GÉANT Data Protection Code of Conduct

(GDPR Version)

Working draft 29 May 2017

The work leading to this Code of Conduct has received funding from the European Community's Horizon2020 programme under Grant Agreement No. 731122 (GN4-2).

TABLE OF CONTENTS

PURPOSE OF THIS CODE OF CONDUCT

This Code of Conduct related to the sector of access management in the European Research Area is ruled by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR), and repealing Directive 95/46/EC.[1]

This Code of Conduct complies with the data protection principles stemming from the General Data Protection Regulation, taking account the specific characteristics of the processing carried out in the academic sector, and respecting the national provisions adopted by member states.

The Code of Conduct presents a harmonized approach to which Service Providers can commit when receiving End Users' personal data from the Home Organisations. Home Organisations will feel more comfortable to release affiliated End-User personal data to the Service Provider if they can see that the Service Provider has taken measures to properly protect the data.

This Code of Conduct constitutes a binding community code for the Service Providers that have committed to it.

Without prejudice to the provisions as set forth in the agreement between the **Home Organisation** and the **Service Provider**, which in all cases takes precedence, this Code of Conduct sets the rules that Service Providers adhere to when they want to receive End Users' Attributes from **Home Organisations** or their Agent for enabling access to their services.

This Code includes three appendices, detailing best practices on how to adhere to the rules of the Code.

These appendices relate to:

(1) information duties towards **End Users**,

(2) information security guidelines for **Service Providers** and,

(3) enforcement procedures for non-compliance with the Code of Conduct.

Following article 40.2 of the GDPR, the following principles and rules will apply to the whole Code of Conduct:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

[1] For further information regarding the purposes of this Code of Conduct, see the Explanatory Memorandum GEANT Code of Conduct of 16 May 2017;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the measures and procedures referred to in Articles 24 and 25 of the GDPR and the measures to ensure security of processing referred to in Article 32 of the GDPR;

(h) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(i) the transfer of personal data to third countries or international organisations; or

(j) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77.

WHO CAN ADHERE THIS CODE OF CONDUCT?

This Code of Conduct is addressed to any **Service Provider** established in any of the Member States of the European Union and in any of the countries belonging to the European Economic Area (all the Member States of the European Union, Iceland, Liechtenstein and Norway).

Furthermore, **Service Providers** established in any third country offering an adequate level of data protection in the terms of the article 45 of the GDPR and International Organisations can also subscribe to this Code of Conduct.

In addition to this, Article 40.3 of the GDPR gives the opportunity to **Service Providers** that do not fall under the territorial scope of the Regulation (Article 3, territorial scope) and that are established outside of the EEA to join this Code of Conduct in order to provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in point (e) of Article 46(2)..

SCOPE

This Code of Conduct is limited to the processing of **Attributes which are released for enabling access to the** Service as described in clause b. Purpose limitation.

In case the Service Provider uses the attributes for purposes other than enabling access to the service, these activities fall out of the scope of this Code of Conduct.

ROLES OF THE PARTIES INVOLVED

This Code of Conduct is addressed to Service Providers acting as data controllers without prejudice of the processing agreement between the Service Provider and the Home Organisation as described in clause q. Precedence.

In the context of this Code of Conduct:

1. A **Home Organisation** acts as a data controller as to the wider relationship with the **End User**, for example operating the IdP server in respect of the Attributes. An Agent who operates the IdP server on behalf of the **Home Organisation** acts as a data processor. This includes also the Federation Operators who operate a (potentially centralised) IdP server on behalf of the **Home Organisation**.

2. A **Service Provider** acts as a data controller in respect of the **Attributes**, processing them for the purposes as described in the clause b. Purpose limitation. In certain circumstances a **Service Provider** may be acting as a data processor, acting on behalf and as instructed by the **Home Organisation**.

3. An **End User** acts as a data subject whose personal data are being processed for the purposes as described in clause b. Purpose limitation.

As far as the disclosure of the **Attributes** of the **End User** is concerned, the **Service Provider** is obliged to comply with the obligations of the Code of Conduct.

The processing of the **Attributes** by the **Service Provider** for enabling access to the service is further explained in the Service-related Privacy Policy.

In the case that a Federation and a Federation operator do not process the **Attributes** of the **End User**, no specific privacy policy needs to be put in place between the End User and the Federation Operator.

PRINCIPLES OF THE PROCESSING OF ATTRIBUTES

To the extent the **Service Provider** acts as a data controller, it agrees and warrants:

A. LEGAL COMPLIANCE

The Service Provider warrants to only process the Attributes in accordance with: this Code of Conduct, contractual arrangements with the Home Organisation or the relevant provisions of the Personal Data protection law applicable to the Service Provider,

Where the Service Provider processes the Attributes, the Service Provider shall comply with:

1. the processing agreement between the Home Organisation and the Service Provider
2. the provisions of this Code of Conduct; and
3. applicable Data Protection Laws

All personal data processing activities carried out in this context shall comply with the GDPR.

The **Service Provider** based in the EEA territory commits to process the End User's **Attributes** in accordance with the applicable European data protection legislation. In principle, a Service Provider established in the EEA territory, subject to the European Data Protection legislation, shall not find himself in a situation where their national data protection laws would contradict this Code of Conduct.

The **Service Provider** based outside the EEA commits to process the End User's Attributes in accordance with the GDPR, this Code of Conduct and the eventual contractual arrangements (e.g: EU model clauses).

The **Service Provider** is expected to examine if any point in this Code of Conduct enters into conflict with the national data protection laws of his jurisdiction. In case of conflict of laws, the national law of his jurisdiction should be applicable and the Service Provider shall not commit to the Code of Conduct.

Service Providers established outside the EEA territory but in a country offering an adequate data protection pursuant to Article 45 of the GDPR, should assess the compliance of this Code of Conduct with their local laws. The **Service Provider** shall not commit to the Code of Conduct.

As far as Service Providers established in countries outside the EEA territory without offering an adequate level of protection pursuant to Article 45 of the GDPR are concerned, they shall, together with this Code of Conduct, engage on binding and enforceable commitments to apply the appropriate safeguards, including as regards data subjects' rights.

Service Providers may be subject to internal regulations and policies of Intergovernmental Organisations.

Regarding the applicable law,, see clause m. Governing law and jurisdiction.

In the event of conflict between the provisions of this Code of Conduct and the provisions of a contractual arrangement with the Home Organisation, see clause q. Precedence

B. PURPOSE LIMITATION

The **Service Provider** warrants processing Attributes of the **End User** solely for the purposes of enabling access to the services.

The Service Providers agree that the End User's personal data is processed for the purposes of the legitimate interests pursued by the Service Provider. The Attributes shall not be further processed in a manner which is not compatible with the initial purposes (Article 5.b of the GDPR).

The Service Provider must ensure that Attributes are used only for enabling access to the service. As far as the use of Attributes deviating purposes is concerned, please, see clause d. Deviating purposes

The Service Provider commits not to process the Attributes for further purposes than enabling access, unless the End User has given prior consent to the Service Provider (see Consent).

.

In practice, enabling access to the service covers:

- **Authorisation:** i.e. managing **End User’s** access rights to services provided by the **Service Provider** based on the **Attributes**. Examples of such **Attributes** are those describing the End User’s **Home Organisation** and organisation unit, their role and position in the **Home Organisation** (whether they are university members, students, administrative staff, etc.) and, for instance, the courses they are taking or teaching. The provenance of those **Attributes** is important for information security purposes; therefore, authorisation cannot be based on an Attribute that a user has self-asserted.

- **Identification** i.e. **End Users** need to have a personal account to be able to access their own files, datasets, pages, documents, postings, settings, etc. The origin of an **Attribute** used for identification is important; to avoid an identity theft, one cannot self-assert their own identifier. Instead, the Identity Provider server authenticates them and provides the **Service Provider** an **Attribute** that contains their authenticated identifier.

- **Transferring real-world's trust** to the online world i.e. if the **Service Provider** supports a user community that exists also in the real world, **Attributes** can be used to transfer that community to the online world. For instance, if the members of the user community know each other's by name in the real world, it is important that their names (or other identifiers) are displayed also in any discussion or collaboration forum offered by the **Service Provider**. The source of those **Attributes** is important; to avoid identity theft, one cannot assume user's name to be self-asserted but retrieved from a trustworthy source.

- **Researcher unambiguity** i.e. ensuring that a researcher's scientific contribution is associated properly to them and not to a wrong person (with potentially the same name or initials). In the research sector, publishing scientific results is part of researchers' academic career and the researchers expect to receive the merit for their scientific contribution. There are global researcher identification systems (such as ORCID and ISNI) which assign identifiers for researchers to help scientific Service Providers to properly distinguish between researchers, even if they change their names or organisation they are affiliated with.

- **Accounting and billing:** Personal data can be processed for accounting (for instance, that the consumption of resources does not exceed the resource quota) and billing purposes. In the research and education sector, the bill is not always paid by the End User but by their Home Organisation, project, grant or funding agency.

- **Information Security:** personal data can be processed for ensuring the integrity, confidentiality and availability of the service (e.g.: incident forensic and response)

- **Other functionalities** offered by the **Service Provider** for enabling access to the services, i.e. using **Attributes** of users for the purposes of other functionalities offered by the Service Provider. It is common that services on the Internet send e-mail or other notifications to their users regarding their services. Examples of scenarios where processing End User's email address or other contact detail falls within the scope of enabling access to the service include for instance:

    - the End User's application to access the resources has been approved by the resource owner;

    - the End User's permission to use a resource is expiring or they are running out of the resource allocation quota;

    - someone has commented the End User's blog posting or edited their wiki page.

Conversely, processing End User's e-mail address for sending them commercial or unsolicited messages does not fall within the scope of enabling access to the service of the **Service Provider**.

C. DATA MINIMIZATION

The Service Provider warrants to minimise the Attributes requested from a **Home Organisation** to those that are adequate, relevant and not excessive for enabling access to the service and, where a number of Attributes could be used to provide access to the service, to use the least intrusive Attributes possible.

The following list presents examples of attributes that are **adequate**, **relevant** and **not excessive** for enabling access in the context of the service:

- an attribute (such as, eduPersonAffiliation, eduPersonEntitlement or schacHomeOrganisation) indicating the End User's permission to use the service:
    - a trusted value provided by the IdP is needed instead of a value self-asserted by the End User
- an attribute (such as, SAML2 PersistentId) uniquely identifying the End User required, for instance, to store the End User's service profile:
    - a trusted value provided by the IdP is needed. The End User cannot self-assert their unique identifier
- if there are several alternative unique identifiers available for the service, the least intrusive must be used
    - pseudonymous bilateral identifier (such as, SAML2 persistentId) is preferred
    - if there is a legitimate reason to match the same End User's accounts between two Service Providers, a Service Provider can request a more intrusive identifier (such as eduPersonPrincipalName or eduPersonUniqueID), whose value for a given user is shared by several Service Providers
    - if there is a legitimate reason for an End User (such as, a researcher) to keep their identity and profile in the Service Provider even when the organisation they are affiliated with changes, a permanent identifier (such as, ORCID identifier) can be used
- a name attribute (such as commonName or DisplayName attribute) is necessary for a wiki or other collaboration platform, if the End Users know each other in real life and need to be able to transfer their existing real-world trust to an online environment.
    - if knowing the contributor’s name is important for the collaboration, the name can be released.
    - otherwise, the user may be indicated as "unknown" or a pseudonym the user has selected or the system has assigned to him/her.

- e-mail address or other contact details, if it is necessary to contact the **End User** for the proper functioning of the services offered by the **Service Provider**.

In the context of this Code of Conduct, under no circumstances a **Service Provider** is authorized to request End User's Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for the purposes of uniquely identifying a natural person or data concerning health or sex life or sexual orientation.

D. DEVIATING PURPOSES

> The Service Provider commits not to process the Attributes for further purposes than enabling access, unless the End User has given prior consent to the Service Provider (see Consent).

If the Service Provider wants to use the Attributes for purposes other than "enabling access to the service" (see clause b. Purpose limitation), it can only do so only if the End User gives his or her consent to the Service Provider.

Examples of deviating purposes[2] are: including End User's e-mail address to a newsletter offering new services, selling the Attributes to third parties, transferring information to third parties such as the search history, profiling activities etc.

E. DATA RETENTION

> The Service provider shall delete or anonymize all **Attributes** as soon as they are no longer necessary for the purposes of providing the service.

Under the GDPR, anonymized data does not constitute personal data; therefore, anonymized data can be kept indefinitely.

[2] Consult Article's 29 Working Party Opinion 03/2013 on purpose limitation. This document can guide the Service Provider to ascertain whether the purpose for the processing of the personal data is compatible or not.

The retention period of the **Attributes** depends on the particularities of the service and it needs to be decided by the **Service Provider**. However, a **Service Provider** shall not store the **Attributes** for an unlimited or indefinite period of time.

The **Service Provider** has to implement an adequate data retention policy compliant with the GDPR and other applicable data protection legislation. The existence of this policy must be communicated in the Service Provider'sprivacy policy (see clause i. Information duty towards Home Organisation).

For instance, the **Attributes** could be deleted after the expiration of the **End User's** session in the web service. On the other hand, for other services, it may be necessary to store the **Attributes** for a longer period of time.

In principle the data must be deleted or anonymised if the **End User** (or their **Home Organisation**) no longer wishes to use the service.

However, in many cases, the **End User** does not explicitly inform the **Service Provider** that they no longer wish to use the service, they just do not log in to the service anymore. In this case it is considered as a good practice to delete or anonymise the **End User's** personal data if they have not logged in for 18 months.

On the other hand, there are also circumstances where an **End User** not signing in does not necessarily mean that they no longer wish to use the service. The **Service Provider** shall implement appropriate processes to manage this type of situations. For instance:

- if the service is an archive for scientific data, the researchers who deposit their datasets to the archive may still remain the owners or custodians of the dataset although they do not log in for a while.

- if the service is a Git (a widely used source code management system) an **End User** uses to publish their computer program code, the **End User** may still want to be able to log in and maintain their code, although they have not logged in for a while.

- if the service is a repository where researchers publish their scientific findings and contribution, the researchers still want to have their name and other **Attributes** attached to the finding, although they do not regularly log in.

- if the service is a collaborative application (such as, a wiki or a discussion board) where the **End User** has their name or other **Attribute** attached to their contribution to let the other users learn and assess the provenance of the contribution and attribute it to a specific person.

The Personal Data, including log files, do not need to be removed or anonymised as long as they are needed:

- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;

- for compliance with a legal obligation which requires processing by International, European or Member State law to which the **Service Provider** is subject;

- for the performance of a task carried out in the public interest;

- for the establishment, exercise or defence of legal claims, such as resource allocation or invoices;
- for exercising the right of freedom of expression and information.

F. Respect the End User's Rights

The Service Provider shall respect End User’s rights, including the right to access to personal data, the right to request correction of any inaccurate information relating to them and the right to request deletion of any irrelevant Personal Data the Service Provider holds about him or her.

G. Transfer of Personal Data to Third Parties

The Service Provider shall 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.

The Service Provider shall not transfer Attributes to any third party (such as a collaboration partner) except:

a) if the third party is a data processor for the Service Provider in which case an ordinary controller-processor relationship applies between the Service Provider and the third party working on behalf of the Service Provider. The Service Provider must conclude a written agreement with such data processor in accordance with applicable laws.

b) if the third party which is also committed to the Code of Conduct. This is expected to be the case for various collaborative research scenarios, where the service is provided to the **End User** by several data controllers working in collaboration.

A typical scenario is a proxy setup where a research collaboration has a **Service Provider** that receives **Attributes** from **Home Organisations** and passes on (parts of) those **Attributes** to third parties providing the actual or additional services. In that case, the proxy **Service Provider** must make sure all third parties receiving Attributes are committed to the Code of Conduct or similar.

In contrast, if none of the **Attributes** received from the **Home Organisation** are being passed on, e.g. when only an internal identifier assigned by the proxy is sent to the third parties, the proxy does not need to make sure those third parties are committed to the Code of Conduct.

In a Service Provider proxy set-up, the organisation acting as the proxy (and operating the proxy server) needs to assume a role as the intermediary between the **Home Organisation** and the third party. For instance, the proxy needs to relay the suspected privacy or security breaches to the **Home Organisation** or its Agent, as described in clause H. Security measures.

c) if prior consent has been given by the **End User** as described in Consent

H. SECURITY MEASURES

The **Service Provider** warrants taking appropriate technical and organisational measures to safeguard Attributes against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. These measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the state of the art and the cost of their implementation.

The **Service Provider** shall implement the security measures described in Appendix 2: Information Security, technical and organisational guidelines for Service Providers. The Service Provider can also implement such additional security measures which, evaluated together, provide at least the same level of security as the level of security provided by the measures described in Appendix 2.

I. INFORMATION DUTY TOWARDS END USER

The **Service Provider** shall provide -at first contact- the **End User** with a Privacy Policy.

This Privacy Policy must be concise, transparent, intelligible and provided in an easily accessible form.

The Privacy Policy shall contain at least the following information:

- the name, address and jurisdiction of the **Service Provider**; where applicable
- the contact details of the data protection officer, where applicable;
- the purpose or purposes of the processing of the **Attributes**;
- a description of the **Attributes** being processed as well as the legal basis for the processing;
- the third party recipients or categories of third party recipient to whom the Attributes might be disclosed, and proposed transfers of **Attributes** to countries outside of the

European Economic Area;

- the existence of the rights to access, rectify and delete the **Attributes** held about the **End User**;
- the retention period of the **Attributes**;
- a reference to this Code of Conduct;
- the right to lodge a complaint with a supervisory authority;

The Privacy Policy can be, for instance, linked to the front page of the service. It is important that the **End User** can review the policy before they log in for the first time. The Privacy Policy shall use clear and plain language.

The **Service Provider** may include additional information, but must include as a minimum the information described above. The additional information could for example refer to the additional data processing activities of the **Service Provider**.

Additional processing activities must comply with the provisions of clause d. Deviating purposes and be included in the Privacy Policy

The Service Providers are advised to make use of the Privacy Policy template that belongs to the supporting material of the Code of Conduct in Appendix 1: Information duty towards End Users.

I. INFORMATION DUTY TOWARDS HOME ORGANISATION

The **Service Provider** commits to provide to the **Home Organisation** or its Agent at least the following information:

a) a machine-readable link to the Privacy Policy;
b) indication of commitment to this Code of Conduct;
c) any relevant updates or changes in the local data protection legislation that may affect this Code of Conduct.

GÉANT has put in place a scalable technical solution allowing Service Providers to add their adherence to this Code of Conduct and to communicate its privacy policy’s URL. This information is shared with the Home Organisation’s Identity Provider server prior to sharing the End User’s Attributes to the Service Provider.

The current technical infrastructure is based on standard SAML 2.0 metadata management and distribution system operated by Federation operators. However this Code of Conduct will apply despite the future changes in the technical infrastructure.

J. SECURITY BREACHES

The **Service Provider** commits to, without undue delay, report all suspected privacy or security breaches, meaning any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed concerning the **Attributes** to the **Home Organisation** or its Agent and, where this is legally required, to the competent data protection authority and/or to the **End Users** whose data are concerned by the security or privacy breach.

Article 33 of the GDPR describes the conditions when a personal data breach must be notified to the supervisory authority. This clause imposes an obligation to notify also the Home Organisation, to allow them taking the necessary technical and organisational measures for mitigating any risk the **Home Organisation** may be exposed to.

For example, if the **Service Provider** suspects that one or more user accounts in the **Home Organisation** has been compromised, the **Service Provider** contacting the **Home Organisation** enables the **Home Organisation** to take measures to limit any further damage (such as, suspend the compromised accounts) and to start the necessary actions to recover from the breach, if any.

The Service Provider shall use the security contact point of the Home Organisation or its Agent as provided in the technical infrastructure (currently, SAML 2.0 metadata), if available, for the reporting. When a security contact is not provided, the Service Provider shall communicate with alternative contact points.

Describe notification duties. When is it necessary to notify?

K. LIABILITY

The Service Provider agrees to hold harmless the **End User**, the **Home Organisation** as well as the Agent who has suffered damage as a result of any violation of this Code of Conduct by the **Service Provider** as determined in a binding and enforceable judicial ruling.

In the event of damages related to the breach of this Code of Conduct (i.e.: using the **Attributes** for other purposes, storing sharing the **Attributes** with third parties etc.), the **Service Provider** will hold the other parties harmless following a binding and enforceable judicial ruling.

For example, in case an **End User** files a complaint against his or her **Home Organisation** for unlawful release of **Attributes**, and it turns out that a **Service Provider** has released the **Attributes** to a third party, the **Home Organisation** will be held harmless against the **End User** by the **Service Provider** if it can prove the **Service Provider** has not complied with all the obligations of this Code of Conduct.

L. TRANSFER TO THIRD COUNTRIES

1. Transfers to parties that have **not** adhered to this Code of Conduct established outside the EEA

The **Service Provider** guarantees that, when transferring **Attributes** to a party that has not adhered to this Code of Conduct and that is based outside the European Economic Area or in a country without an adequate level of data protection pursuant to Article 25.6 of the directive 95/46/EC or Article 45.1 of the GDPR, to take appropriate measures

2. Transfers among Service Providers that have adhered to the Code of Conduct.

This Code of Conduct constitutes an adequate legal basis for cross-border transfers of Attributes among the Service Providers that have adhered to it, whether the Service Provider receiving the Attributes is established in the European Economic Area or not.

Under European data protection legislation, transfers of personal data from the European Economic Area to third countries that do not offer an adequate level of data protection are restricted, unless the recipient territory ensures a so-called *"adequate level of protection"*. However, there is an exhaustive list of derogations to this general prohibition that are relevant for this context:

- **Consent of the End User**: The unambiguous consent of the data subject legitimates data transfers to third countries, even if the recipient does not offer an adequate level of protection. The Service Provider may rely on the End User's freely given informed revocable Consent as described in **Error! Reference source not found.**

- **Contractual guarantees**: The existence of an appropriate contractual framework, supported by Standard contract clauses, either adopted by the European Commission or by a supervisory authority, the use of appropriate safeguards such as Binding Corporate Rules or other legally binding and enforceable instruments are recognised methods of transferring personal data. The use of Standard contract clauses does not exclude the possibility for the contracting parties to include them in a wider contract nor to add other clauses as long as they do not enter in contradiction. When using EU model clauses, the Service Provider needs to verify and ascertain that the other party is able to comply with all contractual obligations set out in the model clauses, especially taking into account local law applicable to such party. [Reference to the section of IOs]

M. GOVERNING LAW AND JURISDICTION

This Code of Conduct shall be interpreted in the light of the GDPR and of the guidance issued by the European advisory body on data protection and privacy[3][always with prejudice to any privileges and immunities of Service Providers being International Organisations, as these are awarded by their constituent and/or statutory documents and international law.].

This Code of Conduct shall be governed by the national laws of the country in which the **Service Provider** is established.

Alternatively, the **Service Provider** and the **Home Organisation** can refer to this Code of Conduct in the case where the **Service Provider** processed personal data on behalf of the **Home Organisation**. In that scenario, the applicable law is the one of the **Home Organisation.**

Any disputes regarding the validity, the interpretation or the implementation of this Code of Conduct shall be settled before the competent courts of the country in which the **Service Provider** is established.

International Private Law shall apply in order to confirm the applicable law and to determine whether a **Service Provider** is established in a country or not.

The Privacy Policy requires specifying the jurisdiction and the applicable law (clause I. Information duty towards End User.)

N. ELIGIBILITY

The Service Provider must be implemented and executed by a duly authorized representative of the **Service Provider**.

Each **Service Provider** must make sure that this Code of Conduct is executed by a person or by several persons who has or have the right to commit the **Service Provider** to this Code of Conduct.

The person administering the service that receives **Attributes** must identify the person or body in his or her organisation that can decide if the **Home Organisation** commits to this Code of Conduct, as typically, the service administrator cannot take this decision on his own.

[3] The Opinion 8/2010 on applicable law of the Article 29 Working Party, as updated in 2015, provides useful guidance on how to determine the applicable law in cross-national collaborations.

O. TERMINATION OF THE CODE OF CONDUCT

The **Service Provider** can only terminate adherence to this Code of Conduct in case of:

- this Code of Conduct being replaced by a similar arrangement,
- the termination of the service provisioning to the Home Organisation or
- the effective notification provided by the authorised by the Service Provider to terminate its adherence to this Code of Conduct

Even after the **Service Provider** has terminated its adherence to the Code of Conduct, the Attributes received continue to be protected by the GDPR (see p. Survival of the clauses).

P. SURVIVAL OF THE CLAUSES

The **Service Provider** agrees to be bound by the provisions of this Code of Conduct that are intended to survive due to their sense and scope after the end, lapse or nullity of this Code of Conduct.[reference to gdpr and other cocos]

Q. PRECEDENCE

The Service Provider warrants to comply with the stipulation that, in the event of conflict between a provision contained in this Code of Conduct and a provision of the agreement concluded between the **Service Provider** and the **Home Organisation**, the provision of the agreement concluded between **Service Provider** and **Home Organisation** takes precedence over the provision of this Code of Conduct.

In case of conflict between the provisions of the agreement between the Service Provider and the Home Organisation, this Code of Conduct and/or the data protection legislation, the following order shall prevail:

1. the processing agreement between the Home Organisation and the Service Provider

2. the provisions of this Code of Conduct; and
3. Applicable Data Protection Laws

If a **Service Provider** has an agreement (possibly a data processing agreement) with (some of) the **Home Organisation**(s) and the agreement is in conflict with this Code of Conduct, that agreement has precedence.

This section allows the **Service Provider** to have a bilateral agreement overriding the Code of Conduct with some **Home Organisations**, meanwhile, this Code of Conduct will still applies to the other **Home Organisations** that have not entered in a bilateral agreement.

CONSENT

The Service Provider shall request for End User's consent in the following scenarios:

1. When the purposes are not cover in b. Purpose limitation
2. When the attributes are released to third parties that are not part of this Code of Conduct
3. When the attributes are released to third parties, which are not part to this Code of Conduct, based in countries not offering an adequate level of protection .

Consent must be freely given, specific, informed and must unambiguously indicate the **End User's** wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of his or her personal data.

In the context of this Code of Conduct, when consent is used (e.g. d. Deviating purposes, g. Transfer of personal data to third parties, l. Transfer to third countries), it can be provided by a written statement, including by electronic means. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates the data subject's acceptance of the proposed processing of his or her personal data. Consent shall always be documented. Furthermore, the **End User** shall be able to withdraw his/her consent online.

Following Recital 43 of the GDPR, the Service Provider shall not rely on consent when there is a clear imbalance between the End User and the Service Provider.

APPENDIX 1: INFORMATION DUTY TOWARDS END USERS

This annex consists of two parts:

I. How to develop a privacy policy.

Although this is a mandatory obligation, practice has shown that many **Service Providers** have problems in developing an appropriate privacy policy for the services they provide. A practical template is provided to assist the **Service Providers**.

II. How the **Home Organisation** should inform the **End User** on the **Attribute release**.

This guideline is primarily for software developers who develop an **End User** interface for the **Attribute** release on an **Identity Provider** server.

HOW TO DEVELOP A PRIVACY POLICY

To understand the interplay of the **Home Organisation** and the **Service Provider** within the frame of the Code of Conduct, it is necessary to know that the Identity federations (and possible interfederation services like eduGAIN) relay the following information (called SAML2 metadata) from the **Service Provider** server to the Identity Provider server managed by the Home Organisation:

- a link to **Service Provider's** privacy policy web page (an XML element with the name mdui:PrivacyStatementURL) which must be available at least in English.
- the Service Provider's name and description (mdui:DisplayName and mdui:Description) at least in English. The name and description are expected to be meaningful also to the end users not affiliated with the service.
- optionally, the **Service Provider's** logo (mdui:logo) that can facilitate the user interface.
- the list of **Attributes** that the **Service Provider** requests from the **Home Organisation** and, for each Attribute, an indication that the Attribute is required. As the legal grounds for the attribute release (Article 7 of the data protection directive and Article 6.1 of the GDPR), the **Home Organisations** are suggested to use the legitimate interests legal grounds.

PRIVACY POLICY TEMPLATE

This template intends to assist **Service Providers** in developing a Privacy Policy document that fulfills the requirements of the GDPR and the Code of Conduct. The second column presents some examples (in italic) and proposes some issues that should be to taken into account.

The Privacy Policy must be provided at least in English. You can add another column to the template for a local translation of the text. Alternatively, the local translation can be a parallel page, and you can use the xml:lang element to introduce parallel language versions of the Privacy Policy page as described in SAML2 Profile for the Code of Conduct.

Name of the service	SHOULD be the same as mdui:DisplayName *WebLicht*
Description of the service	SHOULD be the same as mdui:Description *WebLicht is a service for language research. It provides an execution environment for automatic annotation of text corpora.*

Data controller and a contact person	*Tübingen university, Institute for language research* *Laboratory manager Bob Smith, bob.smith@example.org*
Data controller's data protection officer, if applicable	If the controller has a data protection officer (GDPR Section 4) *Chief Security Officer bill.smith@example.org*
Jurisdiction and supervisory authority	The country in which the Service Provider is established and whose laws are applied. SHOULD be an ISO 3166 code followed by the name of the country and its subdivision if necessary for qualifying the jurisdiction. *DE-BW Germany Baden-Württemberg* How to lodge a complaint to the competent Data protection authority: *Instructions to lodge a complaint are available at ...*
Personal data processed and the legal basis	*A. Personal data retrieved from your Home Organisation:* - *your unique user identifier (SAML persistent identifier) ** - *your role in your Home Organisation (eduPersonAffiliation attribute) ** - *your name ** *B.Personal data gathered from yourself:* - *logfiles on the service activity ** - *your profile* ... ** = the personal data is necessary for providing the service. Other personal data is processed because you have consented to it.* Please make sure the list A. matches the list of requested attributes in the

	Service Provider's SAML 2.0 metadata.
Purpose of the processing of personal data	Don't forget to describe also the purpose of the log files, if they contain personal data (usually they do).
Third parties to whom personal data is disclosed	Notice clause f of the Code of Conduct for Service Providers. Are the 3rd parties outside EU/EEA or the countries or international organisations whose data protection EC has decided to be adequate? If yes, references to the appropriate or suitable safeguards.
How to access, rectify and delete the personal data and object its processing.	*Contact the contact person above.* *To rectify the data released by your Home Organisation, contact your Home Organisation's IT helpdesk.*
Withdrawal of consent	If personal data is processed on user consent, how he/she can withdraw it?
Data portability	Can the user request his/her data be ported to another service? How?
Data retention	When the user record is going to be deleted or anonymised? Remember, you cannot store user records infinitely. It is not sufficient that you promise to delete user records on request. Instead, consider defining an explicit period. *Personal data is deleted on request of the user or if the user hasn't used the service for 18 months.*
Data Protection Code of Conduct	*Your personal data will be protected according to the Code of Conduct for Service Providers, a common standard for the research and higher education sector to protect your privacy.*

HOW THE HOME ORGANISATION SHOULD INFORM THE END USER ON THE ATTRIBUTE RELEASE

The Data protection laws create a set of requirements for the INFORM interactions with the user. This Data protection Code of Conduct proposes a division of responsibility where the INFORM interaction is carried out by the **Home Organisation** of the user, for instance, in an INFORM Graphical User Interface (GUI) installed to the Identity Provider server.

However, the Data protection regulators and the groups developing and enforcing these regulations recognize that there is a balance between full disclosure to meet the requirements and usability. A poor design of the user interaction screens can actually reduce the likelihood that users will understand what is happening.

LAW REQUIREMENTS

INFORMING THE END USER (“INFORM INTERACTION”)

For a **Home Organisation**, informing the end user can be done when a new end user gets his/her account at the institution. At that time, the **Home Organisation** has the first opportunity to inform that the user's **Attributes** may also need to be released to a **Service Provider** when he/she wants to access it. However, the law requires that, additionally, the end user needs to be informed about the specific **Attribute** release every time his/her **Attributes** are to be released to a new **Service Provider**.

The **Service Provider's** obligation to inform the end user depends on if it is a data processor or a controller. As a data controller, the **Service Provider** is responsible for communicating with the End user the issues above; which **Attributes** it will be using, and what it will be doing with them. As a data processor, a **Service Provider** can refer to the **Home Organisation**.

The Article 29 Working Party, EU advisory body contributing to the uniform application of the Data protection directive, took the view that the information must be given directly to individuals - it is not enough for information to be "available[4]".In the Internet, a standard practice to inform the end user on processing his/her personal data in services is to provide him/her a Privacy Policy web page in the service.

In the Web Single Sign-On scenario of SAML 2.0, a convenient place to inform the end user is at the Home Organisation before the Attribute release takes place for the first time. Several federations supporting the European higher education and research communities have already developed tools implementing this approach (e.g. the uApprove module implemented for Shibboleth, the consent module implemented for SimpleSAMLphp). This allows the user's decision to directly affect the transfer of

[4] Opinion 15/2011 on the definition of consent, p.20.

Attributes to the **Service Providers**; if the **Service Providers** were communicating with the user it might have already received all the **Attributes** and values.

GENERAL PRINCIPLES FOR INFORMING THE USER

Information dialogues should be short and concise.

The UK information commissioner proposes a "layered approach"[5], the basic information should appear on the main page, and a hyperlink shall be provided for detail. Merely having a clickable link labelled "privacy policy here" probably wouldn't be enough.

The goal is to provide a human readable form as the primary interface with the ability to click further to see what the 'technical' data is. The Acceptable Usage Policies presented by most Internet services do not suffice as they are rarely read nor understood by the users. The basic information should be provided as short accurate "user-friendly" descriptions; detailed information about "exactly what's going on" can be provided as a link.

Consequently, this profile recommends displaying the **Service Provider's** name, description, logo and requested attributes on the main page. If a user wants to learn more, he/she can click a link resolving to the **Service Provider's** Privacy policy. It is possible that users will actually not do the latter, but at least they have the ability to inform themselves of what is going on.

Layered notices can be particularly useful when describing the attribute values which will be released. In general, LDAP-style attributes are transferred to the SP. However, very few users have any familiarity with the conventions and usage of LDAP attributes. Instead, the Identity Provider could ask the user to release "name"; the link would take the user to a page listing all of the LDAP name attributes and values.

There are other attributes where the values are intentionally opaque (e.g. ePE="urn:mace:rediris.es:entitlement:wiki:tfemc2"). It is NOT reasonable to expect the end user to understand what this value means and to pick up a particular value to be released. Instead, natural language descriptions of the values should be provided.

A good way to explain to a user why there is a transfer of information is "your email, name and affiliation will be transferred". Explaining by analogy is human, albeit not necessarily academic in all disciplines.

[5] *"A layered notice usually consists of a short notice plus a longer notice. The short notice contains basic information, such as the identity of the organisation and the way in which the personal information will be used... The short notice contains a link to a second, longer notice which provides much more detailed information."* (the UK information commissioner's Privacy Notices Code of Practice, page 18).

RECOMMENDATIONS

For all Attributes (INFORM interaction):

1. The user MUST be informed on the attribute release separately for each SP.

2. The user MUST be presented with the mdui:DisplayName value for the SP, if it is available.

3. The user MUST be presented with the mdui:Description value for the SP, if it is available.

4. The user SHOULD be presented with the mdui:Logo image for the SP, if it is available.

5. The user MUST be provided with access (e.g. a clickable link) to the document referenced by the mdui:PrivacyStatementURL.

6. The IDP MUST present a list of the RequestedAttributes defined as NECESSARY. No user consent is expected before release. (However, given how web browsers work, the user may have to click a CONTINUE button in order to continue in the sequence.)

   The IDP MAY list the NECESSARY attributes on the same screen as the username/password entry boxes, making clear that *if* you login then this is what will happen. It MUST be clear to the user that the consequence of their next action will be to release the attributes. NOTE -- the attribute values for the specific user are not available when the login screen is presented, since the user's identity is not yet known.

7. The display software SHOULD provide the ability to configure and display localised descriptions of the attributes (e.g. what PersistentID means) and their values (e.g. what eduPersonEntitlement="urn:mace:rediris.es:entitlement:wiki:tfemc2" means)

8. The display software MAY inform the user of the release of an "attribute group" (eg attributes expressing the user's "name"), and then release all requested attributes in the group (e.g. various forms of the user's name such as cn, sn, givenName and displayName).

9. The display software MAY give the user the option to remember that they have been INFORMed of the release of the necessary attributes.

10. If any of the following has changed since the user accessed this SP for the last time, the user MUST be prompted again for the INFORM interaction

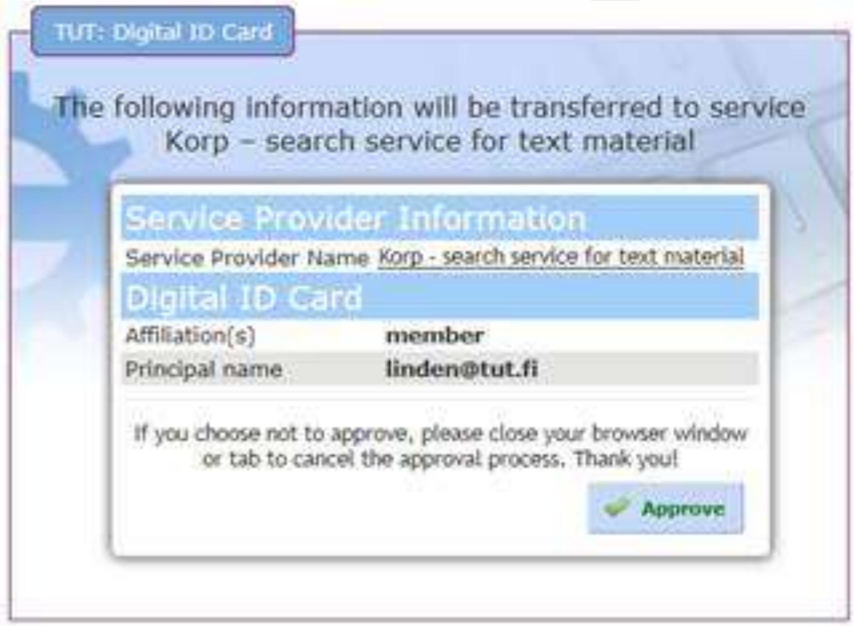
    a. the list of attributes the SP requests
    b. the DisplayName of the SP
    c. the Description of the SP

INTERNATIONALIZATION

The *lang* attribute of the *mdui* elements can be used to match the user's preferred language settings.

SAMPLE NOTIFICATION

Example of how a **Home Organisation** should inform **End Users** and provide an opt-out opportunity before **Attributes** are released to a new **Service Provider**. Clicking the **Service's Provider** name leads to its Privacy policy page.



TUT: Digital ID Card

The following information will be transferred to service Korp – search service for text material

Service Provider Information

Service Provider Name Korp - search service for text material

Digital ID Card

Affiliation(s)	member
Principal name	linden@tut.fi

If you choose not to approve, please close your browser window or tab to cancel the approval process. Thank you!

APPENDIX 2: INFORMATION SECURITY, TECHNICAL AND ORGANISATIONAL GUIDELINES FOR SERVICE PROVIDERS

This annex describes the technical and organizational security measures for protecting the **Attributes** as well as the information systems of the Service Provider where they are processed (such as a SAML SP software, the infrastructures on which the software is deployed and the application(s) it supplies with the Attributes). Note that the scope of this document is limited to what is required to protect the Attributes. The Service Provider may need to define as well other requirements for the protection of its assets.

To address the technical and organisational measures to protect the Attributes as well as the information systems of the Service Provider where they are processed, it is recommended that the **Service Providers** adopt the security measures described in the Sirtfi trust framework (ver 1.0) [SIRTFI] which are copied below for convenience.

NORMATIVE ASSERTIONS

In this section a set of assertions are defined that each organisation shall self-attest to so that they may participate in the Sirtfi trust framework. These are divided into four areas: operational security, incident response, traceability and participant responsibilities.

An attestation to the assertions in this document refers specifically and only to the statements in this section that are identified by labels within square brackets "[", "]".

How comprehensively or thoroughly each asserted capability should be implemented across an organisation's information system assets is not specified. The investment in mitigating a risk should be commensurate with the degree of its potential impact and the likelihood of its occurrence, and this determination can only be made within each organization.

1 OPERATIONAL SECURITY [OS]

Managing access to information resources, maintaining their availability and integrity, and maintaining confidentiality of sensitive information is the goal of operational security.

- [OS1] Security patches in operating system and application software are applied in a timely manner.

- [OS2] A process is used to manage vulnerabilities in software operated by the organisation.

- [OS3] Mechanisms are deployed to detect possible intrusions and protect information systems from significant and immediate threats

- [OS4] A user’s access rights can be suspended, modified or terminated in a timely manner.

- [OS5] Users and Service Owners (as defined by ITIL [ITIL]) within the organisation can be contacted.

- [OS6] A security incident response capability exists within the organisation with sufficient authority to mitigate, contain the spread of, and remediate the effects of a security incident.

2 INCIDENT RESPONSE [IR]

Assertion [OS6] above posits that a security incident response capability exists within the organisation. This section’s assertions describe its interactions with other organisations participating in the Sirtfi trust framework.

- [IR1] Provide security incident response contact information as may be requested by an R&E federation to which your organization belongs.

- [IR2] Respond to requests for assistance with a security incident from other organisations participating in the Sirtfi trust framework in a timely manner.

- [IR3] Be able and willing to collaborate in the management of a security incident with affected organisations that participate in the Sirtfi trust framework.

- [IR4] Follow security incident response procedures established for the organisation.

- [IR5] Respect user privacy as determined by the organisations policies or legal counsel.

- [IR6] Respect and use the Traffic Light Protocol [TLP] information disclosure policy.

3 TRACEABILITY [TR]

To be able to answer the basic questions "who, what, where, and when" concerning a security incident requires retaining relevant system generated information, including accurate timestamps and identifiers of system components and actors, for a period of time.

- [TR1] Relevant system generated information, including accurate timestamps and identifiers of system components and actors, are retained and available for use in security incident response procedures.

- [TR2] Information attested to in [TR1] is retained in conformance with the organisation’s security incident response policy or practices.

4 PARTICIPANT RESPONSIBILITIES [PR]

All participants (IdPs and SPs) in the federations need to rely on appropriate behavior.

- [PR1] The participant has an Acceptable Use Policy (AUP).
- [PR2] There is a process to ensure that all users are aware of and accept the requirement to abide by the AUP, for example during a registration or renewal process.

REFERENCES

[ITIL] Axelos ITIL Glossary of Terms, https://www.axelos.com/glossaries-of-terms

[SIRTFI] A Security Incident Response Trust Framework for Federated Identity, version 1.0: https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf https://www.axelos.com/glossaries-of-terms

[TLP] US Cert Traffic Light Protocol, https://www.us-cert.gov/tlp

APPENDIX 3: HANDLING NON-COMPLIANCE OF SERVICE PROVIDERS

INTRODUCTION

This appendix describes examples of situations of non-compliance to the GÉANT Data Protection Code of Conduct. As a result, actions can be raised and monitoring bodies can intervene.

This Data protection Code of Conduct relies on the following principles:

- The **Home Federation** that has registered a **Service Provider** records a technical indication (currently, using a tag embedded to SAML 2.0 metadata) on the **Service Provider's** adherence to the Code of Conduct. The indication signals that the **Service Provider** believes that its service is being operated in a manner that is consistent with the Code of Conduct.

- The technical infrastructure (currently, SAML 2.0 metadata exchange service) that the federation(s) provides delivers the indications from Service Providers to **Home Organisations'** Identity Provider servers.

- Reminding the **Service Provider** of a potential (suspected) non-compliance issue does not imply to make the reminding party sharing any legal responsibility with the **Service Provider**.

EXAMPLES OF SP NON-COMPLIANCE

The **Service Provider** can violate the Code of Conduct in several ways, such as:

- requesting Attributes which are not relevant for the service (c.f. clause b. Purpose limitation);
- processing the Attributes for an undefined period of time (c.f. clause e. Data retention);
- processing the Attributes for a deviating purpose or transferring them to a third party in a way that violates clause b. Purpose limitation and d. Deviating purposes of the Code of Conduct (for instance, transferring the **Attributes** to a company for commercial purposes without user consent);
- Disclosing the **Attributes** (c.f. clause d. Deviating purposes);
- Omitting to install security patches (c.f. clause H. Security measures and Appendix 2: Information Security, technical and organisational guidelines for Service Providers);
- Omitting to publish a privacy policy or publish an insufficient privacy policy (c.f. clause Appendix 1: Information duty towards End Users).

If anyone (such as an end user, a **Home Organisation** or a Federation Operator) suspects that a **Service Provider** is not complying with the Code of Conduct to which it has committed, the following alternative, mutually non-exclusive, actions are suggested:

1. Contact the Service Provider directly (with a copy to the **Service Provider's** Home Federation), describing the suspected problem, and ask the **Service Provider** to check if it has a compliance problem and correct it,

2. Contact the Service Provider's Home Federation, and request to contact the **Service Provider** and to check if there is a compliance problem and request to correct it. Depending on the Home Federation's policy, there may be also additional measures available for handling non-compliance.

3. Contact the body accredited to monitor compliance with the Code of Conduct, if applicable, as defined in the Article 41 of the GDPR and below;

4. Determine the location of the legal entity operating the **Service Provider**, and lodge a complaint with the competent Supervisory authority (as defined in Articles 57 and 58 of the GDPR).

CODE OF CONDUCT MONITORING BODY

A Federation operator can nominate a body to monitor the **Service Providers'** compliance with the Code of Conduct. The monitoring body must be accredited by a competent supervisory authority.

Only the monitoring body nominated by the Home Federation of the **Service Provider** is competent to assess the compliance of the **Service Provider** with the Code of Conduct.

The monitoring body publishes its contact details and procedures in a public and accessible way.

The monitoring body is responsible for processing complaints received from end users, Home Organisations, Federation Operators or other parties.

Having received a complaint the monitoring body will:

I. ask the **Service Provider** to present its counterpart,

II. give the **Service Provider** at most four weeks' time to revise the issue if the monitoring body finds the **Service Provider** to be non-compliant with the Code of Conduct

III. mandate the Home Federation to remove the **Service Provider's** tag if the Service Provider hasn't fixed the non-compliance issue within the given timeframe.

The **Service Provider** whose tag has been removed can reclaim the tag only after demonstrating to the monitoring body that it has returned to compliance.