Service Provider Privacy Policy Template

SWAMID har tagit fram en exempelmall för hur en "privacy policy" kan se ut om tjänsten använder entitetskategorin GÉANT Data Protection Code of Conduct för att få attribut överförda från en identitetsutfärdare (IdP) till tjänsten (SP). När ni gör en egen anpassning av mallen till tjänsten är det viktigt att gå igenom alla delar och kontrollera att er tjänst fungerar som beskrivet, annars behöver ni ändra texten. Text i grönt är stöd till er när ni anpassar innehållet och ska inte finnas med i slutgiltigt dokument. Text inom < > ska ersättas med egeninformation.

Exempelmall: Överföring av personuppgifter till <namn på tjänsten> i samband med federerad inloggning (Privacy Policy)

Beskrivning av <namn på tjänsten>

Namn på tjänsten ska vara samma som mdui:DisplayName i tjänstens registrerade metadata i SWAMID.

Här beskrivs tjänsten på ett bra sätt riktat mot användare. En kärnfull sammanfattning på max 160 tecken av tjänstens beskrivning ska registreras i mdui:Description i tjänstens registrerade metadata i SWAMID.

<Namn på tjänsten> är en tjänst riktad till <användargrupp> från <exempel på organisationer>.

<Beskrivande text om tjänsten, ca 1-2 textstycken>

Hantering av personuppgifter

Överföring av personuppgifter

Det är viktigt att beskriva exakt vilka uppgifter som överförs och dess syfte. Informationen ska vara tydlig för de personer som dokumentet är avsett för. Den tekniska representationen används för felsökning och ska vara attributnamn som definierats i attributets LDAP-specifikation.

Personuppgifter överförs från identitetsutfärdaren (din inloggningstjänst) till tjänsten för att säkerställa att du som användare får tillgång till din information i tjänsten samt för att ge dig ett användaranpassat gränssnitt.

I samband med inloggning i denna tjänst begärs följande personuppgifter från den identitetsutfärdare du använder:

Personuppgifter	Syfte	Teknisk representation
Unik identifierare	*Att ge dig tillgång till din information*	*eduPersonPrincipleName*
Namn	*Namnet används i listor inuti tjänsten*	*displayName*
E-postadress	*Används för att kunna kontakta dig*	*mail*

Förutom direkta personuppgifter överförs även indirekta personuppgifter såsom vilken organisation användaren tillhör och vilken identitetsutfärdare som har använts vid inloggningen. I kombination med ovanstående personuppgifter kan dessa användas för att unikt identifiera en person.

Övrig behandling av personuppgifter i tjänsten

Här ska det beskrivas vilken ytterligare behandling av personuppgifter och dess syfte som sker inom tjänsten, t ex genom inmatning av personuppgifter från användarens sida ifall tjänsten har en lokal användarprofil som användaren själv kompletterar med information som ej kommer från identitetsutfärdaren. Det handlar också om personuppgifter som kommer ifrån annan källa och knyts ihop med användaren i tjänsten. Tänk också på att personuppgifter som sparas i loggfiler och på andra ställen måste beskrivas.

Överföring av personuppgifter till tredje part

Här ska det beskrivas vilken (om någon) överföring av personuppgifter som sker till tredje part. Tänk på att entitetskategorin GÉANT Data Protection Code of Conduct v1.0 (http://www.geant.net/uri/dataprotection-code-of-conduct/v1) medför kraftiga begränsningar av vilka personuppgifter som får överföras till tredje part.

Utdrag ur GÉANT Data Protection Code of Conduct v1.0:

> *The Service Provider agrees and warrants:*
>
> > *f) [Third parties] not to transfer Attributes to any third party (such as a collaboration partner) except*
> >
> > > *a. if mandated by the Service Provider for enabling access to its service on its behalf, or*
> > > *b. if the third party is committed to the Code of Conduct or has undertaken similar duties considered sufficient under the data protection law applicable to the Service Provider or*
> > > *c. if prior consent has been given by the End User;*

Rättslig grund

Under detta avsnitt ska det beskrivas under vilken rättslig grund enligt Dataskyddsförordningen (GDPR) som personuppgifterna behandlas. Den rättsliga grunden är kopplad till ändamålet med behandlingen.

Tänk på att den rättsliga grunden samtycke ställer väldigt höga krav på frivillighet och kan därför väldigt sällan användas för tjänster som en person använder i sin anställning eller i sina studier.

Rätt till registerutdrag, rättelse och radering av personuppgifter

Här ska användarens rättigheter enligt Dataskyddsförordningen (GDPR) beskrivas. Särskilt viktigt är åtkomst till personuppgifter, rättelse av personuppgifter samt radering av personuppgifter.

För registerutdrag, rättelse och radering av dina personuppgifter, kontakta personuppgiftsansvarig.

Rättelse av personuppgifter som överförts i samband med inloggning gör du i den identitetsutfärdare som du använder för att logga in. Dessa uppgifter rättas i tjänsten vid första inloggningen efter att personuppgifterna är rättade i identitetsutfärdaren.

Rensning av personuppgifter

Här beskrivs översiktligt tjänstens regelverk om automatiserad rensning av personuppgifter inkl. hur länge dessa sparas då användaren inte längre använder tjänsten.

Personuppgiftsansvarig

Här beskrivs kontaktvägar till personuppgiftsansvarig samt dess företrädare (den som inom organisationen är ansvarig/förvaltare för tjänsten). Kontaktvägar ska även anges till organisationens dataskyddsombud. OrganizationDisplayName i tjänstens registrerade metadata i SWAMID ska vara samma som organisationsnamnet i detta avsnitt.

Personuppgiftsansvarig för behandlingen av personuppgifter är <organisation>, <land>. Har du frågor om hur personuppgifter hanteras inom tjänsten tag kontakt med <e-postadress till tjänsteföreträdare>.

Dataskyddsombud är <namn>, <organisation>, <kontaktinformation>. alternativt Kontaktuppgifter till <organisation> dataskyddsombud finns på <URL till informationssida med kontaktuppgifter till dataskyddsombudet>.

GÉANT Data Protection Code of Conduct

Denna tjänst följer det internationella ramverket GÉANT Data Protection Code of Conduct (http://www.geant.net/uri/dataprotection-code-of-conduct/v1) för överföring av personuppgifter från identitetsutfärdare till tjänsten. Ramverket är avsett för tjänster i Sverige, EU och EES som används inom forskning och högre utbildning.

Template: Transfer of personal data to <name of the service> when using federated login (Privacy Policy)

Description of <service name>

The name of the service must be the same as mdui:DisplayName in the service's registered metadata in SWAMID.

<Name of the service> is a service directed towards <user group> from <examples of organisations>.

<Descriptive text about the service, approx. 1-2 paragraphs of text>

Processing of personal data

Transfer of personal data

It is important to clearly describe which data is being transferred and for what purpose. The information must be clear to the persons for whom the document is intended. The technical representation is used for troubleshooting and should be attribute names defined in the attribute's LDAP specification.

Personal data are being transferred from the identity provider (your login service) to the service to ensure that you as a user have access to your information in the service and to provide you with a user-friendly interface.

When logging in to this service, the following personal data are requested from the identity provider you use:

Personal data	Purpose	Technical representation

Unique identifier	*To give you access to your information*	*eduPersonPrincipleName*
Name	*The name is used in lists within the service*	*displayName*
E-mail address	*Used to be able to contact you by e-mail*	*mail*

In addition to direct personal data, indirect personal data are also transferred, such as which organisation the user belongs to and which identity provider has been used when logging in. In combination with the above personal data, these can be used to uniquely identify a person.

Other processing of personal data within the service

Here it must be described which further processing of personal data that takes place within the service and for which reason this is done, for example by entering of personal data from the user if the service has a local user profile which the user himself supplements with information that does not come from the identity provider. There should also be a description regarding personal data that comes from another source and is linked to the user in the service. Keep in mind that personal data stored in log files and elsewhere must be described.

Transfer of personal data to third parties

Here it must be described which (if any) transfer of personal data takes place to third parties. Keep in mind that the entity category GÉANT Data Protection Code of Conduct v1.0 (http://www.geant.net/uri/dataprotection-code-of-conduct/v1) imposes severe restrictions regarding which personal data may be transferred to third parties.

Excerpt from GÉANT Data Protection Code of Conduct v1.0:

> *The Service Provider agrees and warrants:*
>
> *f) [Third parties] not to transfer Attributes to any third party (such as a collaboration partner) except*
>
> *a. if mandated by the Service Provider for enabling access to its service on its behalf, or*
> *b. if the third party is committed to the Code of Conduct or has undertaken similar duties considered sufficient under the data protection law applicable to the Service Provider or*
> *c. if prior consent has been given by the End User;*

Lawful basis

This section describes the Data Protection Regulation (GDPR) lawful basis according to which the service processes personal data. The lawful basis is linked to the purpose of the processing.

Keep in mind that the lawful basis for consent places very high demands on voluntariness and can because of this very rarely be used for services that a person uses in their employment or in their studies.

Right of access, right of rectification and right of erasure of personal data

Here, the user's rights according to the Data Protection Regulation (GDPR) must be described. Particularly important is access to personal data, rectificatio n of personal data and erasure of personal data.

For access, rectification and erasure of your personal data, contact the Personal data controller.

Rectification of personal data that was transferred at the moment of login has to be done in the identity provider that you use to log in. This information is corrected in the service at the moment of the first login after the personal information has been corrected in the identity provider.

Purging of personal data

Here, a general description of the service's routines regarding automated purging of personal data, incl. how long the personal data are stored after the user no longer uses the service, should be entered.

Personal data controller

Here, contact information to the personal data controller and its representative (the person within the organisation who is responsible / administrator for the service) are described. Contact information must also be specified to the data protection officer. OrganizationDisplayName in the service's registered metadata in SWAMID must be the same as the name in this section.

Personal data controller for the processing of personal data is <organisation>, <country>. If you have questions about how personal data are processed within the service, please contact <e-mail address for service representatives>.

Data protection officer is <name>, <organisation>, <contact information>. alternatively Contact information for <organisation> data protection officer can be found at <URL to information page with contact information for the data protection officer>.

GÉANT Data Protection Code of Conduct

This service complies with the international framework GÉANT Data Protection Code of Conduct (http://www.geant.net/uri/dataprotection-code-of-conduct/v1) for the transfer of personal data from identity providers to the service. This framework is intended for services in Sweden, the EU and the EEA that are used in research and higher education.

Exempel på användning av denna mall

Nedan finns exempel på när mallarna på denna sida har använts.

- SWAMID Entity Category Release Check - Privacy Policy
- Överföring av personuppgifter till vid inloggning i Sunets Wiki and Jira
- Överföring av personuppgifter till Ladok i samband med federerad inloggning