

Wilma tietosuojan vaikutusten arviointi (DPIA)

Wilman yleiskuvaus

Wilma on suomalainen sähköinen opetuksen ja oppimisen hallintajärjestelmä. Wilmaa käytetään peruskouluissa, lukioissa, ammatillisissa oppilaitoksissa sekä muissa oppilaitoksissa. Wilma toimii tärkeänä työkaluna koulujen ja kodin välisessä yhteistyössä, helpottaen arjen koulutyön seurantaa ja hallintaa.

Wilma-järjestelmän kuvaus

Wilma sisältää neljä erillistä, mutta tiukasti toisiinsa liittyvää järjestelmäkokonaisuutta: Wilma, Primus, Kurre ja Links. Primus ja Kurre ovat opetushallinnon taustajärjestelmiä, joita pääasiassa opettajat ja muu henkilökunta arjessaan käyttävät täyttäessään opetuslainsäädännön asettamia tehtäviä. Näistä kahdesta edelleen Primus on Kurrea huomattavasti laajemmin käytetty ja ominaisuuksiltaan monipuolisempi. Wilma on puolestaan näiden kahden taustajärjestelmän rinnalle rakennettu selainpohjainen käyttöliittymäsovellus, joka osaltaan koostaa ja rikastaa taustajärjestelmissä käsiteltäviä tietoja. Wilman selainkäyttöliittymä ja erillinen mobiilisovellus ovat myös oppilaiden ja huoltajien saatavilla, siten Visma Wilma -järjestelmäkokonaisuuden tunnetuin järjestelmä. Selainkäyttöliittymän ja mobiilisovelluksen välillä on toiminnallisia eroja. Mobiilisovellus tarjoaa selainkäyttöliittymän toiminnoista lopputähtäjälle vain osan. Wilma Links on digitaalinen työpöytä, joka linkittyy suoraan koko Wilma- ekosysteemiin ja mahdollistaa saumattoman käyttökokemuksen eri palveluiden välillä.

Wilman rajaukset

Wilma ei sisällä mainoksia, käyttäjien profilointia tai toimi koulutuksen järjestäjän arkistona. Wilmaan ei myöskään saa kirjata terveystietoa. Wilma käytössä tulee huomioida, että Primus-tietokanta ei täytä sähköisen arkistolain mukaisia pysyväisarkiston vaatimuksia. Arkistolain mukaiset tiedot arkistoidaan opetuksen järjestäjän (Ruokolahden kunta) tiedonohjaussuunnitelman mukaisesti kunnan sähköiseen arkistoon.

Laki, johon käsittelyn tarkoitus perustuu

EU yleiseen tietosuoja-asetukseen (GDPR) ja Suomen tietosuoja lakiin (Tietosuoja laki 1050/2018), Perusopetuslaki 21.8.1998/628 ja Oppilas- ja opiskelijahuoltolaki 30.12.2013/1287, lukiolaki (714/2018) ja ammatillisesta koulutuksesta annettua lakia (531/2017)

EU yleiseen tietosuoja-asetukseen (GDPR) ja Suomen tietosuoja lakiin asetavat yleiset periaatteet ja vaatimukset henkilötietojen käsittelylle, mukaan lukien koulutuksen kontekstissa käsiteltävät henkilötiedot. Perusopetuslaki, lukiolaki ja ammatillisesta koulutuksesta annettu laki määrittelevät tarkemmin oppilaiden ja opiskelijoiden tietojen käsittelyn erityisesti perusopetuksessa, lukiossa ja ammatillisessa koulutuksessa.

Käytännössä nämä säädökset yhdessä ohjaavat, miten koulutuksen järjestäjät ja oppilaitokset saavat käsitellä oppilaiden ja opiskelijoiden henkilötietoja, kuten tietoja heidän edistymisestään, läsnäolostaan, arvosanoistaan ja muista koulunkäyntiin liittyvistä asioista.

Henkilöt, joiden tietoja käsitellään

Opetuksen henkilökunta, opiskelijat ja huoltajat. Lisäksi muita henkilötietoja, esim. koulukurattori, kouluterveys, rekisteripitäjän yhteyshenkilöt.

Erityisten henkilötietoryhmien käsittely

Uskontokunta

Tärkeä huomioida että viestinnän ja pedagogisten asiakirjojen yhteydessä voidaan käsitellä erityisiä henkilötietojen. Poikkeukset näiden tietojen käsittelyssä perustuvat perusopetuslakiin (21.8.1998/628, erityisesti 26 §: Perusopetuksen suorittaminen, 947/2022), oppilas- ja opiskelijahuoltolakiin (30.12.2013/1287), Lukiolakiin (714/2018) sekä ammatillisesta koulutuksesta annettuun lakiin (531/2017)

Rekisterinpitäjän ja henkilötietojen käsittelijän roolit

Visma Wilma toimii henkilötietojen käsittelijän roolissa ja Ruokolahden kunta rekisterinpitäjänä. Henkilötietojen käsittelystä on sovittu käsittelijän ja rekisterinpitäjän välisessä DPA-sopimuksessa.

Henkilötietojen käsittelyn perusteet

Wilman ja Ruokolahden kunnan välillä on DPA-sopimus.

Erityisten henkilötietoryhmien käsittelyn perusteet

Opetuksen lainsäädäntö Poikkeukset näiden tietojen käsittelyssä perustuvat perusopetuslakiin (21.8.1998/628, erityisesti 26 §: Perusopetuksen suorittaminen, 947/2022), oppilas- ja opiskelijahuoltolakiin (30.12.2013/1287), Lukiolakiin (714/2018) sekä ammatillisesta koulutuksesta annettuun lakiin (531/2017)

Henkilötunnusten käsittelyn perusteet

Tietosuojalaki 5.12.2018/1050

Henkilötietojen käsittelyn tiedottaminen

Wilma tarjoaa palveluntoimijan näkökulmasta tietosuojaselosteen henkilötietojen käsittelystä. Kunnan oma tietosuojaseloste löytyy [kotisivuilta](#).

Henkilötietojen poistaminen

Rekisterinpitäjällä on mahdollisuus poistaa henkilötietoja palvelusta yksilökohtaisesti. Palvelussa ei ole automatiikkaa tietojen poistoon, poisto on aina yksilökohtaista

Palvelutuotannon sijainti

Amazon Web Services -palvelussa EU:n toimialueella. Varmistukset on hajautettu EU/ETA-alueelle toisiin AWS:n toimialueisiin. Visman tuottamat tukipalvelut tuotetaan Suomesta.

Henkilötietojen siirrot ETA-alueen ulkopuolelle

Käsittelijä tai mikään sen alakäsittelijöistä ei käsittele henkilötietoja EU/ETA-alueen ulkopuolella.

Tietoturva

Wilma-palvelukokonaisuus ja siihen liittyvät tietojärjestelmät on ISO27001-auditoitu säännöllisesti ulkoisen auditointiorganisaation toteuttamana.

Salaukset

Tietoliikenne on aina salattua koko tietoliikenneketjun kattavasti. Asiakastiedot on salattu levyjärjestelmissä (AES-256 levossa). Salasanat ja muut tietokantaan tallennetut tiedot, jotka on määritelty salattavaksi ovat salattuja. Tietokannan ylläpitäjällä ei ole pääsyä salattuihin tietoihin. Salausavainten hallinta on toteutettu AWS:n Key Management Servicen avulla ja avaimiin on pääsy vain Vismalla. Tiedonsiirroissa sallitaan ainoastaan SFTP-yhteys tai selaimen yli käytettävä TLS-yhteys.

Salasanat

Visman salasanapolitiikka määrittää yleiset ja yhteiset toimintamallit. Se määrittää salasanan minimipituuden, kompleksisuussäännöt, salasanojen vaihtovälin ja muita salasanan muotoon ja käsittelyyn liittyviä ehtoja.

Tietojen anonymisointi ja pseudonymisointi

Wilmassa ei voida anonymisoida tai pseudonymisoida henkilötietoja, koska järjestelmä on luotu henkilötietojen käsittelyä varten. Tietoja voidaan poistaa oikeus tulla unohdetuksi -periaatteen mukaan.

Lisäturvatoimeenpiteet

Wilmassa on tuki monivaiheiseen tunnistautumiseen (MFA), joka on Wilma-käyttäjän turvallisuutta parantava toiminto. MFA:n käyttöä ei voi pakottaa Wilma-käyttäjille, vaan kukin käyttäjä voi ottaa sen käyttöön halutessaan itse.

Käyttöoikeudet

Palvelun käyttäjähallinnassa on vähintään kaksi eri käyttäjätasoa, kuten ylläpitäjä ja peruskäyttäjä. Käyttöoikeudet voidaan rajoittaa työntekijöiden työtehtävien mukaisesti siten, että eri käyttäjäryhmillä on eritasoisia oikeuksia. Ohjelmistossa on kuitenkin tiettyjä rajoituksia, jotka estävät käyttöoikeuksien riittävän tarkkuuden.

Käyttäjän tunnistautuminen

Wilman tunnistautumiseen voidaan yhdistää Suomi.fi-tunnistautuminen (huoltajat). Huollettavat yhdistetään palveluun Suomi.fi valtuuksien avulla. Wilmassa löytyy myös oma tunnushallinta, joka toimii sähköpostitunnuksella ja salasanalla, siihen voidaan lisätoimeenpiteenä kytkeä MFA käyttöön (ei pakollinen).

Henkilötietojen säilytysajat

Wilmassa ei voida määrittää henkilötietojen säilytysaikoja. Henkilötiedot arkistoidaan lakiperusteen päättymisen jälkeen. Niin kauan kuin palvelusopimus on voimassa ja kattaa henkilötietojen käsittelyn, käyttäjien henkilötietoja ei voida anonymisoida poistamisen sijasta. DPA-sopimuksessa määritellään tietojen poistaminen.

Lokit

Wilma kerää karkeasti jaettuna kahdenlaisia lokitietoja. Lukulokia, joka auttaa oppilaitosten pääkäyttäjiä selvittämään yksittäiseen henkilöön liittyviä tapahtumia. Wilmalla kerätään myös erilaisia teknisiä lokeja, joihin oppilaitosten henkilökunnalla ei ole pääsyoikeuksia. Wilmassa on käytettävissä lukuloki, jossa näkyy yksittäisen henkilön osalta häneen kohdistuneet lukutapahtumat sekä hänen tekemät lukutapahtumat. Lukutapahtuma tarkoittaa siis tiedonkatselua. Lukuloki on erikoistilanteissa pääkäyttäjien käyttöön tarkoitettu toiminto. Lokitietojen katselu on rajattu tiukasti vain pääkäyttäjien oikeudeksi. Vastaavasti järjestelmätoimittajan puolella lokitietoihin pääsy on rajattu tiukasti vain olennaisten teknisten asiantuntijoiden saataville, eikä lokitietoja tarkastella ilman oppilaitoksen pääkäyttäjältä tullutta pyyntöä. Teknisiin lokeihin pääsy on vain Vismalla. Tekniset lokitiedot on salattu, eikä niitä voi jälkikäteen muokata tai poistaa. Myös teknisten lokien katselu on luonnollisesti lokin piirissä. Teknisillä lokeilla kerätään tietoa mm. seuraavista tilanteista tai kohdista jäljitettävyyden varmistamiseksi: virhelaskurit, joiden perusteella voidaan selvittää tiedonsiirron ongelmia onnistuneista ja epäonnistuneista sisäänkirjautumisista ja niiden yrityksistä sekä onnistuneet ja epäonnistuneet tapahtumat, joilla on merkitystä tietoturvan kannalta. Lisäksi erilaisissa virhetilanneselvityksissä on mahdollista korottaa lokituksen tarkkuutta ja siten päästä tarkemmin virhetilanteen taustalla vaikuttavan juurisyyn jäljille. Ns. luovutuslokia, eli lokia tietojen luovuttamisesta kolmansille osapuolille, ei kerätä.

Lokien säilytysajat

Lokien säilytysajat voivat vaihdella suojattavan kohteen mukaan, yleisesti se sijoittuu kuuden ja 24 kuukauden välillä. Tarkkoja säilytysaikoja henkilötietojen osalta ei ole määritelty tietosuoja-asetuksessa. On rekisteripitäjän vastuulla arvioida, kuinka pitkään henkilötietoja tulisi säilyttää ottaen huomioon niiden käyttötarkoitus. Henkilötietoja on lupa säilyttää ainoastaan niin kauan kun se on tarpeellista niiden käyttötarkoituksen kannalta. Visma pyrkii noudattamaan lokien säilytysajoissa tietosuoja-asetuksen että tiedonhallintalain ohjeistuksia huomioiden myös kuntien ja organisaatioiden käyttötarkoituksen tarpeet.

Varmuuskopiointi

Varmistuksia otetaan kerran päivässä ja näitä varmistuksia säilytetään 30 päivää taaksepäin. Ruokolahden kunnalla on mahdollista ottaa myös omia varmistuksia haluamassaan aikataulussa erillisen ohjeistuksen mukaisesti.

Tietojen siirto järjestelmästä toiseen

Lähtökohtaisesti tietoja ei siirretä rekisterinpitäjältä toiselle. Tietoja voidaan kuitenkin siirtää poikkeustapauksissa hyödyntäen csv-, xml- tai json-muotoja.