rekisteröity voi käyttää oikeuksiaan toimittamalla pyynnön rekisterinpitäjälle ensisijaisesti sähköisellä tietojenpyyntölomakkeella tai vapaamuotoisella kirjeellä.
Tietosuojaselosteet ja tietopyyntölomakkeet löytyvät osoitteesta:
https://kustavi.fi/kunta-ja-hallinto/tietosuoja/asiakkaan-oikeudet/

Tietopyynnön voi toimittaa joko
1) kunnan sivuilla olevan sähköisenlomakkeen kautta tai
2) asioimalla henkilökohtaisesti, jonka yhteydessä tarkistetaan rekisteröidyn henkilöllisyys.

Asiakas voi tulla noutamaan pyytämänsä tiedot kunnan virastolta. Tiedot voidaan toimittaa hänelle myös postitse.

Kuntaan saapuneiden tietopyyntöjen määrä 1.1.2022 – 31.12.2022 välisenä aikana.
Kaikki toimialat
- tietosuoja-asetuksen mukaiset tietopyynnöt yhteensä: 0 kpl
- julkisuuslain mukaiset tietopyynnöt 1 kpl

5 Rekisterinpitäjän vastuut ja velvoitteet

5.1.1 Osoitusvelvollisuus

Tietosuoja-asetus velvoittaa kuntaa osoittamaan noudattavansa tietosuoja-asetusta esimerkiksi dokumentoimalla henkilötietojen käsittelyyn liittyvät prosessit ja muut käytännön tietosuojatoimenpiteet. Osoitusvelvollisuus merkitsee käytännössä sitä, että vain riittävällä ja asianmukaisella dokumentaatiolla ja koulutuksella kunta voi osoittaa toimivansa asetuksen mukaisesti.

5.1.2 Käsittelyn oikeusperusta

Rekisterinpitäjän tulee huolehtia, että henkilötietoja käsitellään vain asianmukaisin edellytyksin ja määritellä ne tarkoitukset, joihin henkilötietoja käsitellään ja varmistua, ettei tietoja käsitellä muihin tarkoituksiin.
Asetuksen mukaan lainmukaisia käsittelyn edellytyksiä ovat muun muassa:
- Rekisteröidyn vapaaehtoinen ja informoitu suostumus. Rekisterinpitäjän velvollisuuksiin kuuluu pystyä osoittamaan jälkikäteen, että suostumus on annettu.
- Sellaisen sopimuksen täytäntöön paneminen, jossa rekisteröity on osapuolena.
- Rekisterinpitäjän lakisääteinen velvoite.

5.1.3 Tietosuojavastaava

Kunnalla on nimetty tietosuojavastaava, jonka tehtävänkuvaan kuuluu seurata organisaation tietojenkäsittelyyn liittyviä toimintatapoja ja huolehtia, että ne vastaavat asetuksessa tai muualla erityislainsäädännössä säädettyä. Hän myös ohjaa ja auttaa organisaatiota tietosuojaperiaatteiden ja vaatimusten toteuttamisessa. Lisäksi tietosuojavastaava toimii kontaktipisteenä sekä valvontaviranomaiseen että rekisteröityihin.

5.1.4 Sisäänrakennettu ja oletusarvoinen tietosuoja

Tietosuoja-asetuksen vaatimusten toteutuminen tulee taata määrittelyvaiheesta koko käsiteltävien henkilötietojen elinkaaren ajan. Jotta sisäänrakennetun ja oletusarvoisen tietosuojan velvollisuuksista voidaan huolehtia, pitää tietosuojavaatimukset analysoida ja toteuttaa aikaisessa vaiheessa. Käytännössä tämä tarkoittaa tietosuojan sisällyttämistä järjestelmien ja sovellusten hankintoihin sekä projektinhallintaan.

5.1.5 Ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksista

Rekisterinpitäjillä on velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksesta henkilökohtaisesti niille rekisteröidyille, joiden tietoja loukkaus koskettaa. Oikeus astuu voimaan, jos loukkaus todennäköisesti aiheuttaa suuren riskin yksilön oikeuksille ja vapauksille, esimerkiksi identiteetinvarkauksien, maksuvälinepetosten tai muun rikollisen toiminnan muodossa.

6 Kunnan henkilötietorekisterit ja keskeiset tunnusluvut

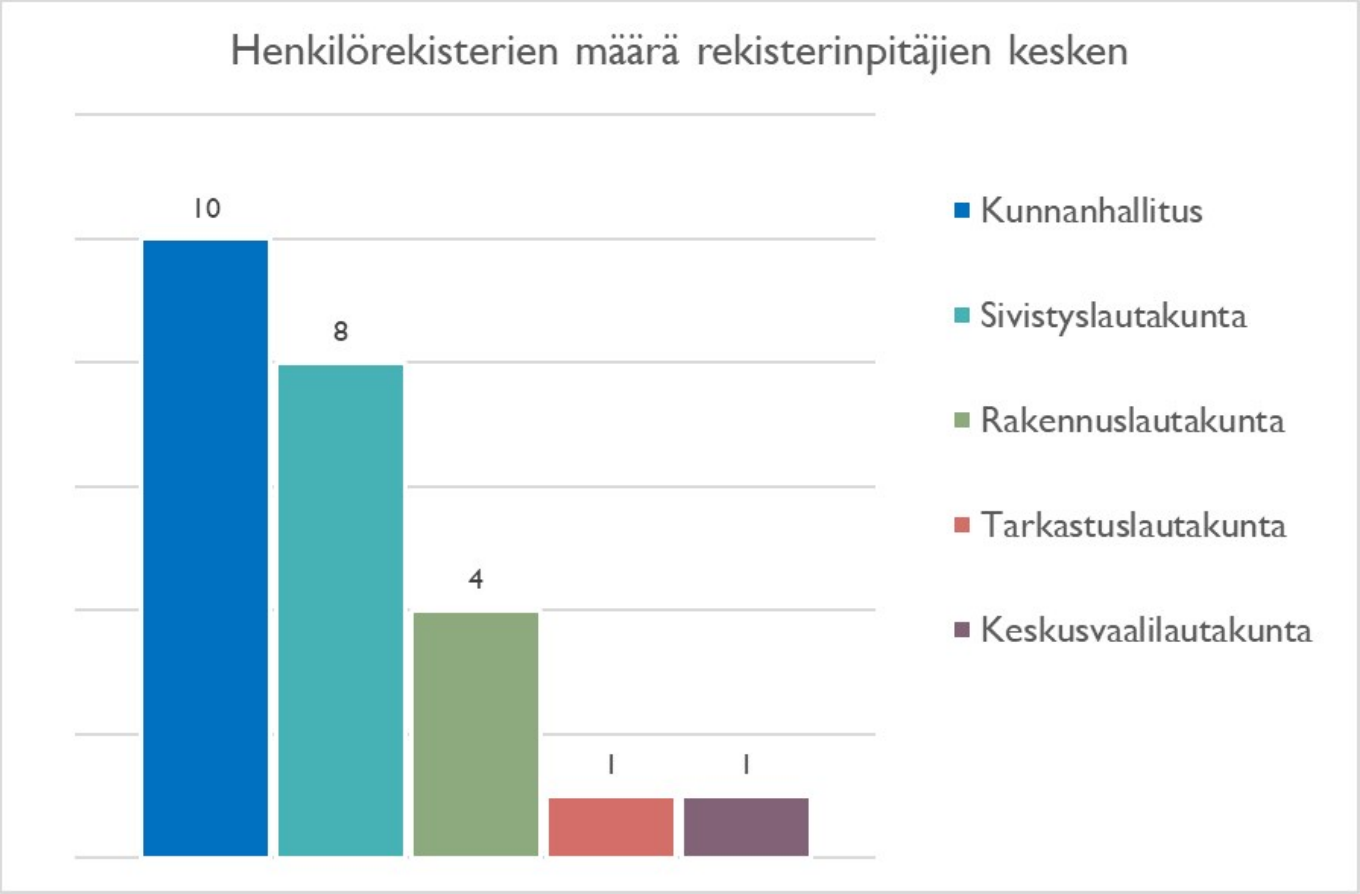
Koko kunnan henkilötietoja sisältävien rekisterien määrä on 24.

Kunnan henkilötietoja sisältävät tietovarannot on jaettu kolmeen eri pääryhmään.

1. Kuntalaisia koskevat lakisääteiset henkilörekisterit
   Tämä ryhmä sisältää isoimman osat rekistereistä (15 kpl) ja kyseisiä rekistereitä on kaikilla kunnan toimialoilla.
2. Kuntalaisia koskevat rekisteröidyn suostumukseen perustuvat henkilörekisterit
   Näitä rekistereistä kunnassa on (4 kpl) ja kyseisiä rekistereitä on usealla kunnan toimialalla.
3. Kunnan henkilökuntaa koskevat rekisterit
   Näitä rekistereistä kunnassa on (5 kpl) ja kyseisiä rekistereitä on usealla kunnan toimialoilla.

6.1 Vastuun jakautuminen kunnassa

Rekisterinpitäjän vastuu henkilörekistereistä jakautuu kunnanhallituksen ja lautakuntien välillä seuraavasti:



7 Tiedon hallinta

Tiedonhallinnalla tarkoitetaan viranomaisen tehtävien hoidossa tai sen muussa toiminnassa syntyviin tarpeisiin perustuvia toimia ja tietoturvallisuustoimenpiteitä viranomaimen tietoaineistojen, niiden käsittelyvaiheiden ja tietoaineistoihin sisältyvien tietojen hallinnoimiseksi riippumatta tietoaineistojen tallentamistavasta ja muista käsittelytavoista. Kustavin kunnassa tiedonhallintaa kuvataan ja ohjataan tiedonhallintalain vaatimusten mukaisella tiedonhallintamallilla, tiedonohjaussuunnitelmalla sekä asiakirjajulkisuuskuvauksella.

7.1 Tiedonhallintamalli ja tiedonohjaussuunnitelma

Tiedonhallintamallissamme kuvataan tiedonhallintayksikön eli Kustavin kunnan toiminta, tietopääoma ja tietojärjestelmät.

Tiedonohjaussuunnitelmassamme kuvaamme kunnan tehtävät ja käsittelyprosessit, tehtävien hoidossa syntyvän asiakirjallisen tiedon ohjaus- ja hallintaperiaatteet sekä tietojen säilytysajat.

Tiedonhallintamallin ja tiedonohjaussuunnitelman ylläpito on jatkuva prosessi, jota päivitetään tehtävien muuttuessa.

7.2 Asiakirjajulkisuuskuvaus

Asiakirjajulkisuuskuvauksemme antaa yleiskuvan tiedonhallinnasta ja siitä, miten ja missä laajuudessa keräämme ja käsittelemme tietoja lakisääteisissä tehtävissämme. Asiakirja julkisuuskuvaus toteuttaa julkisuusperiaatetta. Tavoitteena on auttaa asiakasta kohdistamaan tietopyyntönsä ja yksilöimään tietopyynnön sekä opastaa tietoaineistojen omatoimisessa haussa ja käytössä.
Asiakirjajulkisuuskuvaus on saatavilla https://kustavi.fi/kunta-ja-hallinto/asiakirjajulkisuus/

7.3 Keskeiset tietojärjestelmät

Kunnalla on sekä keskitettyjä koko konsernin tietojärjestelmiä että toimialakohtaisia järjestelmiä, joista keskeisimmät ovat:

- Dynasty 10 – Asianhallintajärjestelmä
- Populus – Henkilöstohallinto
- ProEconomica – Taloushallinto
- Titania – Työajanseuranta
- Microsoft 365 – Toimisto työkalut
- MultiPrimus/Wilma – Oppilastietojen hallintajärjestelmä
- Daisy – Varhaiskasvatuksen hallintajärjestelmä
- Aurora – Kirjaston asiakasjärjestelmä
- Kuntanet7 – Rakennusvalvonta
- Lupapiste – Rakennusvalvonnan lupakäsittely
- Vesikanta plus – Vesihuollon asiakkaat

8 Dokumentaatio ja koulutus

Kunnalla on tietosuojakäsikirja, jota päivitetään säännöllisesti tietosuojavastaavan toimesta. Käsikirja sisältää esimerkiksi kunnan tietosuojapolitiikan, rekisterikuvaukset, kriisiviestinnän ohjeet, tietosuojaselosteet ja tietosuojavastaavan tehtävänkuvan.

Kunnan uudet työntekijät perehdytetään kunnan tietosuojakäytänteisiin koulutuksella. Kunnassa työskenteleville työntekijöille järjestetään tarpeen mukaan lisäkoulutusta.

Yleisen tietosuojakoulutuksen lisäksi Tietosuojavastaava julkaisee henkilöstölle joka toinen viikko ilmestyvän uutiskirjeen kunnan intranetissä.

9 Rekisterinpitäjän ja -käsittelijän väliset sopimukset

Tietosuoja-asetus asettaa velvoitteita sopimusehtojen kannalta, lähtökohdaksi on otettava asetuksen asettama velvollisuus sopia henkilötietojen käsittelystä sopimuksella, kun joku muu (kuten kunnan palveluntuottaja) käsittelee tietoja rekisterinpitäjän (kunta) puolesta. Se kohdistuu sekä rekisterinpitäjään että henkilötietojen käsittelijään. Tietosuoja-asetuksessa säädetään sopimisvelvoitteen lisäksi tietosuojaa koskevan sopimuksen minimisisältö eli ne kohdat, joista ainakin tulee sopia.

Rekisterinpitäjän ja -käsittelijän välisellä sopimuksella (DPA) varmistetaan, että käsittelijä käsittelee henkilötietoja ainoastaan sopimuksessa sovittujen ehtojen mukaisesti.

10 Tietosuojauksen periaatteet

Kustavin kunta suhtautuu asiakkaidensa tietojen suojaamiseen sekä tietoturvaan vakavasti.

Tiedon luottamuksellisuus, virheettömyys ja käytettävyys varmistetaan huolellisella käsittelyllä. Henkilötiedot suojataan asianmukaisia teknisiä ja organisatorisia suojakeinoja käyttämällä. Tällaisia keinoja ovat muun muassa palomuurien, salaustekniikoiden ja turvallisten laitetilojen sekä kulunvalvonnan ja turvallisuusjärjestelmien käyttö. Suojakeinoja ovat lisäksi hallittu käyttöoikeuksien myöntäminen ja seuranta, henkilötietojen käsittelyyn osallistuvan henkilöstön osaamisen varmistaminen sekä alihankkijoiden huolellinen valinta.

Tietosuojan keskeinen ohjausdokumentti on kunnan tietosuojakäsikirja, jossa on kuvattu muun muassa vastuut, tietosuojavastaavan rooli, henkilörekisterit tietosuojaselosteineen, toimintaympäristö, rekisteröidyn oikeuksien toteuttaminen ja rekisterinpitäjän sopimusasiat.

10.1 Suurimmat uhkatekijät

Yleisesti voidaan sanoa, että palvelujen digitalisointi ja pilvipalveluihin siirtyminen on johtanut riippuvuuteen sähköisistä tietojärjestelmistä ja sitä kautta myös tietoturvariskien ja kyberturvariskien korostumiseen. Näistä esimerkkeinä useat kyberiskut eri kuntiin vuoden 2022 aikana.

Erilaiset käyttäjätunnuksien kalastelu viestit pysyivät myös vuoden 2022 yhtenä suurimpana jatkuvana uhkana.

Etätyöskentely on tullut jäädäkseen ja on johtanut siihen, että yhä useampi laite toimii etäyhteyksin ja työntekijä joutuu ottamaan suurempaa vastuuta tietoturvan ja tietosuojan

osalta. Työntekijöiden ohjeistus tietosuojasta ja tietoturvasta huolehtimiseen tulee pysymään tärkeässä roolissa.

Riskien osalta yhtenä haavoittuvuutena on poikkeamat, jotka johtunut inhimillisestä virheestä joko järjestelmäasetuksissa, prosessissa tai yksittäisen henkilön työtehtävissä.

10.2 Tapahtuneet tietoturvaloukkaukset

Vuoden 2022 aikana ei tapahtunut yhtään tietosuojaloukkausta, joka olisi vaatinut raportointia tietosuojavaltuutetun toimistolle.

Vähäisempiä tietosuojaloukkauksia, joista on kirjattu tietosuojarikkomus, ei tapahtunut vuoden 2022 aikana.

11 Kehittämiskohteet ja keskeisimmät muutokset vuonna 2023

-Tiedonhallintalain siirtymäsäännösten mukaan kolmas siirtymäaika päättyy 1.1.2023 seuraaville lain kohdille, näiden toteutusta jatketaan 2023:

- Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen (12§)
- Tietoaineistojen ja tietojärjestelmien tietoturvallisuus (13§)
- Tietojen siirtäminen tietoverkossa (14§)
- Tietoaineistojen turvallisuuden varmistaminen (15§)
- Tietojärjestelmien käyttöoikeuksien hallinta (16§)

-Jatkuvana kehittämiskohteena henkilöstökoulutukset ja tietoisuuden kasvattaminen painopisteenä henkilöstön tietoturva- ja tietosuojatietoisuuden ja osaamisen kasvattaminen.

-Uuden arkistolain vaatimuksien huomioiminen esimerkiksi sähköisessä arkistoinnissa.

-Tiedonhallinnan ja tietosuojan järjestäminen luotettavasti ja lainsäädännön vaatimusten mukaisesti edellyttää jatkossa yhä suurempaa asiantuntijuutta ja tämän vuoksi kunta päätti tietosuojavastaavan tehtävien ulkoistamisesta 1.2.2023 alkaen.