

Henkilötietojen käsittely, Espoon kaupungin keskitetty käyttövaltuuksien hallinta- ja lokirekisteri, Microsoft AD ja Azure AD

1. Rekisterinpitäjä

Espoon kaupunki

etunimi.sukunimi@espoo.fi

2. Rekisterin vastuhenkilö

Tietohallintojohtaja Maarit Waskilampi-Kuikka

3. Rekisterin yhteyshenkilö

Työasemaympäristön päällikkö Juha Valtaharju

PL 670, 02070 ESPOON KAUPUNKI
p. 09 816 21 (vaihde)

4. Tietosuojavastaava

tietosuoja@espoo.fi

5. Mihin tarkoitukseen henkilötietoja käsitellään?

Rekisterin henkilötietojen tarkoituksena on ylläpitää Espoon kaupungin tietoverkon ja liitännäisten palveluiden käyttäjätunnuksia ja käyttöoikeuksia henkilökunnan, luottamushenkilöiden, koulun oppilaiden ja yhteistyökumppaneiden osalta.

Tietojen käsittelyllä varmistetaan tietoturvan toteutuminen ja toiminnan jatkuvuus. Tietojen käsittelyn seurannalla ja valvonnalla varmistetaan tietosuojan toteutuminen, käyttäjäidentiteetin suojaaminen, sekä oppilaiden ja työntekijöiden oikeusturvan toteutuminen. Tietojen perusteella voidaan selvittää virhetilanteita ja valvoa tietojärjestelmien käyttöä

Espoon kaupungin työntekijät ja koulujen oppilaat ovat samassa käyttövaltuuksien hallinta- ja lokirekisterissä. Oppilaan nimi, sähköposti, oppilasnumero ja koulu näkyvät ympäristön käyttäjille hakutoimintoa käytettäessä esimerkiksi Teamsissä ja OneDrivessa. Koko henkilöstö on hyväksynyt tietoturvasitoumuksen ja ympäristön käyttöoikeudet ovat henkilökohtaisia ja salasanalla suojattuja

Rekisterin tietoja käytetään kaupungin toimialueen käyttöoikeuksien hallintaan ja kirjautumiseen useisiin palveluihin kuten intranet, sähköposti ja tiedostopalvelut. Lisäksi tietoja käytetään ongelmatilanteiden selvitykseen, asiakaspalveluun, yhteystietojen hallintaan sekä IT-järjestelmien lokitietojen keräämiseen ja seurantaan.

6. Mikä on henkilötietojen käsittelyperuste?

EU:n yleisen tietosuojasetuksen 6 artiklan 1 c ja e-kohta: käsittely on tarpeen rekisterinpitäjän lakisääteisen veloitteen noudattamiseksi ja käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi.

7. Mitä tietoja käsitellään?

Henkilökunta, luottamushenkilöt, yhteistyökumppanit:

- Käyttäjän nimi
- Ryhmä, joihin henkilö kuuluu
- Toimiala/Yksikkö
- Sähköpostiosoite
- Käyttäjätunnus
- Salasana
- Kryptattu henkilötunnus
- Puhelinnumero (työpaikan matkapuhelin ja/tai pöytäpuhelin)
- Tilin ominaisuustietoja
- Työosoite
- IP-osoite, lokaatitieto

Opetustoimi:

- Henkilön etu- ja sukunimi
- Käyttäjätunnus
- Salattu salasana
- Sähköpostiosoite
- Salattu ainutkertainen tunniste
- Opetusryhmät
- Koulu
- Luokka
- Oppilaitostunnus
- Henkilön roolitietoja: henkilökunta / opiskelija
- IP-osoite, IP-osoitteen mahdollistama lokaatitieto (taso, joka perustuu siis siihen mihin verkon operaattori on verkon rekisteröinyt)

Lokitietoihin tallentuu joitakin tunnistamistietoja (mm. käyttäjätunnus tai sähköpostiosoite) ja henkilötietoja seuraavien palvelujen käytön yhteydessä: viestintäpalvelut, sovellusten ja verkkopalveluiden pääsyvalvonta, verkon pääsynvalvonta ja yhteydet, käyttöjärjestelmä- ja sovelluslokit.

TIETOJEN JULKISUUS JA SALASSAPIDETTÄVYYS:

Rekisteriin sisältyvät tiedot ovat salassa pidettäviä.

SALASSAPIDON PERUSTEET:

Tietojen salassapidosta on viranomaisen toiminnan julkisuudesta annetun lain 24 §:ssä.

8. Mistä tiedot saadaan?

Hallinnon henkilötietojen tietolähde on HR -järjestelmä, jonka avulla kerätään, analysoidaan, muokataan, välitetään ja tallennetaan henkilöstöhallinnon tietoja. Nämä tiedot siirretään palveluntarjoajan konesaleissa olevaan paikalliseen hakemistoon (Active Directory) josta tieto siirretään Azure AD palveluun.

Opetustoimen pääasiallinen tietolähde on Visman Primus kouluhallintojärjestelmä ja siinä olevat henkilökunta-, opettaja- ja opiskelijarekisterit.

Keskitettyyn lokijärjestelmään tallentuu tiedot eri IT-järjestelmien tuottamista lokitiedoista (tietoliikennelaitteet, palvelimet, työasemat, tietojärjestelmät, tietokannat, sovellukset).

9. Luovutetaanko tai siirretäänkö tietoja kaupungin ulkopuolelle?

Henkilötietoja ei säännönmukaisesti luovuteta. Lokitietoja voidaan luovuttaa muille viranomaisille, esimerkiksi poliisille, tietosuojavaltuutetulle tai Kyberturvallisuuskeskukselle tietoturvapoikkeamien ja rikosten selvittelyä varten. Tietyissä tapauksissa palveluntuottajilla on pääsy lokitietoon. Espoon kaupungin paikallisen AD:n tiedot kopioidaan Azure AD pilvipalveluun.

Microsoftin alihankkijat

- Luettelo Microsoftin käyttämistä alihankkijoista:

<https://go.microsoft.com/fwlink/p/?linkid=2096306>

10. Siirretäänkö tietoja EU/ETA-alueen ulkopuolelle?

Henkilötietoja siirretään Euroopan unionin tai Euroopan talousalueen ulkopuolelle (Microsoft online)

Siirtoperuste:

Microsoft Online-palvelujen sopimusehdot ja komission hyväksymät mallisopimuslausekkeet (liitteessä 2) ovat luettavissa Microsoftin internet-sivuilla:

<https://www.microsoftvolumelicensing.com/Downloader.aspx?Documenttype=OST&lang=Finnish>
<https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=18029>

11. Kuinka kauan tietoja säilytetään?

Tietojen säilyttämisessä ja hävittämisessä noudatetaan Espoon kaupungin arkistonmuodostussuunnitelmaa / tiedonohjaussuunnitelmaa sekä arkistolaitoksen kulloinkin voimassa olevia säännöksiä ja määräyksiä.

Henkilötietoja säilytetään paikallisessa hakemistopalvelussa 360 päivää palvelun käytön päättymisestä. Henkilötietoja säilytetään pilvipalvelussa 90 päivää palvelun käytön päättymisestä. Lokitietoja säilytetään vähintään kahden vuoden ajan. Jos käyttäjän toimintaa joudutaan arvioimaan jälkikäteen, ko. tietoja säilytetään selvityksen edellyttämän ajan.

12. Miten tietoja suojataan?

Henkilötietoja käsitellään tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen (tietosuoja-asetus 5 artikla 1 f-kohta). Tietojen käsittelyä sääntelee mm. tietojen käyttötarkoitussidonnaisuus, tarpeellisuusvaatimus, täsmällisyysvaatimus. Jokainen työntekijä voi käsitellä vain niitä henkilötietoja, joita hän tarvitsee työtehtävissään.

Salassa pidettävien ja arkaluonteisten tietojen suojaamiseen kiinnitetään erityistä huomiota mm. työprosessien kuvaamisissa ja käyttöoikeuksien luovutuksissa. Tietojen salassapidosta on säännökset viranomaisen toiminnan julkisuudesta annetun lain 24 §:ssä.

Henkilötiedot on suojattu koulun ja viraston työntekijän tehtävien perusteella määritellyin käyttöoikeuksin. Käyttöoikeus on rajattu tehtävän mukaisesti ja perustuu käyttäjärooleihin, joille on määritely oikeus tehtävänmukaisiin näyttöihin ja toimintoihin. Eri käyttöoikeusryhmissä on määritely erikseen tietojen luku-, kirjoitus-, tallennus- ja poisto-oikeudet. Kaikki verkon käyttäjät hyväksyvät käyttöoikeussitoumuksen, joka sisältää mm. vaitiolositoumuksen. Palvelinlaitteisto on suojatussa ja valvotussa tilassa palveluntuottajan konesalissa. Sähköisesti käsiteltävät tiedot liikkuvat salattuna avoimessa internetissä. Rekisterin tiedot varmuuskopioidaan automaattisesti säännöllisin väliajoin.

Rekisteriä käyttävät keskeiset tietojärjestelmät ja niiden käyttötarkoitus:

- Sovelluskehityksen palvelut
- IT / Infra tukipalvelut
- MS Office365-palveluiden käyttäjätunnusten ja käyttöoikeuksien hallinnointi, salasanojen resetointipalvelu itsepalveluna, päätelaitteiden pääsynhallintapalvelu, federaatio- ja tunnistautumispalvelut, oppilaiden sähköposti ja kalenterijärjestelmä, verkkolevypalvelu, viestintäjärjestelmä, ryhmätyöskentelytila, sekä sosiaalisen median palvelu, että muita oppimista tukevia palveluja.
- Käyttövaltuushallinnan järjestelmä
- Päätelaiteriippumaton laite- ja sovellushallintapalvelu
- Tiedon suojaamispalvelu
- Kuntalaispalvelut

13. Rekisteröidyn oikeudet

Tarkempi ohjeistus tietosuoja-asetuksen mukaisten tietopyyntöjen osoittamisesta:

https://www.espoo.fi/fi-FI/Asioi_verkossa/Tietosuoja/Asiakkaiden_oikeudet

13.1. Miten voin tarkastaa tietoni?

Sinulla on oikeus saada rekisterinpitäjältä jäljennös käsiteltävistä henkilötiedoista. Rekisterinpitäjän on toimitettava tiedot ilman aiheetonta viivytystä ja joka tapauksessa kuukauden kuluessa pyynnön vastaanottamisesta. Määräaikaa voidaan tarvittaessa jatkaa enintään kahdella kuukaudella ottaen huomioon pyyntöjen monimutkaisuus ja määrä.

Jos rekisterinpitäjä ei toteuta toimenpiteitä rekisteröidyn pyynnön perusteella, rekisterinpitäjän on ilmoitettava viipymättä ja viimeistään kuukauden kuluessa pyynnön vastaanottamisesta rekisteröidylle syyt siihen ja kerrottava mahdollisuudesta tehdä valitus valvontaviranomaiselle ja käyttää muita oikeussuojakeinoja.

Rekisteröidyn pyynnöt ja niihin liittyvät toimenpiteet ovat maksuttomia. Kuitenkin jos rekisteröidyn pyynnöt ovat ilmeisen perusteettomia tai kohtuuttomia, erityisesti jos niitä esitetään toistuvasti, rekisterinpitäjä voi joko periä kohtuullisen maksun ottaen huomioon tietojen tai viestien toimittamisesta tai pyydetyn toimenpiteen toteuttamisesta aiheutuvat hallinnolliset kustannukset; tai kieltäytyä suorittamasta pyydettyä toimea.

13.2. Milloin voin vaatia tietojeni oikaisemista?

Sinulla on oikeus saada virheelliset, epätarkat, vaillinaiset, vanhentuneet tai tarpeettomat henkilötiedot, joita säilytämme, korjatuiksi tai täydennetyiksi toimestamme.

13.3. Milloin voin vaatia tietojeni poistamista

Sinulla on oikeus saada rekisterinpitäjä poistamaan sinua koskevat henkilötiedot ilman aiheetonta viivytystä tietyin edellytyksin. Oikeutta tietojen poistamiseen ei ole, jos lakisääteisen veloitteen noudattaminen edellyttää tietojen käsittelyä tai jos käsittely tapahtuu yleistä etua koskevan tehtävän suorittamista tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämistä varten. Näissä tapauksissa henkilötiedot hävitetään vasta laissa säädetyn määräajan jälkeen.

13.4. Milloin voin vaatia tietojeni käsittelyn rajoittamista?

Jos sinusta kerätyt eivät pidä paikkaansa, voit vaatia rajoittamaan asiakastietojesi käsittelyä, kunnes tietojen paikkansapitävyys on varmistettu.

13.5. Valituksen tekeminen

Sinulla on oikeus tehdä valitus valvontaviranomaiselle, jos koet henkilötietojen käsittelyn olevan tietosuojalainsäädännön vastaista. Voit tehdä valituksen tietosuojavaltuutetun toimistoon: www.tietosuoja.fi