

Henkilötietojen käsittelyn kuvaus ja Rekisterinpitäjän ohjeistus

1. Osapuolet

Rekisterinpitäjä: Saavutettavuuskirjasto Celia

Henkilötietojen Käsittelijä: Sopimuksessa ilmoitettu Palvelukumppani

2. Liitteen tarkoitus

Rekisterinpitäjä on tehnyt Henkilötietojen Käsittelijän kanssa Sopimuksen palvelusta, jossa Henkilötietojen Käsittelijä toimii Rekisterinpitäjän ylläpitämään henkilörekisteriin kuuluvien henkilötietojen käsittelijänä. Tässä dokumentissa kuvataan käsittelytoimet, joita Henkilötietojen Käsittelijä tekee Rekisterinpitäjän puolesta, henkilötietojen tyypit sekä käsiteltävät henkilötiedot. Henkilötietojen Käsittelijää sitovat tekniset ja organisatoriset toimenpiteet on kuvattu Rekisterinpitäjän ohjeistuksessa.

3. Henkilötietojen käsittelyn tarkoitus ja luonne

Henkilötietojen käsittelyn tarkoitus: uusien henkilöasiakkaiden rekisteröinti Celian asiakkaisiksi kirjastojärjestelmään, henkilöasiakkaiden tietojen ylläpito ja henkilöasiakkaiden avustaminen Celian palveluiden käytössä sekä Palvelukumppanin työntekijöiden käyttäjätunnusten ylläpito.

Henkilötietojen käsittelyn oikeusperuste:

- EU:n yleinen tietosuoja-asetus artikla 6 kohta 1 a: Rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten.
- EU:n yleinen tietosuoja-asetus artikla 6 kohta 1 b: Käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä.

- EU:n yleinen tietosuoja-asetus artikla 6 kohta 1 c: Rekisterinpitäjän lakisääteisen velvoitteen hoitaminen.
- EU:n yleinen tietosuoja-asetus artikla 9 (erityiset henkilötiedot) kohta 2 b: Rekisterinpitäjän lakisääteisten velvoitteen hoitaminen.

Ensisijaisesti käsittely tapahtuu perustuen Rekisterinpitäjän lakisääteiseen tehtävään liittyen. Toissijaisesti on mahdollista, että Rekisteröity antaa suostumuksensa käsittelyyn ja henkilötietojen käsittelyä suoritetaan suostumuksen ollessa voimassa.

Henkilötietojen Käsittelijä saa tunnukset Celian hallinnoimaan järjestelmään, jossa Henkilötietojen Käsittelijä pystyy toteuttamaan Sopimuksessa esitetyt tehtävät. Henkilötietojen Käsittelijä käsittelee järjestelmän henkilötietoja vain silloin kun sille on peruste Sopimuksessa sovittujen tehtävien hoitamiseksi. Tällöinkin henkilötietoja käsitellään vain siinä laajuudessa kuin on tarpeen.

4. Henkilötietojen käsittelyn kesto

Henkilötietojen Käsittelijä käsittelee tässä liitteessä yksilöityjä henkilötietoja niin kauan kuin Sopimus on voimassa.

5. Henkilötietojen tyypit ja Rekisteröityjen ryhmät

Käsiteltävät Henkilötiedot koskevat seuraavia Rekisteröityjen ryhmiä:

- Henkilöasiakkaat
- Työntekijät

Käsiteltävät Henkilötiedot koostuvat seuraavista Henkilötietojen tyypeistä:

- **Henkilöasiakastiedot** kuten nimi, kotiosoite, puhelinnumerot, sähköpostiosoite, syntymäaika ja lukemiseste.
- **Työntekijä- ja henkilöstötiedot** kuten nimi, käyttäjätunnus ja sähköpostiosoite.

Erityiset Henkilötietoryhmät:

- Henkilöasiakkaan terveyteen liittyvät tiedot, lukemisesteeseen liittyvät tiedot.

Rekisterinpitäjä määrittelee henkilöasiakkuuden itsessään erityisiä henkilötietoryhmiä koskevasi arkaluonteiseksi henkilötiedoksi ja näin ollen salassa pidettäväksi.

6. Rekisterinpitäjän ohjeistus

- Celian henkilöasiakastieto on linjattu erityisiä henkilötietoryhmiä koskevasi arkaluonteiseksi tiedoksi. Celia käsittelee arkaluonteista, Art. 9 mukaista erityisiä henkilötietoryhmiä koskevaa tietoa Celialle kansallisessa laissa säädetyn tehtävän suorittamiseksi (Laki Saavutettavuuskirjasto Celiasta 787/2022). Tietosuojalaki määrää erityisien henkilötietojen suojaamisen toimenpiteistä ja näin ollen arkaluonteisten tietojen käsittelyyn tulee suhtautua erityisellä huolellisuudella.
- Henkilötietojen Käsittelijä noudattaa voimassa olevan tietosuojalainsäädännön edellyttämää hyvää tietojen käsittelytapaa ja julkisuuslaissa sekä tiedonhallintalaissa tarkoitettua hyvää tiedonhallintatapaa, henkilötietojen suojaamista koskevia säännöksiä sekä Rekisterinpitäjän ohjeistusta tietojen käsittelystä.
- Henkilötietojen Käsittelijä ohjeistaa ja kouluttaa tarvittavat tietoturva- ja tietosuojakäytännöt henkilöstölleen vähintään tämän liitteen ja lainsäädännön vaatimusten edellyttämällä tavalla. Sama vaatimus koskee mahdollisten alihankkijoiden henkilöstöä.
- Henkilötietojen Käsittelijä varmistaa, että henkilötietojen käsittelyyn osallistuvat henkilöt sitoutuvat noudattamaan Sopimuksessa sovittua salassapitovelvollisuutta taikka että heitä koskee lakisääteinen salassapitovelvollisuus. Sama vaatimus koskee mahdollisten alihankkijoiden henkilöstöä.
- Henkilötietojen Käsittelijän tulee ilmoittaa Rekisterinpitäjälle Pääkäyttäjää koskevien käyttöoikeuksien muutoksista, jos Pääkäyttäjän tehtävät muuttuvat käyttöoikeuksien osalta.
- Henkilötietojen Käsittelijän ja sen alihankkijoiden tilojen tulee olla asianmukaisesti suojattu lukituksella ja muilla tarpeellisilla toimenpiteillä luvattoman pääsyn estämiseksi järjestelmään ja siellä oleviin salassa pidettäviin tietoihin.
- Henkilötietojen Käsittelijän on ilmoitettava Rekisterinpitäjälle henkilötietojen tietoturvaloukkauksesta sekä muista tuottamistaan palveluiden olennaisista häiriö- tai ongelmatilanteista, joilla voi olla vaikutuksia Rekisteröityjen asemaan ja oikeuksiin. Ilmoitus on tehtävä ilman aiheetonta viivytystä siitä, kun Henkilötietojen Käsittelijän tai sen käyttämä alihankkija on saanut loukkauksen tietoonsa. Ilmoitus tulee tehdä Celian tietosuojavastaavalle.

- Rekisterinpitäjä ja Henkilötietojen Käsittelijä sopivat tietojen luovutuksista ulkopuolisille. Henkilötietojen Käsittelijä ei luovuta tietoja ilman Rekisterinpitäjän kirjallista lupaa.
- Henkilötietojen Käsittelijä ymmärtää, että järjestelmään tallentuu sitä käytettäessä Henkilötietojen Käsittelijän tietoa.
- Rekisterinpitäjällä tai sen valtuuttamalla audittoijalla on sopimusliitteen 2 Tietosuojasopimuksen mukaisesti oikeus auditoida tai tarkastaa Sopimuksessa ja sen liitteissä sovittu toiminta varmistaakseen, että Henkilötietojen Käsittelijä noudattaa Sopimusta ja erityisesti toteutettaviksi vaadittuja teknisiä ja organisatorisia turvatoimia.
- Rekisterinpitäjä ohjeistaa, miten tietojärjestelmässä käsitellään henkilötietoja. Palvelun kohteena olevan järjestelmän käyttäjävaltuuksien myöntämismekanismi on sellainen, että niiltä osin, kun prosessi on Henkilötietojen Käsittelijän vastuulla, myöntöprosessista jää jälki, josta nähdään, millä perusteella käyttäjälle on myönnetty käyttövaltuus.
- Henkilötietojen Käsittelijän tulee käyttää käyttövaltuuksia luodessaan henkilökohtaisia tai roolikohtaisia käyttövaltuuksia, joista yksittäisen käyttäjän käyttövaltuudet voidaan selvittää.
- Henkilötietojen Käsittelijä varmistaa niiltä osin, kun käyttölaitteet ja ohjelmistot tai järjestelmät ovat Henkilötietojen Käsittelijän vastuulla, että ne tekevät riittäviä lokeja ja kirjausketjuja toiminnastaan ja Henkilötietojen Käsittelijä säilyttää palvelun kohteeseen liittyvät pääsynvalvontalokit niin, ettei niitä päästä jälkikäteen muuttamaan. Jotta lokit täyttävät riittävyysvaatimukset, lokien tulee sisältää tapahtuman ajankohta, suoritettu tai yritetty toimenpide, tekijä ja tämän valtuudet, tapahtumapaikka (esim. IP-osoite), muutostiedon lähde sekä tiedot toimenpiteen onnistumisesta. Epäonnistuneissa tapauksissa on kirjattava syy (esim. käyttöoikeuden puute).
- Henkilötietojen Käsittelijältä vaaditaan erityistä huolellisuutta salassapitovelvollisuuden, tietoturvan ja tietosuojan osalta. Salassapitovelvollisuuden lisäksi henkilötietojen näkyvyys on rajoitettu mahdollisimman suppeaksi ja henkilötietojen käsittelyä tehdään vain perustellusta syystä.

Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan seuraavia suojaustoimenpiteitä, joihin Henkilötietojen Käsittelijän on aktiivisesti ryhdyttävä:

- Henkilöstö on koulutettu tietoturvan ja tietosuojatehtävien hoidon mukaisesti.
- Henkilöstölle on annettu ajantasaisia ohjeita ja määräyksiä tietosuojaan sekä tietoturvaan liittyen.
- Henkilöstöllä on riittävät salassapitositoumukset tai heitä koskee lakisääteinen salassapitovelvollisuus.
- Henkilötietojen Käsittelijän tiloissa toteutetaan tilavalvontaa, johon sisältyy sisätilan tai sen osan tekninen valvonta valvontalaitteiston (kuten kameravalvonnan tai kulunvalvonnan) avulla.
- Henkilötietojen Käsittelijällä on asianmukainen ja käsittelyn luonne huomioiden riittävän sisältöinen prosessi sisäiseen käytönvalvontaan koskien Rekisterinpitäjän tarjoamaa tietojärjestelmää.
- Henkilötietojen Käsittelijä toteuttaa tietojärjestelmien tietoturvaa voimassa olevan henkilötietojen käsittelyn ja tietosuojan liittyvän lainsäädännön mukaisesti.
- Jos Henkilötietojen Käsittelijä käsittelee tietoa muualla kuin Rekisterinpitäjän tarjoamassa tietojärjestelmässä, tiedot tulee salata.
- Jos Henkilötietojen Käsittelijä käsittelee henkilötietoa muualla kuin Rekisterinpitäjän tarjoamassa tietojärjestelmässä, tiedot tulee mahdollisuuksien mukaan anonymisoida tai pseudonymisoida.
- Henkilötietojen Käsittelijä toteuttaa aktiivisesti tietoturvan ja tietosuojan auditointeja tiloihin, laitteisiin ja ohjelmiin, joilla ja jossa Rekisterinpitäjän tietoja käsitellään.
- Henkilötietojen Käsittelijän etäkäyttöyhteyksissä on käytössä riittävä salaus ja Rekisterinpitäjän tarjoamaan järjestelmään kirjaudutaan laitteilla, joissa käytetään tietoturvan kannalta asianmukaisia salasanoja/auktorisointimekanismeja.
- Henkilötietojen Käsittelijä käyttää niillä laitteilla, joilla Rekisterinpitäjän tarjoamaan järjestelmään kirjaudutaan tarkastus- ja valvontaratkaisuja (esim. lokitukset, henkilökohtaiset käyttäjätunnukset vahvalla salasanalla).
- Tietojen suojaamisesta on huolehdittava kaikissa käsittelyn vaiheissa alkaen tietojen keräämisestä ja päättyen tietojen tuhoamiseen. Käsittelyn turvallisuus edellyttää niiltä laitteilta, joilla Rekisterinpitäjän tarjoamaan järjestelmään kirjaudutaan, esimerkiksi kykyä taata tietojen jatkuva luottamuksellisuus, eheys,



Saavutettavuuskirjasto

CELIA

käytettävyys ja vikasietoisuus sekä kykyä palauttaa tietojen saatavuus ja pääsy tietoihin nopeasti fyysisen tai teknisen vian sattuessa.

