REFEDS Data Protection Code of Conduct

REFEDS Best Practice
Version 2.0
28th March 2022

License:

Table of Contents

PURPOSE OF THIS CODE OF CONDUCT

This Code of Conduct relates to the processing of personal data for online access management purposes in the research and education sector as a best practice set of guidelines to help to meet the requirements set by the General Data Protection Regulation[1]. This Code of Conduct is not endorsed by the European Data Protection Board and is therefore only considered as a Best Current Practice.

Notwithstanding the provisions as set forth in an agreement between the **Home Organisation** and the **Service Provider Organisation**, which in all cases takes precedence, this Code of Conduct defines a set of rules that **Service Provider Organisations** can commit to when they want to receive **End Users**' **Attributes** from **Home Organisations** or their Agent for enabling the **End Users** to access their Services. **Home Organisations** will feel more comfortable to release affiliated **End Users**' **Attributes** to the **Service Provider Organisation** if they can see that the **Service Provider Organisation** has taken measures to properly protect the **Attributes**.

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

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

(1) Principles of the processing of attributes

(2) Glossary of Terms

(3) Purpose limitation and data minimisation

WHO CAN ADHERE THIS CODE OF CONDUCT?

Territorial Scope

This Code of Conduct is addressed to any **Service Provider Organisation** established in any of the Member States of the European Union and in any

[1] 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

other countries belonging to the European Economic Area (Iceland, Liechtenstein and Norway).

Furthermore, **Service Provider Organisations** established in any third country or International organization offering an adequate level of data protection in the terms of Article 45 of the GDPR or appropriate safeguards in the terms of the Article 46 of the GDPR can also subscribe to this Code of Conduct.

Functional Scope

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

In case the **Service Provider Organisation** uses the **Attributes** for purposes other than enabling the **End User** to access the Service, these activities fall out of the scope of this Code of Conduct.

The **Service Provider Organisations** and the communities representing the **Service Provider Organisations** can agree to apply the Code of Conduct also to other **Attributes**, such as those the **Service Provider Organisations** manage and share themselves, as further described in the Attribute Providers section.

ROLES OF THE PARTIES INVOLVED

This Code of Conduct is addressed to **Service Provider Organisations** acting as data controllers notwithstanding potential processing agreement between the **Service Provider Organisation** 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 Identity Provider (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 Organisation** 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 Organisation** may be acting as a data processor, acting on behalf and as instructed by the **Home Organisation**. A **Service**

Provider Organisation can also manage (and be a Data Controller for) extra **Attributes** of an **End User** and further become an Attribute Provider, as described in the Attribute Providers section. **Service Provider Organisations** may manage and register several independent Services, however, those doing so are asked to commit to the Code of Conduct for each Service separately.

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.

The processing of the **Attributes** by the **Service Provider Organisation** for enabling the **End User** to access the Service is further explained in the Service-related Privacy Notice.

PRINCIPLES FOR PROCESSING OF ATTRIBUTES

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

A. **Legal Compliance;** The Service Provider Organisation warrants to only process the Attributes in accordance with: the relevant provisions of the GDPR, this Code of Conduct and a contractual agreement with the Home Organisation, if any.

B. **Purpose Limitation;** The Service Provider Organisation warrants that it will process Attributes of the End User only for the purposes of enabling access to the Service. The Service Provider Organisation commits not to process the Attributes for purposes other than enabling the End User to access the Service.

C. **Data Minimisation;** The Service Provider Organisation commits to minimise the Attributes requested 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.

D. **Information Duty Towards End Users;** The Service Provider Organisation shall provide the End User with a publicly readable Privacy Notice before they initiate the federated login for the first time. This Privacy Notice must be concise, transparent, intelligible and provided in an easily accessible form. The Privacy Notice shall contain at least the following information:

   a. the name, address and jurisdiction of the Service Provider Organisation; where applicable;

   b. the contact details of the data protection officer, where applicable;

   c. the purpose or purposes of the processing of the Attributes;

   d. a description of the Attributes being processed as well as the legal basis for the processing;

   e. 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;

   f. the existence of the rights to access, rectify and delete the Attributes held about the End User;

   g. the retention period of the Attributes;

   h. the right to lodge a complaint with a Supervisory Authority.

E. **Information Duty Towards Home Organisation;** The Service Provider Organisation commits to provide to the Home Organisation or its Agent at least the following information:

   a. a machine-readable link to the Privacy Notice;

   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.

F. **Data Retention;** The Service Provider Organisation shall delete or anonymize all Attributes without undue delay as soon as they are no longer necessary for the purposes of providing the Service.

G. **Security Measures;** The Service Provider Organisation warrants taking appropriate technical and organisational measures to safeguard Attributes against accidental or unlawful destruction or accidental loss, alteration, unauthorised 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.

H. **Security Breaches;** The Service Provider Organisation 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.

I. **Transfer of Personal Data to Third Parties;** The Service Provider Organisation shall not transfer Attributes to any third party (such as a collaboration partner) except:

   a. if mandated by the Service Provider Organisation for enabling the End User to access 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 Organisation or;

   c. if prior consent has been given by the End User.

J. **Transfer of Personal Data to Third Countries;** The Service Provider Organisation guarantees that, when transferring Attributes to a party that is based outside the European Economic Area or in a country without an adequate level of data protection pursuant to Article 45.1 of the GDPR or the recipient is an International Organisation, to take appropriate safeguards (Article 46) or use the derogations pursuant to Article 49.

K. **End User's Consent;** When consent is used, as per Article 7 of GDPR, inter alia, it must be freely given, specific, informed and must unambiguously indicate the End User's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of their personal data. Furthermore, the End Users shall be able to withdraw their consent.

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

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 Data Protection Board or its predecessor, always notwithstanding any privileges and immunities of Service Provider Organisations being International Organisations, as these are awarded by their constituent and/or statutory documents and international law. If there are any disputes regarding the validity, interpretation or implementation of this Code of Conduct, the parties shall agree on how and where to settle them.

N. **Eligibility;** The Code of Conduct must be implemented and executed by a duly authorised representative of the Service Provider Organisation.

O. **Termination of the Code of Conduct;** The Service Provider Organisation can only terminate adherence to this Code of Conduct in case of:

   a. this Code of Conduct being replaced by a similar arrangement, or;

   b. the termination of the Service provisioning to the Home Organisation or;

   c. the effective notification provided by the authorised representative of the Service Provider Organisation to terminate its adherence to this Code of Conduct.

P. **Survival of the Code of Conduct;** The Service Provider Organisation 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 until the processing terminates.

Q. **Precedence;** The Service Provider Organisation 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 Organisation and the Home Organisation, the provision of the agreement concluded between Service Provider Organisation 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 Organisation and the Home Organisation, this Code of Conduct and/or the data protection legislation, the following order shall prevail:

a. the agreement between the Home Organisation and the Service Provider Organisation;

b. applicable Data Protection Laws (such as other country specific law on Data protection or Privacy); and

c. the provisions of this Code of Conduct.

Appendix 1 provides a normative interpretation of the above principles.

ATTRIBUTE PROVIDERS

An Attribute Provider is an organisation other than the **Home Organisation** that manages extra **Attributes** for **End Users** of a **Home Organisation** and releases them to the **Service Provider Organisation**.

According to Section Functional Scope, the **Service Provider Organisation** and the communities representing the **Service Provider Organisation** can agree to apply the Code of Conduct also to other **Attributes**, such as those the **Service Provider Organisations** manage and share themselves. The organisation managing the extra **Attributes** becomes an Attribute Provider.

When the Code of Conduct is applied to **Attributes** managed by Attribute Providers, the **Service Provider Organisation** further agrees and warrants the following:

- (see clause H. Security Breaches) the **Service Provider Organisation** commits to report all suspected privacy or security breaches also to the Attribute Provider;
- (see clause L. Liability) the **Service Provider Organisation** agrees to hold harmless also the Attribute Provider who has suffered damage as a result solely of any violation of this Code of Conduct by the **Service Provider Organisation** as determined in a binding and enforceable judicial ruling;
- (see clause Q. Precedence) the **Service Provider Organisation** warrants to comply also 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 Organisation** and the Attribute Provider, the provision of the agreement concluded between **Service**

Provider Organisation and Attribute Provider takes precedence over the provision of this Code of Conduct.

APPENDIX 1: PRINCIPLES OF THE PROCESSING OF ATTRIBUTES

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

A. Legal compliance

The **Service Provider Organisation** warrants to only process the **Attributes** in accordance with: the relevant provisions of the GDPR, this Code of Conduct and a contractual agreement with the **Home Organisation**, if any.

The **Service Provider Organisation** shall ensure that all personal data processing activities carried out in this context comply with the GDPR.

The **Service Provider Organisation** 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 Organisation** established in the EEA territory, subject to the European Data Protection legislation, shall not find itself in a situation where their national data protection laws would contradict this Code of Conduct.

Service Provider Organisations 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 the laws of its jurisdiction. If observance of any provision of the Code of Conduct would place the **Service Provider Organisation** in breach of such laws, the national law of its jurisdiction shall prevail over such provision of the Code of Conduct, and compliance with national law to this extent will not be deemed to create any non-compliance by the **Service Provider Organisation** with this Code of Conduct.

The **Service Provider Organisation** based outside the EEA and countries offering adequate data protection commits to process the End User's **Attributes** in accordance with the GDPR, this Code of Conduct and any other contractual or other arrangements, such as the use of EU model clauses. Such **Service Provider Organisations** shall make binding and enforceable commitments to apply the appropriate safeguards, including as regards data subjects' rights[2], in addition to committing to abide by this Code of Conduct.

Service Provider Organisations that are International Organisations may be subject to their own internal rules, regulations and policies. Such International Organisations, which may not be subject to GDPR, shall make binding and enforceable commitments to apply appropriate safeguards.

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 Organisation** warrants that it will process **Attributes** of the **End User** only for the purposes of enabling access to the Service. The **Service Provider Organisation** commits not to process the **Attributes** for purposes other than enabling the **End User** to access the Service.

The **Service Provider Organisation** must ensure that **Attributes** are used only for enabling the **End User** to access the Service. See Appendix 3 for how this shall be interpreted.

The Attributes shall not be further processed in a manner which is not compatible with the initial purposes (Article 5.b of the GDPR). Processing of Attributes for any purpose other than enabling the End User to access the Service is outside the scope of this Code of Conduct.

Examples of purposes other than enabling access to the service (deviating purposes[3]) are: sending the **End User** commercial or unsolicited messages, including End User's e-mail address to a newsletter offering new services, selling the **Attributes** to third parties, transferring information to third

[2] In the event where an EU End User would lodge a complaint against a Service Provider Organisation based outside the EU (i.e. in the US), the competent European Data Protection Authority would be able to investigate on the alleged violation of data protection.

[3] Consult the Article 29 Working Party’s 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.

parties such as the search history, profiling activities etc.

C. Data Minimisation

The **Service Provider Organisation** commits to minimise the **Attributes** requested 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.

See Appendix 3 for how data minimisation is coupled with the purpose limitation (Clause B) and how it maps to the **Attributes** commonly available from the **Home organisations**.

In the context of this Code of Conduct, under no circumstances is a **Service Provider Organisation** authorised to request End User's **Attribute** 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. Information Duty Towards End Users

The **Service Provider Organisation** shall provide the **End User** with a publicly readable Privacy Notice before they initiate the federated login for the first time. This Privacy Notice must be concise, transparent, intelligible and provided in an easily accessible form. The Privacy Notice shall contain at least the following information:

a. the name, address and jurisdiction of the **Service Provider Organisation**; where applicable;

b. the contact details of the data protection officer, where applicable;

c. the purpose or purposes of the processing of the **Attributes**;

d. a description of the **Attributes** being processed as well as the legal basis for the processing;

e. 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;

f. the existence of the rights to access, rectify and delete the **Attributes** held about the End User;

g. the retention period of the **Attributes**;

h. the right to lodge a complaint with a Supervisory Authority.

The Privacy Notice 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 Notice shall use clear and plain language.

The Privacy Notice can be Service specific and does not need to be the same for different Services of a **Service Provider Organisation**.

The **Service Provider Organisation** needs to describe in its Privacy Notice how **End Users** can exercise their right to access, request correction and request deletion of their personal data.

The **Service Provider Organisation** 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 Organisation**.

The **Service Provider Organisations** are advised to make use of the Privacy Notice template that belongs to the supporting material of the Code of Conduct.

E. Information Duty Towards Home Organisation

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

a. a machine-readable link to the Privacy Notice;

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.

The technical infrastructure allows **Service Provider Organisations** to publicly announce their adherence to this Code of Conduct and to communicate its Service Privacy Notice's URL. When a **Service Provider Organisation** has several Service Privacy Notices, the URL of each Service Privacy Notice will be provided to the **Home Organisation**. This information is shared with the **Home Organisation**'s Identity Provider before it releases the End User's **Attributes** to the **Service Provider Organisation**, enabling the **Home Organisation** to present it to the End User.

F. Data Retention

The **Service Provider Organisation** shall delete or anonymize all **Attributes** without undue delay 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.

The retention period of the **Attributes** depends on the particularities of the Service and it needs to be decided by the **Service Provider Organisation**. However, a **Service Provider Organisation** shall not store the **Attributes** for an unlimited or indefinite period of time. The **Service Provider Organisation** 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's Privacy Notice (see clause D. Information Duty Towards End Users). In principle the personal 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 Organisation** 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 a significant period of time.

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 Organisation** shall implement appropriate processes to manage this type of situation. 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 source code control system (for example, git), 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 Organisation** is subject;
- for the performance of a task carried out in the public interest;
- for the establishment, exercise or defense of legal claims, such as resource allocation or invoices;
- for exercising the right of freedom of expression and information.

G. Security Measures

The **Service Provider Organisation** warrants taking appropriate technical and organisational measures to safeguard **Attributes** against accidental or unlawful destruction or accidental loss, alteration, unauthorised 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 Organisation** shall implement the security measures described in the Security Incident Response Trust Framework for Federated Identity (Sirtfi) and signal it to the **Identity Provider**.

H. Security Breaches

The **Service Provider Organisation** 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 to take the necessary technical and organisational measures for mitigating any risk the **Home Organisation** may be exposed to.

For example, if the **Service Provider Organisation** suspects that one or more user accounts in the **Home Organisation** has been compromised, the **Service Provider Organisation** 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 Organisation** shall use the security contact point of the **Home Organisation** or its Agent as provided in the technical infrastructure (currently, SAML 2.0 metadata), or an appropriate alternative, for the reporting.

I. Transfer of Personal Data to Third Parties

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

a. if mandated by the **Service Provider Organisation** for enabling the **End User** to access 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 Organisation** or;

c. if prior consent has been given by the End User.

The **Service Provider Organisation** shall not transfer **Attributes** to any third party (third party means a data controller other than the **Home organisation** or the Service Provider Organisation such as a collaboration partner) except:

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

b. if the third party is 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 where a research collaboration has a **Service Provider Organisation** that receives **Attributes** from **Home Organisations** and passes on (parts of) those **Attributes** to third parties providing the actual Services. In this case, where the **Service Provider Organisation** acts as a proxy for the third parties, the **Service Provider Organisation** must ensure that all third parties receiving **Attributes** are committed to the Code of Conduct or similar (such as a Data Processing Agreement or a Data Transfer Agreement).

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.

The organisation operating a proxy service, as described above, must act as 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 G. Security Measures.

c. if prior consent has been given by the **End User.** For the requirements of such consent, see clause K. End User's Consent.

If transfer to a third party includes also a transfer to a third country, the next clause imposes further requirements.

J. Transfer of Personal Data to Third Countries

The **Service Provider Organisation** guarantees that, when transferring **Attributes** to a party that is based outside the European Economic Area or in a country without an adequate level of data protection pursuant to Article 45.1 of the GDPR or the recipient is an International Organisation, to take appropriate safeguards (Article 46) or use the derogations pursuant to Article 49.

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 so-called *"appropriate safeguards"*:

- 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 Organisation** 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.

If the appropriate safeguards cannot be applied, Article 49 of the GDPR provides with an exhaustive list of *derogations* for the consideration of the Service Provider Organisation.

If transferring **Attributes** to a third country involves also a transferring them to a third party, also clause I. Transfer Of Personal Data To Third Parties needs to be satisfied.

K. End User's Consent

When consent is used, as per Article 7 of GDPR, inter alia, it must be freely given, specific, informed and must unambiguously indicate the End User's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of their personal data. Furthermore, the **End Users** shall be able to withdraw their consent.

When a **Service Provider Organisation** relies on End User's consent (e.g. clause I. Transfer of Personal Data to Third Parties, clause J. Transfer of Personal Data 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 privacy settings options of a software or another statement or conduct (i.e. a clear affirmative action) which clearly indicates the data subject's acceptance of the proposed processing of their personal data. Consent shall always be documented.

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

Notice that this Code of Conduct for **Service Provider Organisations** does not make normative requirements on the **Home Organisation**'s legal grounds to release **Attributes** to the **Service Provider Organisation**.

L. Liability

The **Service Provider Organisation** agrees to hold harmless the **End User and** the **Home Organisation** (as well as the Agent) who has suffered damage as a result solely of any violation of this Code of Conduct by the **Service Provider Organisation** 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, sharing the **Attributes** with third parties etc.), the **Service Provider Organisation** will hold the other parties harmless following a binding and enforceable judicial ruling.

For example, in case an **End User** files a complaint against their **Home Organisation** for unlawful release of **Attributes** after a **Service Provider Organisation** has released the **Attributes** to a third party, the **Service Provider Organisation** agrees to assume the liabilities of the **Home Organisation** towards the **End User** in respect of a breach of this Code of Conduct by the **Service Provider Organisation**.

A **Service Provider Organisation** shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

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 Data Protection Board or its predecessor[4], always notwithstanding any privileges and immunities of **Service Provider Organisations** being International Organisations, as these are awarded by their constituent and/or statutory documents and international law.

If there are any disputes regarding the validity, interpretation or implementation of this Code of Conduct, the parties shall agree on how and where to settle them.

This Code of Conduct shall be interpreted in the light of the GDPR and of guidance issued by the regulatory authorities such as the European Data Protection Board.

If there are disputes regarding the validity, interpretation or implementation of this Code of Conduct which cannot be settled amicably, the parties shall agree on how and where to settle them. For instance, if there is a dispute between a **Home Organisation** and **Service Provider Organisation** who are established in the same EU Member State, the parties can agree on using the local law and court. If the parties cannot come to an agreement, the Dutch laws and courts are assumed.

If at least one party to the dispute is an International Organisation, the dispute must be submitted to final and binding arbitration. In the absence

[4] 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.

of agreement over applicable arbitration rules, any dispute, controversy or claim arising out of or in relation to this Code of Conduct, or the existence, interpretation, application, breach, termination, or invalidity thereof, shall be settled by arbitration in accordance with the PCA Arbitration Rules 2012.

N. Eligibility

The Code of Conduct must be implemented and executed by a duly authorised representative of the **Service Provider Organisation**.

Each **Service Provider Organisation** must make sure that the commitment to this Code of Conduct is done by a person or by several persons (sometimes called a "signature authority") who has or have the right to commit the **Service Provider Organisation** to this Code of Conduct.

The person administering the Service that receives **Attributes** must identify the person or body in their organisation that can decide if the **Service Provider Organisation** commits to this Code of Conduct, as the Service administrator cannot necessarily take this decision on their own.

O. Termination of the Code of Conduct

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

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

Even after the **Service Provider Organisation** has terminated its adherence to the Code of Conduct, the **Attributes** received continue to be protected by the principles enshrined in this Code of Conduct (see clause P. Survival of the Code of Conduct).

P. Survival of the Code of Conduct

The **Service Provider Organisation** 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 until the processing terminates.

Q. Precedence

The **Service Provider Organisation** 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 Organisation** and the **Home Organisation**, the provision of the agreement concluded between **Service Provider Organisation** 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 Organisation** and the **Home Organisation**, this Code of Conduct and/or the data protection legislation, the following order shall prevail:

1. the agreement between the **Home Organisation** and the **Service Provider Organisation**;
2. applicable Data Protection Laws (such as other country specific law on Data protection or Privacy); and
3. the provisions of this Code of Conduct.

If a **Service Provider Organisation** 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 Organisation** to have a bilateral agreement overriding the Code of Conduct with some **Home Organisations**, meanwhile, this Code of Conduct will still apply to the other **Home Organisations** that have not entered into a bilateral agreement.

APPENDIX 2: GLOSSARY OF TERMS

Agent: the organisation operating the Identity Provider on behalf of the Home Organisation, if applicable.

Attribute(s): the End User's Personal Data as managed by the Home Organisation (or its Agent) and requested by the Service Provider Organisation, such as (but not limited to) name, e-mail and role in the Home Organisation.

Attribute Provider: an organisation other than the Home Organisation that manages extra Attributes for End Users of a Home Organisation and releases them to the Service Provider Organisations.

Data Controller: the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for their nomination may be designated by national or Community law

Data Processor: a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

EEA: European Economic Area.

End User: any natural person affiliated with a Home Organisation, e.g. as a researcher or student, making use of the Service of a Service Provider Organisation.

End User's consent: any freely given, specific, informed and unambiguous indication of the End Users wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.

Federation: an association of Home Organisations and Service Provider Organisations typically organised at national level, which collaborate for allowing cross-organisational access to Services.

Federation Operator: an organisation that manages a trusted list of Identity Providers and Services registered to a Federation.

GDPR: Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Home Organisation: the organisation with which an End User is affiliated, operating the Identity Provider by itself or through an Agent. It is responsible for managing End Users' identity data and authenticating them.

Identity Provider (IdP): the system component that issues Attribute assertions on behalf of End Users who use them to access the Services of Service Provider Organisations.

International Organisation: an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

Personal Data: any information relating to an identified or identifiable natural person.

Processing of personal data: any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Service: an information society service, in the sense of Article 1 point 2 of Directive 98/34/EC. This means any service provided, at a distance, by electronic means and at the individual request of a recipient of services.

Service Provider Organisation: an organisation that is responsible for offering the End User the Service they desire to use.

Supervisory Authority: an independent public authority responsible for monitoring the application of the GDPR and the national data protection legislations in order to protect the rights and freedoms of the data subjects in relation to the processing of their personal data.

APPENDIX 3: PURPOSE LIMITATION AND DATA MINIMISATION

Clause B requires that the **Service Provider Organisation** will process **Attributes** of the **End User** only for the purposes of enabling them to access the Service and Clause C requires that the **Attributes** must be adequate, relevant and not excessive for that purpose. This appendix discusses what enabling an **End User** to access a Service means and proposes some **Attributes** commonly available in **Home Organisations** that may serve the need.

Authorisation:

- **Description:** managing **End User's** access rights to Services provided by the **Service Provider Organisation** 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 an **End User** has self-asserted.
- Suggested Attributes:
  - eduPerson(Scoped)Affiliation
  - eduPersonEntitlement
  - schacHomeOrganisation

Identification:

- **Description: End Users** need to have a personal identifier with the **Service Provider Organisation** 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, an **End User** cannot self-assert their own identifier. Instead, the Identity Provider authenticates them and the **Home Organisation** (or Attribute Provider) provides the **Service Provider Organisation** with an **Attribute** that contains their authenticated identifier.
- Suggested Attributes:
  - a pseudonymous bilateral identifier (such as, SAML2 PairwiseID or PersistentID) is preferred;
  - if enabling access to the Service requires matching the same End User's accounts between two **Service Provider Organisations**, a **Service Provider Organisation** can request a more intrusive

identifier (such as SAML2 Subject ID, eduPersonPrincipalName or eduPersonUniqueID), whose value for a given user is shared by several **Service Provider Organisations**;

  - if there is a legitimate reason for an **End User** (such as a researcher) to keep their identity and profile in the **Service Provider Organisation** even when the organisation they are affiliated with changes, a permanent identifier (such as, ORCID identifier) can be used.

Transferring real-world trust to the online world:

- **Description:** if the **Service Provider Organisation** 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 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 Organisation**. The source of those **Attributes** is important; to avoid identity theft, the **Service Provider Organisation** must retrieve users' names from trustworthy sources and not rely on self- assertions.
- Suggested Attributes:
  - displayName
  - commonName, surName, GivenName

Researcher unambiguity:

- **Description:** 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[5]. There are global researcher identification systems (such as ORCID and ISNI) which assign identifiers for researchers to help scientific **Service Provider Organisations** to properly distinguish between researchers, even if they change their names or organisation they are affiliated with.
- Suggested Attributes:
  - eduPersonOrcid

Accounting and billing:

- **Description:** personal data can be processed for accounting (for instance, that the consumption of resources does not exceed the

[5] See Article 27(2) of the Universal Declaration of Human Rights.

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:

- **Description:** personal data can be processed to ensure the integrity, confidentiality and availability of the Service (e.g.: incident forensic and response). This requires collecting proper audit trail from the service.

Other functionalities:

- **Description:** Other functionalities offered by the **Service Provider Organisation** for enabling the **End User** to access the Service. 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 e-mail 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 on the End User's blog posting or edited their wiki page.

- **Suggested Attributes**:
    - mail