

EU:n GDPR tietosuoja-asetuksen huomioonottaminen ja toteutus Asio Ohjelmistoissa



EU:n GDPR tietosuoja-asetus astui voimaan 25.5.2018 ja velvoittaa yrityksiä läpi toimialojen huomioimaan asetuksen tuomat tieto- ja yksityisyydensuojan velvoitteet kaikessa toiminnassaan ja ohjelmistoissaan.

GDPR koskee kaikkia henkilötietoja käsitteleviä organisaatioita sekä yksityisellä että julkisella sektorilla, järjestöissä ja säätiöissä sekä joissain tapauksissa myös yksityishenkilöitä.

Tietosuoja-asetusta sovelletaan kaikkien henkilötietojen käsittelyyn: asiakkaat, työntekijät, palvelun käyttäjät, toimittajat, alihankkijat ja kumppanit. Ohjelmistotoimittajan näkökulmasta GDPR tarkoittaa uusia henkilötietojen käsittelyyn liittyviä käytäntöjä, prosesseja sekä mittavia muutoksia ohjelmistojen henkilötietojen käsittelyyn liittyvissä toiminnallisuuksissa ja käytössä.

GDPR ei myöskään pysähtynyt 25.5.2018, vaan asetusta ja asetukseen liittyviä tulkintoja päivitetään jatkuvasti, joka edellyttää ohjelmistotoimittajalta jatkuvaluontoista ohjelmiston ja toiminnallisten prosessien ylläpitoa GDPR-yhteensopivana.

Asio-Data Oy huomioi GDPR-velvoitteet kaikessa toiminnassaan ja ohjelmistoissansa.

Syksyllä 2017 aloitimme asiakkaidemme kanssa keskustelun GDPR:n edellyttämistä toimenpiteistä Asio-ohjelmistojen käyttäjäorganisaatioissa ja Asio-ohjelmistoilta edellytettäviltä uusilta GDPR-toiminnoilta. Korostimme asiakasviesteissämme henkilötietojen käsittelyyn liittyvän valvonnan ja seurannan merkitystä.

Perehdyimme kattavasti GDPR-asetuksen sisältöön ja mitä se edellyttää ohjelmistotoimittajalta, ja laadimme sen pohjalta toiminta- ja ohjelmistokehityssuunnitelman, jolla ohjelmistomme ja käytäntömme saatetaan takarajaan mennessä GDPR-yhteensopiviksi.

Alkuvuonna 2018 kehitimme ja päivitimme ohjelmistoamme sisältämään kattavat uudet ohjelmalliset GDPR toiminnot tarkoitettuna Asio-ohjelmiston pääkäyttäjille. Koulutimme henkilöstömme GDPR:n tuomiin henkilötietojen käsittelyyn liittyviin velvoitteisiin ja suojeleuohjeisiin sekä rajasimme henkilöstömme pääsyn asiakkaidemme henkilötietojen käsittelyä koskeviin toimenpiteisiin salassapitovelvollisuuden alla operoiville ylläpidollisille tukiroolihenkilöillemme.

Päivitimme ohjelmistojemme ylläpidolliset sopimukset kattamaan GDPR-velvoitteet niin hajautettua pilvipalvelua kuin omaa palvelinta käyttävien asiakkaidemme sekä ohjelmisto- ja palvelun toimittajan rooliin sisältyvien velvoitteiden osalta.

Alkuvuodesta 2018 julkistimme Asio-ohjelmistosta version v18, joka sisältää uuden ohjelmiston pääkäyttäjille tarkoitetun ohjelmiston hallintapaneelista löytyvän GDPR-toimintoperheen ja ohjelmalliset pääkäyttäjän GDPR-työkalut.

Hallintapaneelin GDPR-toiminnallisuuksia kehitettiin ja laajennettiin edelleen alkuvuonna 2019 julkistetussa Asio-ohjelmistoversiossa v19 sekä tammikuussa 2020 julkistetussa versiossa v20.

Asiakkaan velvollisuutena on säännöllisesti käyttää Asio-ohjelmiston GDPR-tietojen poisto- ja pseudonymisointitoimintoja. Asiakkaan tulee omaa henkilötietojen käsittelyä ja rekisterinpitoa varten laatia GDPR-toimintasuunnitelma, jossa määritellään rekisteriin kirjattaviin eri henkilökategorioidiin sovellettava toimintatapa ja aikataulu. Esimerkiksi vuositilastointia varten voi olla tarpeen ensin nopealla aikataululla pseudonymisoida vierailijoiden henkilötiedot ja tilastointikauden päätyttyä suorittaa tarpeettomiksi käyneiden henkilötietojen poisto. **Asiakkaalla on velvollisuus poistaa järjestelmästä sellaiset käyttäjätilit, joiden olemassaoloon ei ole perusteita.** Asiakkaalla on velvollisuus valvoa, että käyttäjille ei ole annettu tarpeettoman laajoja oikeuksia.



Asio v20 GDPR-toimintoperhe sisältää seuraavat ohjelmalliset pääkäyttäjän GDPR-toiminnot.

Toiminto, jolla voidaan listata, pseudonymisoida ja/tai poistaa kaikki henkilöön Asion eri tietojoukoissa liittyvät kirjaukset.

Toiminto, jolla voidaan käyttäjäkohtaisesti nähdä, millä hakuehdoilla hän on hakenut henkilötietoja ja kuinka monta vastausta on saanut.

Toiminto, jolla voidaan nähdä, kuka on siirtynyt selailemaan tietyn henkilön perustietoja.

Toiminto, jolla voidaan käyttäjäkohtaisesti listata, mitä henkilön perustietoja on muutettu ja minä ajankohtana.

Toiminto, jolla voidaan siirtää henkilön perustiedot rajapintatiedostoon.

Toimintoperhe, jolla voidaan massaoperaatiolla poistaa tai pseudonymisoida vanhentuneiksi katsottuja tietoja eri tietojoukoissa siten, että tietojen sisäinen integriteetti ei vahingoitu.

Huomautus: Ohjelmistosta on tietoisesti jätetty tietojen anonymisointimahdollisuus pois. Tämän päätöksen perusteena on keskeisten asiakasryhmiemme henkilötietojen säilytystarpeen perusluonne. On mahdollistettava tilanne, jossa henkilölle tulee voida kertoa esimerkiksi hänen koulutushistoriansa hyvinkin pitkän ajan takaa.

Ohjelmistokehitys on jatkuvaa ja Asio ohjelmistojen GDPR-ominaisuuksia päivitetään sitä mukaa, kun uutta tietoa GDPR-velvoitteista on saatavilla sekä asiakaspalautteen pohjalta.

Omaa palvelinta käyttäviä Asiakkaitamme on hyvissä ajoin kehotettu ottamaan uusi versio käyttöön ennen lakiuudistuksen voimaantulon takarajaa toukokuussa 2018. Asion hajautettua pilvipalvelinta käyttävillä asiakkailla uudet toiminnallisuudet ovat olleet automaattisesti käytettävissä takarajaan mennessä eikä mitään toimenpiteitä ohjelmapäivitysten osalta heidän toimestaan tarvita. Asiakkaiden velvollisuutena on kuitenkin perehtyä uusiin GDPR-toimintoihin ohjelmistoversioissa v18, v19 ja v20 sekä ottaa ne käyttöön omassa toiminnassaan ja käytännössään soveltuvin osin. GDPR toiminnot on tehty järjestelmän PHP-ohjelmaan.

Tässä dokumentissa kuvatut, **vain pääkäyttäjälle sallitut toiminnot** on lisätty Asion ohjelmistoversioihin v18 ja v19. Massaoperaatioihin tarkoitettu GDPR-toimintoperhe kuvataan tämän dokumentin osassa 2.

Osa 1: Henkilön tietojen selailu, pseudonymisointi, poisto ja siirto

Toiminto löytyy hallintapaneelista *Henkilötietojen ylläpidosta* painikkeella *Henkilön kaikki tiedot*.

AsioEduERP - Henkilötietojen ylläpito v18.16 / Tietojen päivitys - Google Chrome
https://asp.asio.fi/dev/henkilo/index.php?func=sel&a_rowid=6997&a=1520960168&a=1520960168&poiminta=&ret=

Henkilötietojen ylläpito v18.16 / Tietojen päivitys

Tallenna Poista henkilö Kopioi henkilö Uusi haku Uusi henkilö
Henkilötietolomake Henkilön kaikki tiedot Suoritukset Tapahtumat Asiantuntijuuksien kiinnitys Luokittusten kiinnitys Alaiset Kustannuspaikat Toimenpidekirjaukset Henkilötietojen listaus

Henkilön tiedot Suppeat Laajat

Sukunimi	<input type="text" value="Ojala"/>	Etinimi	<input type="text" value="Risto Tapani"/>
Kutsumanimi	<input type="text" value="Ripa"/>	Sukupuoli	<input type="text" value="Mies"/>
HeTu [1]	<input type="text" value="010101-0101"/>	Henkilön tunnistenumero	<input type="text" value="57016"/>
Henkilön rooli	<input type="text" value="Opettaja"/>	Opiskelijan tila	<input type="text" value="(työssä)"/>

Työtiedot

Työnantaja/yritys Voit nopeuttaa työnantajatiedon poimintaa kirjoittamalla oikeanpuoleiseen kenttään haluamasi yrityksen nimen alkuosan. Paina tämän jälkeen "Poimi"-painiketta.

Titteli/asema	<input type="text" value="Työmiehes"/>	Tehtävänimike / Ammattiala (4)	<input type="text" value="Opiskelijat ja koululaiset"/>
Osasto	<input type="text" value="IT-osasto"/>	Vastuualue	<input type="text" value="Ohjelmointi"/>
Koulutusala	<input type="text" value="IT-osa"/>		
Peruskustannuspaikka	<input type="text" value="Kust.p. 76543"/>	Tili	<input type="text" value="Tili 2018"/>
Toiminto	<input type="text" value="Toiminto 44"/>	Projekti	<input type="text" value="Projekti 7777"/>
Osaamisprofiili	<input type="text" value="Ei osaa juuri mitään"/>		

Yhteystiedot

Osoitetarkenne	<input type="text" value="Rappu 2"/>		
Katuosoite	<input type="text" value="Työmiehentie 12"/>		
Postinumero	<input type="text" value="00100"/>	Postitoimipaikka	<input type="text" value="Ene"/>
Puhelin	<input type="text" value="0101010101"/>	Matkapuhelin/Työpuhelin	<input type="text" value="05076543211"/>
Telefax	<input type="text" value="Ei faxia"/>	Sähköposti	<input type="text" value="asio@asio.fi"/>
Auton rek.nro	<input type="text" value="ABC-123"/>		
Maa	<input type="text" value="Andorra"/>		
Kansalaisuus	<input type="text" value="Suomi"/>	Syntymäpaikka	<input type="text" value="Espoo"/>
Kieli	<input type="text" value="suomi"/>	WWW-sivu	<input type="text" value="www.asio.fi"/>
Sijaintikunta	<input type="text" value="Akaa"/>		

Koulutus ja muut taidot

Oppiaino	<input type="text" value="DI"/>	Koulutus	<input type="text" value="Akateeminen loppudiplomi"/>
Kielitaidot	<input type="text" value="suomi, ruotsi, englanti, saksa"/>		
Erityisavut	<input type="text" value="Ei juuri mitään"/>		

1. Henkilöön liittyvien kaikkien tietojen selailu tietojoukoittain ryhmiteltyinä

Henkilötietoja esiintyy näissä tietojoukoissa (tietyt lokitiedot ja tekstiviestit sekä sähköpostit käsitellään erikseen):

- Henkilön perustiedot
- Käyttöoikeustiedot
- Henkilö varauskohteena (poisto vain, jos ei varauksia)
- Varauskohteen vastuuhenkilönä
- Ryhmän luokanvalvojana
- Ryhmän vastuuopettajana/valmentajana
- Ryhmän nimikko-opettajana/-valmentajana
- Työnantajatiedot
- Henkilöasiakastiedot
- Kurssi-ilmoittautumiset (email avaimena)
- Kurssi-ilmoittautumiset. Käsitelty, mutta ei hyväksytyt (email avaimena)
- Kurssivaraukset
 - Muutos: Nimet, yhteyshenkilönimi ja syntymäaika
 - Tyhjäys: Ammatti, email, majoittuja, ruokailutoive
- Kurssivarauksen yhteyshenkilönä
 - Tyhjäys: Yhteyshenkilötunnus ja nimi
- Majoitusvaraukset, hlö rekisteristä
 - Muutos: Nimet, Yhteyshenkilönimi ja syntymäaika
 - Tyhjäys: Ammatti, email_majoittuja, ruokailutoive
- Suoraan kirjatut majoitusvaraukset
 - Poistetaan pääohjelmalla
- Majoitusvarauksen yhteyshenkilönä
- Tilaisuuksien osallistujatiedot, henkilö poimittu
- Tilaisuuksien osallistujatiedot, henkilö kirjattu suoraan
- Markkinointiluokitukset
- Asiantuntijuudet
- Alaisena
- Alaiset
- Toimenpidekirjaukset
- Kurssi-, tentti- ja hyväksymistulosilmoitukset
- Kurssitilan muutokset
- Suoritukset ja tapahtumat opiskelijana
- Suoritukset ja tapahtumat opettajana
- Varauksia henkilökalenterissa
- Opettajana/valmentajana varauksessa
- Kurssiohjelmaan merkittynä luennoitsijana
- Kurssiohjelmaan yhteyshenkilönä
- Kurssiassistenttina kurssitiedoissa
- Vastuukouluttajana kurssitiedoissa
- Kurssin koordinoijana (suunnittelijana) kurssitiedoissa
- Suoraan kirjattuna laskun viiitehenkilönä
- Henkilötietojen muutoksiin tehdyt lokimerkinnot
- Opetuksensuunnittelun ei-lukitut aikataulut
- Opettajan aikatoiveet
- OSU-pienryhmien opettajakytkennot
- Varauslomake-toiminnon OSU-pohjat

Esimerkki henkilöön liittyvistä tietojoukoista:

Henkilön kaikki tiedot / Ojala Risto / 57016

Markkinointiluokitukset (attributes_p) / Henkilönumero 57016

	Tunnus	Koodi	Pääloukka	Alaluokka	Tyyppi
<input type="checkbox"/>	57016	2042	Yksittäiset kurssit	13tv2_13510	H
<input type="checkbox"/>	57016	2042	Yksittäiset kurssit	13tv2_13510	H
<input type="checkbox"/>	57016	2042	Yksittäiset kurssit	13tv2_13510	H
<input type="checkbox"/>	57016	3164	Kurssikokonaisuudet	JAN123_16090	H
<input type="checkbox"/>	57016	3164	Kurssikokonaisuudet	JAN123_16090	H
<input type="checkbox"/>	57016	3164	Kurssikokonaisuudet	JAN123_16090	H

Poista valitut rivit

Asiantuntijuudet (attributes_p) / Henkilönumero 57016

	Tunnus	Koodi	Pääloukka	Alaluokka	Tyyppi
<input type="checkbox"/>	57016	4098	Kielitaito	ruotsi	H

Poista valitut rivit

Alaisena (attributes_p) / Henkilönumero 57016

	Tunnus	Koodi	Nimi1	Nimi2	Tyyppi
<input type="checkbox"/>	53382	57016	Ojala Risto	Ojala Risto	H

Poista valitut rivit

Kattavampi esimerkkilistaus-liite on ladattavissa Asio ohjelmistoversio v18 julkistus sivustoltamme osoitteessa <https://www.asio.fi/julkistukset/v18/>.

2. Henkilöön liittyvien tietojen tyhjäys ja poisto

Jokaisen tietojoukon osalta ohjelmaan on kirjattu logiikka, joka mahdollistaa tiedon tai tietojen tyhjäyksen ja/tai poiston. Tietyt tiedot poistetaan asianomaisilla ylläpito-ohjelmilla. Tyhjäyksellä tarkoitetaan myös tietojen pseudonymisointia näiden sääntöjen mukaan:

- **Henkilöturvatus:** Muutetaan muotoon 0101VV.
- **Sukunimi, etunimi, kutsumanimi ja muut selkokieiset henkilönimet:** Muutetaan muotoon NN.

Joidenkin, tilastoinnissa ja laskutuksessa tarvittavien tietojen tyhjäys on estetty. Näitä ovat:

- **Asion sisäinen henkilötunnus:** Toimii indeksinä useimpiin muihin tauluihin.
- **Sähköpostiosoite ja Työnantaja/yritys:** Ensin on tyhjättävä/poistettava ne tietojoukot, joissa sähköpostiosoite/työnantaja toimii indeksinä. Tämän jälkeen tiedon tyhjäys on mahdollinen.
- **Sukupuoli:** Tarvitaan tilastoinnissa.
- **Henkilön rooli:** Tarvitaan tilastoinnissa.
- **Postinumero:** Tarvitaan tilastoinnissa.
- **Maa:** Tarvitaan tilastoinnissa.
- **Kansalaisuus:** Tarvitaan tilastoinnissa.
- **Syntymäpaikka:** Tarvitaan tilastoinnissa.
- **Kieli:** Tarvitaan tilastoinnissa.
- **Sijaintikunta:** Tarvitaan tilastoinnissa.
- **Tilastotiedot:** Tarvitaan tilastoinnissa.
- **Kurssitunnus ja viikkonumero:** Tarvitaan tilastoinnissa.
- **Majoituksen ajankohta, huonetyyppi, huoneiden lukumäärä ja majoittujien lukumäärä:** Tarvitaan tilastoinnissa.

Ohjelma huolehtii siitä, että toisistaan riippuvien tietojoukkojen ”lapsia” ei poisteta ennen kuin ”vanhemmat” on poistettu.

Ohjelma mahdollistaa tiettyjen lokimerkintöjen, mm. henkilöön liittyvien perustietojen muutosten ja toimenpiteiden (esim. markkinointiviestintä) poiston. Mahdollisissa myöhemmissä selvittelyissä tarvittavia lokikirjauksia ei kuitenkaan poisteta. Näitä ovat mm. henkilön suorittamat henkilötietoihin kohdistuneet hakuoperaatiot tai hänen tietoihinsa kohdistuneet katselut.

Asio-Datan ylläpitohenkilöstö poistaa Asion Sanomapalvelimen kautta lähetetyt tekstiviestit ja sähköpostit kuuden kuukauden välein.

Esimerkki perustietojen tyhjäyksestä:

Perustiedot (person_p) / Henkilönumero 23660		Pseudonymisoi
<input type="checkbox"/> pseudo	Sukunimi <small>Katso taulukon alataidan ohjeet</small>	Testaaja
<input type="checkbox"/> pseudo	Etunimi <small>Katso taulukon alataidan ohjeet</small>	Teppo
<input type="checkbox"/> pseudo	Kutsumanimi	asdas
	Sukupuoli	Mies
<input type="checkbox"/> hetu	He Tu	asdasd
	Henkilön tunniste	23660
	Henkilön rooli	Opiskelija
<input type="checkbox"/> tyhjäys	Työnantaja / yritys <small>Katso taulukon alataidan ohjeet</small>	Asio
<input type="checkbox"/> tyhjäys	Katuosoite	Kyyluodontie 5
	Postinumero	00200
<input type="checkbox"/> tyhjäys	Postitoimipaikka	Helsinki

3. Tietojen pseudonymisointi

Ohjelma toimii seuraavien periaatteiden mukaisesti:

Pseudonymisoinnilla muutetaan tai tyhjätyään henkilön identifioimiseen tarvittavat keskeiset tiedot niin, ettei henkilö tietojärjestelmään tehdyissä kirjauksissa ole tunnistettavissa. Tietoja ei muutamia, vähemmän oleellisia tietojoukkoja lukuun ottamatta poisteta.

Pseudonymisointi tarkoittaa henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn henkilöön ilman lisätietoja. Tällaiset lisätiedot täytyy säilyttää huolellisesti erillään henkilötiedoista.

Vaikka tiedot olisi pseudonymisoitu, niiden avulla yksilö voidaan edelleen erottaa joukosta ja yhdistää eri tietoaineistoissa.

Pseudonymisoidut tiedot ovat yhä henkilötietoja, ja niiden käsittelyssä on sovellettava tietosuojasäännöksiä.

Esimerkiksi henkilötietojen koodaaminen on pseudonymisointia. Koodattuja tietoja ei voida yhdistää tiettyyn henkilöön ilman koodiavainta. Koodiavaimen haltija voi kuitenkin purkaa tietoaineiston salauksen ja helposti tunnistaa uudelleen jokaisen rekisteröidyn. Henkilötiedot voidaan myös suojata peitenimillä. Esimerkiksi tietokannoissa jokin henkilöön liittyvä tieto voidaan korvata toisella. Pseudonymisointi onkin tavallista muun muassa tutkimustoiminnassa ja tilastoinnissa.

Pseudonymisointi voidaan suorittaa niille tiedoille, jotka on indeksoitu henkilön perustietoon kuuluvalla, informaationvälillä neutraalilla henkilönnumerolla. Pääosa muutettavista ja tyhjätävistä tiedoista on kirjattu henkilön perustietoihin, mutta myös joissakin muissa tietojoukoissa saattaa olla tietosuojattavaa tietoa.

Ne henkilöön liittyvät kirjaukset, joissa nimitieto on kirjattu suoraan, kannattaa poistaa ohjelman massatoiminnoilla (kts. Osa 2). Poisto voidaan suorittaa myös pseudonymisointiprosessin jälkeen edellyttäen, että henkilön Asio-henkilönumero on käytössä.

Ohjelma ei poista/muuta niitä lokitietoja, joita saatetaan tarvita myöhemmissä selvittelyissä. Esimerkkinä ne lokikirjaukset, joihin on merkitty henkilön tietoihin kohdistuneet poiminnot ja haut (kuka, koska, hakukriteerit).

Ennen pseudonymisointia kannattaa kohdehenkilön Asio-henkilönumero ja -nimi merkitä muistiin ja tallentaa (turvalliseen paikkaan) niin, että siitä ilmenee toimenpiteen suorittaja ja ajankohta. Tämä tieto voi olla tärkeää mm. silloin, kun on kyse edellä kuvatuista jälkikäteiselvityksistä. Tämän tiedon tallentamien on sallittua ja kulkee pseudonymisoinnin käsitteistössä nimellä *koodiavain*. Koodiavain muodostetaan massapseudonymisoinneissa (Osa 2) ohjelman toimesta automaattisesti.

Ohjelma ei käsittele niitä tietoja, jotka pääohjelmassa on merkitty manuaalisesti suoritettaviksi. Näihin kuuluvat mm. henkilöasiakas- ja käyttöoikeustiedot.

4. Henkilön perustietojen lisäysten/muutosten lokikirjaukset

Henkilöön liittyvät muutuskirjaukset esitetään näin:

Henkilötietojen ylläpidon kautta tehtyjen muutosten lokikirjaukset (loki2_p/henkilo) / Henkilönumero 38188				
<input type="checkbox"/> anonym	Etunimi	Claudio	asio6	13.05.2014 17:56:42
<input type="checkbox"/> anonym	Sukunimi	Camacho	asio6	13.05.2014 17:56:42
<input type="checkbox"/> clear	Maksuhäiriömerkintä	38188 test only test only	asio6 asio6	29.01.2016 12:11:35 29.01.2016 12:58:30
<input type="checkbox"/> anonym	Kutsumanimi	Clasu	asiotest123	13.03.2018 18:35:38
<input type="checkbox"/> clear	Titteli / asema	Suunnittelija	asiotest123	13.03.2018 18:36:06
<input type="checkbox"/> clear	Vvh-jakaja (käytössä vain Savoniassa)	0.00	asio6	13.05.2014 17:56:42
<input type="checkbox"/> clear	Osaamisprofiili	Hyvä lähes kaikessa mitä tekee.	asiotest123	13.03.2018 18:36:06
<input type="checkbox"/> ssn	HeTu	010101	asio6	13.05.2014 17:56:42
<input type="checkbox"/> clear	Katuosoite	Isokaari 12 Isokaari 12 B 11	asiotest123 asiotest123	13.03.2018 19:41:00 13.03.2018 19:41:06

Huom.: tietojen poisto suoritetaan ylläpito-ohjelmalla.

Henkilötietojen lokitauluun (henkilo_loki_p) tehdään lisäksi vastaavat merkinnät hieman pelkistetympin (eri esimerkki kuin ylhäällä).

datetime	user	ip	person_id	tablename	row	field	action	program
0180921092017	asio6	192.168.0.14	10032	person_p	36		show	henkiloyllapito
0180921092017	asio6	192.168.0.14	10032	person_p	36	mobilephone	update	henkiloyllapito
0180921092017	asio6	192.168.0.14	10032	person_p	36	postal_address	update	henkiloyllapito
0180921092017	asio6	192.168.0.14	10032	person_p	36	postal_code	update	henkiloyllapito
0180921091835	asio6	192.168.0.14	10032	person_p	36		show	henkiloyllapito

5. Tietojen hakuun liittyvät lokikirjaukset

5.1. Henkilörekisteriin kohdistuneet hakuoperaatiot

Perustiedot ja asiantuntijuudet:

Näistä tehdään lokikirjaukset uuteen lokitauluun, joka sisältää tiedon siitä, kuka haki, koska ja millä hakutekijöillä sekä saatujen vastausten lukumäärä. Lokitaulun selailu tehdään järjestelmänhoitajan työkaluilla. Asion palvelinta käyttävien tulee ottaa yhteyttä Asio-Datan tukeen.

Tässä esimerkki tietyn käyttäjän suorittamien poimintojen hakutekijöistä:

datetime	user	ip	tablename	request	results
20180313185100	asiotest123	192.168.0.14	person_p	sex in ('N') and postal_address like '%espo%' and...	0
20180313185038	asiotest123	192.168.0.14	person_p	diet like '%vegaani%'	0
20180313185016	asiotest123	192.168.0.14	person_p	position like '%toimitus%'	0
20180313184748	asiotest123	192.168.0.14	person_p	postal_address like '%helsinki%'	19
20180313183923	asio6	192.168.0.14	person_p	lastname like 'cama%'	9

Esimerkkikäsky:

```
SELECT user, DATETIME, ip, request, results
FROM haku_loki_p
WHERE DATETIME
BETWEEN '20181001'
AND '20181115'
ORDER BY user
LIMIT 0, 30
```

5.2. Henkilötietojen katselu

Tämä lokitoiminto kirjaa ne toiminnot, joissa käyttäjä on avannut tietyn henkilön perustietojen ylläpito näytön (vaikka ei olisi tehnyt siihen päivityksiä). Kirjaukset tehdään tätä tarkoitusta varten perustettuun uuteen lokitauluun. Lokitaulun selailu tehdään järjestelmänhoitajan työkaluilla. Asion palvelinta käyttävien tulee ottaa yhteyttä Asio-Datan tukeen.

Tämä listaus kertoo, kuka, koska ja mistä on katsonut tutkittavan henkilön tietoja:

user	datetime	ip
asio6	20180313183926	192.168.0.14
asio6	20180313183916	192.168.0.14
asiotest123	20180313183607	192.168.0.156
asiotest123	20180313183538	192.168.0.156
asiotest123	20180313183501	192.168.0.156

Esimerkkikäsky tapauksessa, jossa listataan aikaväliltä kaikki selailu (kuka selaillut kenen tietoja):

```
SELECT user, p.lastname, p.firstname, h.person_id, DATETIME, ip
FROM henkilo_loki_p h, person_p p
WHERE DATETIME
BETWEEN '2018100100000000'
AND '2018111600000000'
AND h.person_id = p.person_id
ORDER BY user, person_id
```

5.3. Henkilötietojen lisäykset ja muutokset

Tässä esimerkki, jolla haetaan tieto siitä, ketkä ovat aikavälillä lisänneet tai muuttaneet tietoja. Tarkat muutostiedot löytyvät toiminnolla *Henkilön kaikki tiedot*.

```
SELECT lastname, firstname, person_id, creator_id, creation_date, modifier_id, modification_date
FROM `person_p`
WHERE creation_date
BETWEEN '181001'
AND '181115'
OR modification_date
BETWEEN '181001'
AND '181115'
ORDER BY lastname, firstname
LIMIT 0, 500
```

6. Tekstiviestit ja sähköpostit

Sanomapalvelimen kautta lähetetyt tekstiviestit tuhoetaan Asion toimesta laskutuskausittain eli puolen vuoden välein. Tekstiviestien välitystä hoitava operaattori (Nextup Oy) tuhoaa viestit omalta palvelimeltaan kolmen kuukauden jaksoissa. Sähköpostit jäävät välityspalvelimille, mutta niiden poistaminen Asion lähetystietokannoista sisältyy massatoimintoihin.

Osa 2: Massapseudonymisoinnit ja -poistot

Käytettävissä on myös laaja toimintokokonaisuus, joka on tarkoitettu vanhojen tietojen massasiivoukseen joko pseudonymisoiden tai poistaen.

Ohjelma on jaettu toimintokokonaisuuksiin, jotka soveltuvin osin suositellaan käsiteltäviksi ohjelman esittämässä järjestyksessä. Oleellista näissä toiminnoissa on se, että henkilöstä ei saa jäädä "orpoja" kirjauksia. Emme siis voi poistaa vain henkilön perustietoja, koska hän voi olla omistajana (esim. kalenteri) tai kohteena erityyppisissä varauksissa (vaikkapa opettajana). Poistot ja pseudonymisoinnit tulee siis tehdä suunnitelmallisesti.

Kaikkien osioiden hakuperiaate (paria poikkeusta lukuun ottamatta) on seuraava: Ohjelmaosio poistaa tai pseudonymisoi ne tiedot, joissa tietojoukon tuorein tieto on vanhempi kuin käyttäjän ilmoittama rajapäivä. Edellytyksenä on myös se, että kyseisen henkilön perustietoihin ei ole tehty muutoksia rajapäivän jälkeen.

Poistoista ja pseudonymisoinneista tehdään lokikirjaukset kussakin osiossa kuvattavalla tavalla. Pääkäyttäjän on syytä pitää erillistä kirjanpitoa siitä, milloin ja mitä hän on poistanut tai pseudonymisoinut.

Henkilön perustietojen pseudonymisoinnin yhteydessä ohjelma muodostaa koodiavainluettelon, jonka pseudonymisoijan tulee tallettaa turvalliseen paikkaan irralleen henkilötietojen käsittelyjärjestelmästä.

Toimintoperhe löytyy Asio-järjestelmän ylläpitotoiminnoista otsikolla GDPR.

Ohjelmien suoritus saattaa kestää kauan. Mm. tästä syystä ohjelma käsittelee vain rajatun määrän henkilötietoja kerralla. Käyttäjäorganisaation on syytä sisällyttää vanhojen tietojen siivous osaksi säännöllistä Asio-järjestelmän sisältöhuoltoa.

Seuraavassa esitetään jokaisesta toiminnallisuudesta lyhyt kuvaus. Laajempi selvitys on liitetty ohjelmistossa kunkin toiminnallisuuden ohjeistustekstiksi.

Kurssien osallistujien ja majoittujien pseudonymisointi / poisto

Ohjelman avulla voidaan pseudonymisoida niiden opiskelijoiden perustiedot, kurssivaraukset ja -ilmoittautumiset, joilla uusin kurssivaraus on aikaisempi kuin rajapäivä (varauksen loppupäivän perusteella) eikä henkilön perustietoihin ole tehty muutosta rajapäivän jälkeen. Ohjelma mahdollistaa myös samoin periaattein haettujen varausten ja ilmoittautumisten poiston sekä kyseisten opiskelijoiden perustietoihin suoritettavan pseudonymisoinnin. Ilmoittautumisten poisto suoritetaan sekä henkilönumeron että sähköpostiosoitteen (ei-hyväksytyt) perusteella.

Ohjelma käsittelee niitä henkilöitä, jotka on kirjattu henkilörekisteriin (ei siis ns. suoraan tehtyjä kirjauksia). Ohjelma käsittelee vastaavasti myös pelkät majoitusvaraukset ja kokousten osallistujatiedot.

Opiskelijoiden suoritustietojen poisto

Ohjelman avulla poistetaan ne opiskelijoiden suoritustiedot, joissa uusin suoritusmerkintä on aikaisempi kuin rajapäivä eikä henkilön perustietoihin ole tehty muutosta rajapäivän jälkeen. Opiskelijatiedot pseudonymisoidaan.

Opettajana opetusvarauksessa / yhteyshenkilönä tilavarauksessa

Ohjelman avulla pseudonymisoidaan tai poistetaan tilavarauksista ne opettaja- ja yhteyshenkilökiinnitykset, joissa uusin varaus on aikaisempi kuin rajapäivä eikä henkilön perustietoihin ole tehty muutosta rajapäivän jälkeen.

Kurssin vastuuhenkilönä, sihteerinä, opettajana ja luennoitijana

Ohjelman avulla pseudonymisoidaan tai tyhjätään kurssin perustiedoista ne vastuuhenkilö-, sihteeri-, opettaja- ja luennoitsijakiinnitykset, joissa kurssin loppupäivä on aikaisempi kuin rajapäivä eikä henkilön perustietoihin ole tehty muutoksia rajapäivän jälkeen. Poistoja ei suoriteta.

Vahvistamattomat kurssi-ilmoittautumiset

Toiminto listaa ennen rajapäivää tehdyt ilmoittautumiset, joita ei ole vahvistettu. Ohjelma mahdollistaa poistot, mutta ei pseudonymisointia.

Orpoja kirjauksia

Ohjelman avulla voidaan poistaa ns. "orvot" varauskirjaukset eli varaukset tai ilmoittautumiset, joihin merkiytyä henkilöä ei löydy henkilörekisteristä. Toiminto listaa kaikista kyseeseen tulevista tietojoukoista ne henkilöihin liittyvät tietorivit, joista ei ole yhteyttä henkilötunnuksen tai sähköpostiosoitteen kautta henkilön perustietoihin.

Viestintäloki

Ohjelman avulla poistetaan viestintään liittyviä kirjauksia.

Hetun tyhjäys

Ohjelman avulla tyhjätään henkilöturva- ja yritystunnuksia.

Henkilöasiakkaiden pseudonymisointi / poisto

Ohjelman avulla pseudonymisoidaan tai poistetaan asiakasrekisteriin kirjattuja henkilöasiakkaita.

Käyttäjän tilavausten poisto

Ohjelman avulla poistetaan valittujen käyttäjien tekemät, rajapäivää vanhemmat tilavaraukset. Käyttäjän tietoja ei poisteta, vaikka häneltä poistettaisiin kaikki varaukset.

Henkilöt, joilla henkilörekisterikirjauksen lisäksi vain mahdollinen käyttöoikeus ja/tai kalenteri ja/tai viestintäkirjauksia

Ohjelman avulla pseudonymisoidaan tai poistetaan ne henkilöt, joilla ei ole varauksia, kurssi-ilmoittautumisia, suorituksia tai muita kytkentöjä. Ohjelma tarkistaa, onko tällaisella henkilöllä kalenteri, käyttöoikeus ja/tai viestintäkirjauksia. Rajapäiväkäsittelyä sovelletaan henkilörekisterin luontikirjaukseen tai viimeisimpään muutoskirjaukseen.

Ohjelma tutkii myös sen, onko henkilö kirjattu varauksiin opettajaksi tai vastuuhenkilöksi tai kurssin toimihenkilöksi eikä nosta näitäkään henkilöitä tuloslistalle.

Ohjelma soveltuu oman henkilökunnan osalta vanhentuneiden rekisteröintien siivoamiseen ja muiden osalta loppusiivoukseen sen jälkeen, kun varaustiedot ovat pseudonymisoitu tai poistettu tämän toimintoperheen muilla ohjelmilla.

Henkilöt, joilla lisäksi on vain kurssivarauksia ja/tai -ilmoittautumisia

Tämä ohjelma on tarkoitettu lyhytkurssiohjelman käyttäjille. Ohjelman avulla pseudonymisoidaan tai poistetaan ne henkilöt, joilla on kurssi-ilmoittautumisia ja -varauksia sekä niihin liittyviä suorituksia ja markkinointikytkentöjä. Mikäli henkilöllä on näiden lisäksi muita kytkentöjä (poislukien käyttöoikeus, kalenteri ja viestintäkirjaukset), henkilöä ei poimita käsiteltävien henkilöiden listalle.

Rajapäiväkäsittelyä sovelletaan henkilörekisterin luontikirjaukseen tai viimeisimpään muutuskirjaukseen, kurssi-ilmoittautumien päiväkseen sekä kurssivarausjakson (yksittäiset kurssit) päättymispäivään.

Ohjelma tutkii myös sen, onko henkilö kirjattu varauksiin opettajaksi tai vastuuhenkilöksi tai kurssin toimihenkilöksi eikä nosta näitäkään henkilöitä tuloslistalle.

Ohjelma poistaa (poistovaihtoehto) henkilön kaikki suoritukset ja muut kiinnitykset (esim. markkinointi), mikäli edellä esitetyt ehdot täyttyvät. Pseudonymisointivaihtoehdossa näihin tietoihin ei kosketa.

Keskeisten lokitietojen leikkaus

Ohjelman avulla leikataan loki2_p rajapäivän perusteella. Tähän tauluun tallennetaan valtaosa varauksiin ja henkilöihin liittyvistä tietolisäyksistä, -muutoksista ja -poistoista

GDPR-lokin leikkaus

Ohjelman avulla leikataan henkilö_loki_p rajapäivän perusteella. Leikkaamisella tarkoitetaan rajapäivää vanhempien tietojen poistamista.



© Asio-Data Oy 2020

www.asio.fi