Tuote: GDPR-sovelluskirjasto

Viimeksi muokattu 01.09.2023

Perustiedot

Kuka tiedot antoi? *

MET-1-1.1

Kerro, missä roolissa annat tuotteen tiedot.

Valmistaja/palveluntarjoaja

Tuotteen lyhyt esittely

MET-1-2.1.

Kerro tuotteesta lyhyesti englanniksi.

Sovelluskirjasto.fi / GDPR-library EU is Due Diligence tool for software buyers. We offer you as a software vendor possibility to maintain gdpr-information of your product in the library.

Esittelysivu (jos on)

MET-1-3.1

https://sovelluskirjasto.fi/

1-5 sovellusta kuvaavaa luokkaa

Järjestelmänhallinta ja tukiohjelmat, Tiedonhallinta- ja käsittely

1. Tuotteen yleiset ehdot

Onko palvelussa ikäraja käyttäjille?

GEN-1-3.1

Ei

Valmistusmaa/palveluntarjoajan kotimaa *

GEN-1-5.1

Suomi

ISO-sertifioinnit

GEN-1-6.1

Valmistajalle myönnetyt ISO-sertifioinnit (27001, 27701).

Tyhjä/ei vastausta

Onko palvelusta asennettavissa mobiilisovellus?

GEN-1-7.1

Tyhjä/ei vastausta

Lisenssityyppi GEN-1-8.1

Nimetty käyttäjä

Onko virtualisointi mahdollista? GEN-1-9.1

Ei

Palvelukohtainen tietosuojaseloste (jos on) GEN-2-1.1

https://www.sovelluskirjasto.fi/en/privacy-policy/

Palvelun tietoturvakuvaus (jos on) GEN-2-2.1

Tyhjä/ei vastausta

Tietosuojavastaavan yhteystiedot GEN-2-3.1

Tyhjä/ei vastausta

Onko palvelussa mainoksia tai linkkejä kaupalliseen palveluihin? * GEN-2-4.1

Mikäli palvelussa on kaupallista sisältöä, kuvaa tarkemmin, mitä ja minkä ikäisille kaupallinen sisältö on tarkoitettu.

Ei

Käytetäänkö palvelussa evästeitä, joihin kysytään suostumus käyttäjiltä? GEN-2-5.1

Suostumus vaaditaan niin sanotuille ei-välttämättömille evästeille, jotka voivat liittyä esimerkiksi kolmansien osapuolten tekemään seurantaan. Sen sijaan kirjautumiseen ja palvelun toimintoihin liittyvät evästeet eivät vaadi erillistä suostumusta.

Ei

2. Käyttäjähallinta (loppukäyttäjät)

Käytetäänkö palvelua henkilökohtaisilla käyttäjätunnuksilla? UMA-1-1.1

Jos palvelussa on kirjautumisen vaativia osia, käytetäänkö niissä henkilökohtaisia tunnuksia ja salasanoja?

Kyllä

Onko palvelun käyttäjähallinnassa vähintään kaksi käyttäjätasoa: ylläpitäjä ja peruskäyttäjä? UMA-1-2.1

Vähintään kahdella käyttäjätasolla tarkoitetaan sitä, että palvelussa on mahdollista olla ylläpitäjiä, jotka voivat hallinnoida muiden käyttäjien tunnuksia ja käyttöoikeuksia.

Ei

Lisätietoa (englanniksi)

Customers who have signed an agreement get basic user rights to the service.

Voidaanko käyttöoikeudet rajata työntekijöiden työtehtävien mukaisesti eri käyttäjäryhmiin kohdistuvat oikeudet huomioiden? UMA-1-3.1

Vastuussa olevan rekisterinpitäjän on voitava hallita järjestelmän käyttöoikeuksia käyttäjien roolien ja tehtävien mukaisesti.

Ei

Lisätietoa (englanniksi)

There is no need to limit users' access rights in the service.

Mitä vaihtoehtoja palvelussa on integroida käyttäjähallinta organisaation keskitettyyn käyttäjärekisteriin ja kertakirjautumiseen (SSO)? UMA-1-4.1

Anna tarvittaessa lisätietoja integraatiomahdollisuuksista.

Tyhjä/ei vastausta

Lisätietoa (englanniksi)

SSO integration is coming later.

Onko kirjautuminen muiden palveluntarjoajien tunnuksilla mahdollista? UMA-1-5.1

Voiko palveluun kirjautua esimerkiksi Googlen, Microsoftin, Facebookin tai Applen tunnuksilla?

Ei

Voidaanko kirjautumisessa käyttää monivaiheista todentamista (MFA)? UMA-1-6.1

Ei

Onko käyttäjien vahva tunnistautuminen mahdollista? UMA-1-7.1

Voidaanko palvelun käyttäjiltä saada vahva tunnistautuminen esimerkiksi sähköisen henkilökortin tai pankkitunnusten avulla?

Ei

Tallentuuko kaikkien kirjautuneiden käyttäjien toiminnasta kattavat lokitiedot? * UMA-2-1.1

Vastuussa olevan rekisterinpitäjän on huolehdittava, että tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos järjestelmä edellyttää kirjautumista.

Kyllä

Tallentuuko lokiin kaikki henkilötietojen katselut? UMA-2-2.1

Tallentuuko lokiin esimerkiksi tieto siitä, jos ylläpitäjä katsoo muiden käyttäjien tietoja?

Kyllä

3. Tekninen tietojen suojaaminen

Millaisia integraatioita (rajapintoja) järjestelmään liittyy ja miten ne on suojattu ulkopuolisilta? * TDP-1-1.1

Vastuussa olevan rekisterinpitäjän on toteutettava suojattavien tietojen siirto tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä. Tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan turvallisesti ennen suojattavien tietojen siirtoa.

The service has a REST API. Use of the interface requires the conclusion of an agreement and a customer-specific password. An encrypted network connection is used for data transfer.

Tapahtuuko kaikki palvelussa tehtävä henkilötietojen käsittely niin, että verkkoyhteys on salattu ja käyttäjä tai tiedonsiirron osapuolet varmistettu? TDP-2-1.1

Kun salassa pidettävää tietoa siirretään tietoverkoissa, tieto salataan salausratkaisulla, jossa ei ole tunnettuja haavoittuvuuksia ja joka tukee moderneja salausvahvuuksia ja -asetuksia. Lisäksi vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen suojattavien tietojen siirtoa. Vaatimus koskee sekä käyttäjille tarkoitettuja toimintoja että palveluun kuuluvia rajapintoja.

Kyllä

Onko palvelua mahdollista käyttää niin, että kaikki henkilötiedot tallentuvat ainoastaan salatussa muodossa? TDP-2-2.1

Tallennetaanko henkilötiedot esimerkiksi tietokantaan salatussa muodossa sen sijaan, että tiedot olisivat selväkielisinä? Lisäksi edellytetään, että salauksen purkamiseen tarkoitetut tiedot (salausavaimet) säilytetään erillään tallennetuista tiedoista.

Ei

Onko palvelun tietosisältö varmuuskopioitu vähintään kerran päivässä ja onko varmuuskopioinnin palauttaminen mahdollista tehdä tarvittaessa nopeasti? * TDP-3-1.1

Varmistus- ja palautusprosessit on suunniteltu ja toteutettu siten, että ne vastaavat tietosuojalainsäädännön vaatimuksia tietojen eheydestä ja käytettävyydestä.

Kyllä

Voidaanko monivaiheinen todennus (MFA) pakottaa päälle kaikille käyttäjille kirjautumisessa? TDP-4-2.1

Monivaiheisen todennuksen pakottaminen tarkoittaa, että palvelu voidaan konfiguroida siten, että jokaiselta käyttäjältä vaaditaan sen käyttöönottoa.

Ei

Asennetaanko palveluun liittyvien ohjelmistokomponenttien tietoturvapäivitykset säännöllisesti ilman viivytystä? TDP-5-1.1

Kyllä

Onko tietoturvaa auditoitu ulkopuolisen tahon toimesta? Jos on, kenen toimesta? * TDP-5-2.1

Vastuussa olevan rekisterinpitäjän on varmistettava, että käytettävään tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet.

Ei

Tehdäänkö palveluun säännöllisiä tietoturva- ja haavoittuvuustestauksia? TDP-5-3.1

Vastuussa olevan rekisterinpitäjän tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja käytettävyys on varmistettava riittävällä testauksella säännöllisesti.

Kyllä

Lisätietoa (englanniksi)

The data security of the server is regularly monitored.

4. Tietosuoja

Mihin rooliin palveluntarjoaja asemoi itsensä tietosuojan osalta? DPR-1-2.1

Palveluntarjoaja määrittelee käsittelemiensä henkilötietojen osalta, toimiiko se rekisterinpitäjänä, yhteisrekisterinpitäjänä vai ainoastaan asiakasorganisaation henkilötietojen käsittelijänä.

Rekisterinpitäjä

Onko palveluun mahdollista asettaa käyttäjille näkyville asiakasorganisaation nimi sekä linkki sen oman tietosuojaselosteeseen? DPR-1-4.1

Palvelun käyttäjien tulisi aina nähdä, mikä taho on palveluun liittyvä rekisterinpitäjä, ja sen tulisi informoida henkilötietojen käsittelystä.

Ei

Onko palveluntarjoajalla pääsy asiakasorganisaation tallentamiin henkilötietoihin? * DPR-1-5.1

Tallentuvatko henkilötiedot palveluun sellaisessa muodossa, että palveluntarjoajalla on pääsy niihin? Onko palvelussa muita toimintoja, jotka johtavat palveluntarjoajan pääsyyn henkilötietoihin?

Kyllä

Lisätietoa (englanniksi)

The service provider creates user accounts for the customer's employees and manages them.

Syntyykö palvelun käytössä rekisteriä, jossa palveluntarjoaja on asiakasorganisaation kanssa yhteisrekisterinpitäjä? DPR-1-6.1

Ei

Syntyykö palveluntarjoajalle henkilötietorekisteriä käyttäjistä, jossa se on rekisterinpitäjä? DPR-1-7.1

Kyllä

Lisätietoa (englanniksi)

The service provider creates user accounts for the customer's employees and manages them.

Onko palveluntarjoajalla ajantasainen lista henkilötietojen alikäsittelijöistä, josta ilmenee kunkin alikäsittelijän nimi, sijainti, käsittelytarkoitus ja mahdollinen siirtoperuste EU/ETA-alueen ulkopuolelle? * DPR-1-8.1

Vastuussa olevan rekisterinpitäjän tulee saada tiedot kaikista palveluun liittyvistä henkilötietojen käsittelijöistä. Käsittelyssä tulisi käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet.

Kyllä

Linkki alikäsittelijöiden listaan (jos on) DPR-1-9.1

Tyhjä/ei vastausta

Käsitteleekö palveluntarjoaja tai jokin sen alikäsittelijöistä henkilötietoja EU/ETA-alueen ulkopuolella? DPR-1-10.1

Palveluntarjoaja on tunnistanut toimintaansa liittyvät kansainväliset henkilötietojen siirrot EU/ETA-alueen ulkopuolelle ja niihin käytettävät siirtoperusteet, sekä varmistanut, että siirrettäville henkilötiedoille taataan kolmannen maan lainsäädännössä tai käytettävillä täydentävillä suojatoimilla sellainen henkilötietojen suojan taso, joka vastaa olennaisilta osin EU:n tietosuojalainsäädännön tasoa.

Kyllä

Lisätietoa (englanniksi)

In Macedonian co-operation firm

Jos henkilötietoja käsitellään EU/ETA-alueen ulkopuolella, millä perusteella henkilötietoja siirretään? DPR-1-11.1

Komission hyväksymät vakiolausekkeet (artikla 46:2(c) ja artikla 46:2(d))

Lisätietoa (englanniksi)

Personal data is primarily processed within the EU/EEA area only. Personal data may, however, be transferred outside the EU/EEA especially if a services provider we use is located outside the EU/EEA.

If personal data were to be transferred outside the EU/EEA to a country that is not included in the EU Commission's decision on an adequate level of data protection, we will make sure that the processing, transfer and storage of your data is carried out on the grounds required by law and with adequate protection mechanisms, such as using the standard contract clauses confirmed by the EU Commission.

Voiko henkilötietoja siirtyä kolmansiin ei-turvallisiin maihin kuten Yhdysvaltoihin? * DPR-1-12.1

Ei-turvallisilla mailla tarkoitetaan maita, joiden viranomaisilla voi olla pääsy henkilötietoihin, tai joiden lainsäädännössä ei taata vastaavaa tietosuojan tasoa kuin EU:n tietosuojalainsäädännössä.

Ei

Mitä henkilötietoja palveluntarjoaja käsittelee? * DPR-2-1.1

Luettelo käsiteltävistä rekisteröityjen ryhmistä ja henkilötietojen tyypeistä.

Company name (employer)
Name of the person

Email address
Username and password
Log history of data entries and edits in the service, mainly: (1) who entered/edited data, (2) entries/edits made, (3) time stamp – this data is collected to ensure reliability of data in the service
Customary contact and billing details required for billing and invoicing paid services
Customary correspondence with users

Onko palvelu tarkoitettu myös erityisten henkilötietojen (esim. terveystiedot) käsittelyyn? *
DPR-2-2.1
Onko palvelu nimenomaisesti suunniteltu EU:n yleisen tietosuoja-asetuksen tarkoittamien erityisten henkilötietojen käsittelyyn?

Ei

Ovatko käyttäjiin liittyvät pakolliset ja vapaaehtoiset kentät määriteltävissä ylläpitäjän toimesta?
DPR-2-3.1

Kyllä

Tarjoaako palveluntarjoaja käyttäjille kattavat tiedot henkilötietojen käsittelystä palvelussa?
DPR-2-4.1

Kyllä

Käsitteleekö palveluntarjoaja henkilötietoja tietosuojalainsäädännön mukaisesti? *
DPR-2-5.1
Palveluntarjoajan oma vakuutus tuotteen GDPR-yhteensopivuudesta.

Kyllä

Mitä menetelmiä on käytössä, joilla varmistetaan, ettei tietoja käytetä muihin tarkoituksiin?
DPR-2-6.1
Palveluntarjoajan tulee käsitellä henkilötietoja vain DPA-sopimuksen ja rekisterinpitäjän antamien ohjeiden mukaisiin tarkoituksiin.

Tyhjä/ei vastausta

Onko palvelussa toiminto henkilötietojen pseudonymisointiin?
DPR-2-7.1

Ei

Tehdäänkö palvelun toiminnoissa profilointia, pisteytystä tai henkilöiden arviointia?
DPR-2-10.1
Liittyy tarpeeseen tehdä vaikutustenarviointi.

Ei

Käsitelläänkö käyttäjien sijaintitietoja? *
DPR-2-11.1
Liittyy tarpeeseen tehdä vaikutustenarviointi.

Ei

Voiko palvelussa määritellä henkilötietojen säilytysajat tai sen kriteerit? * DPR-2-12.1

Henkilötietojen käsittelyaika tulee voida määritellä.

Ei

Lisätietoa (englanniksi)

The customer must inform the service provider when the data of its employees must be deleted.

Voiko käyttäjien henkilötiedot anonymisoida poistamisen sijasta? DPR-2-13.1

Ei

Onko palveluntarjoaja tunnistanut tietosuojamäärittelyissään kaikki palvelun käyttöön selvästi liittyvät henkilötiedot? DPR-3-1.1

Rekisterinpitäjän ja palveluntarjoajan tulee tunnistaa kaikki käsittelemänsä henkilötiedot.

Kyllä

Vakuuttaako palveluntarjoaja, että rekisteröityjen oikeudet toteutuvat EU:n yleisen tietosuoja-asetuksen (GDPR) mukaisesti? * DPR-4-1.1

Palveluntarjoajan antama vakuutus rekisteröityjen oikeuksien toteutumisesta kuten tietojen tarkistamisesta ja korjaamisesta.

Kyllä

Lisätietoa (englanniksi)

The service provider uses personal data of the customer's employees only in accordance with the agreement and GDPR.

Miten ja milloin henkilötiedot poistetaan? * DPR-4-4.1

Henkilötietojen käsittelyaika tulee voida määritellä.

The customer must inform the service provider when the data of its employees must be deleted.

5. DPA-sopimus

Onko palveluntarjoajan kanssa mahdollista tehdä sopimus henkilötietojen käsittelystä (DPA)? * DPA-1-1.1

Rekisterinpitäjän tulee tehdä henkilötietojen käsittelijän kanssa EU:n yleisen tietosuoja-asetuksen vaatimukset täyttävä sopimus.

Ei

Linkki DPA-sopimuksen vakiomalliin (jos on) DPA-1-2.1

Tyhjä/ei vastausta

Onko DPA:ssa määritelty käsiteltävät henkilötiedot? DPA-1-3.1

Ei vastattu

Onko DPA:ssa määritelty henkilötietojen käsittelytarkoitukset? DPA-1-4.1

Henkilötietojen käsittelijän tulee käsitellä henkilötietoja vain DPA-sopimuksen ja rekisterinpitäjän antamien ohjeiden mukaisiin tarkoituksiin.

Ei vastattu

Voidaanko DPA:n yhteydessä antaa ohjeita, jotka palveluntarjoajan tulee huomioida henkilötietojen käsittelyssä? DPA-1-5.1

Rekisterinpitäjän tulee antaa henkilötietojen käsittelyä koskevat ohjeet ja varmistaa, että henkilötietoja käsitellään niiden mukaisesti.

Ei vastattu

Onko DPA:ssa sovittu, että palveluntarjoaja huolehtii salassapitovelvollisuudesta työntekijöilleen? DPA-1-6.1

DPA-sopimuksessa tulee varmistaa henkilötietojen käsittelyn luottamuksellisuus.

Ei vastattu

Onko DPA:ssa sovittu, että palveluntarjoaja sallii rekisterinpitäjän tekemän valvonnan ja auditoinnin? DPA-1-7.1

EU:n yleisen tietosuoja-asetuksen vaatimus DPA-sopimukselle.

Ei vastattu

Onko palveluntarjoajalla nimetty yhteyshenkilö tietosuoja-asioihin liittyen? DPA-1-8.1

Ei vastattu

Onko DPA:ssa määritelty tietojen poisto? DPA-1-9.1

Henkilötietojen käsittelyn päättyessä palveluntarjoaja vastaa tietojen poistamisesta tai palauttamisesta rekisterinpitäjälle.

Ei vastattu

Jos henkilötietojen käsittelyssä käytetään alikäsittelijöitä, onko EU:n yleisen tietosuoja-asetuksen (GDPR) noudattaminen ja riittävien suojatoimien toteuttaminen varmistettu sopimuksessa? DPA-2-1.1

Palveluntarjoajan tulee käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat EU:n yleisen tietosuoja-asetuksen mukaiset riittävät suojatoimet.

Ei vastattu

DPA-sopimuksen mukaiset alikäsittelijät tai linkki alikäsittelijöiden listaan (jos on) DPA-2.2.1

Tyhjä/ei vastausta

Palveluntarjoaja sitoutuu ilmoittamaan viipymättä kaikista tietoturvaloukkauksista DPA-3-1.1.

Palveluntarjoajan on ilmoitettava kirjallisesti henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan sen tietoonsa.

Ei vastattu

Käsitteleekö käsittelijä tai jokin sen alikäsittelijöistä henkilötietoja ETA-alueen ulkopuolella? * DPA-4-1.1

Palveluntarjoajan tulee tunnistaa toimintaansa liittyvät kansainväliset henkilötietojen siirrot EU/ETA-alueen ulkopuolelle ja niihin käytettävät siirtoperusteet, sekä varmistaa, että siirrettäville henkilötiedoille taataan kolmannen maan lainsäädännössä ja käytännöissä sellainen henkilötietojen suojan taso, joka vastaa olennaisilta osin EU:n yleisen tietosuoja-asetuksen tasoa.

Ei

Lisätietoa (englanniksi)

There is no DPA agreement for the service

Jos henkilötietoja käsitellään ETA-alueen ulkopuolella, millä perusteella henkilötietoja siirretään? DPA-4-2.1

Henkilötietojen siirrolle EU/ETA-alueen ulkopuolelle edellyttää laillista siirtoperustetta.

Ei vastausta

Jos henkilötietojen siirtoperusteena käytetään EU-komission vakiosopimuslausekkeita (SCC), mistä vakiolausekkeista on kyse? DPA-4-3.1

Tiedonsiirtoja kolmansiin maihin koskevat vakiolausekkeet (46 artikla) komission verkkosivuilla: Standard clauses for data transfers to third countries https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en

Ei vastausta

Voidaanko henkilötietoja luovuttaa kolmannen maan viranomaisille? * DPA-4-4.1

Mikäli henkilötietoja siirretään EU:n/ETA:n ulkopuolelle maahan, jossa viranomaiset voivat päästä käsiksi henkilötietoihin, tulee rekisterinpitäjän arvioida, tarvitaanko ns. täydentäviä suojatoimia.

Ei

Jos tietoja siirretään EU/ETA-alueen ulkopuolelle, onko palveluntarjoajalla dokumentaatiota, joka auttaa tietojensiirron vaikutusten arvioinnissa (transfer impact assessment, TIA)? DPA-4-5.1

Mikäli henkilötietoja siirretään EU:n/ETA:n ulkopuolelle, tulee rekisterinpitäjän arvioida, tarvitaanko ns. täydentäviä suojatoimia. Suositukset 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

Ei vastattu

Jos tietoja siirretään EU/ETA-alueen ulkopuolelle, mitä täydentäviä suojatoimia käytetään? DPA-4-6.1

Tyhjä/ei vastausta