GÉANT Data Protection Code of Conduct

Explanatory memorandum
for the Article 29 Working Party

20th November, 2014

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007–2013) under Grant Agreement No. 605243 (GN3plus).

Contents

Summary 4
1. Context 6
1.1. Who we are 6
1.2. Access to research infrastructures 6
1.3. Federated Identity Management 8
1.4. The relationship triangle 9
1.5. Academic Identity Federations 10
1.6. eduGAIN interfederation service 11
2. Data protection directive requirements 12
2.1. Personal data (Article 2.a) 12
2.2. Data controller/data processor (Article 2.d,e) 12
2.3. Purpose of processing (Article 6.b) 12
2.4. Informing the End User (Article 11) 12
2.5. Relevance of Attributes (Article 6.c) 13
2.6. Keeping Attributes up-to-date (Article 6.d) 13
2.7. Legal grounds (Article 7) 14
Controller legitimate interests 14
Data subject consent 15
2.8. Security of processing (Article 17) 15
3. Requirements from the research and education sector 16
3.1. Scalability 16
3.2. Balance risk with the ease of collaboration 16
3.3. Sustain and recover from incidents and misbehaving entities 16
3.4. Minimise the risk of a Home Organisation's liability for a Service Provider's misbehaviour and vice versa 16
3.5. Suggest good practices to the Home Organisations 17
3.6. Minimise the Federation Operator's role 17
3.7. The importance of a global approach 18

4. GÉANT Data Protection Code of Conduct 18
4.1. Goal and approach 18
4.2. Supporting documents 19
4.3. Supplementary tools 20
5. Geographical/jurisdiction considerations 21
5.1. Attribute release to EU/EEA or country with adequate protection 21
5.2. Attribute release to a third country 22

Appendix A: GÉANT Data Protection Code of Conduct
Appendix B: GÉANT Data Protection Code of Conduct (French translation)

Summary

Modern research is highly cross-national and collaborative. Researchers in thousands of research organisations access services in other organisations using electronic means. GÉANT develops and operates a pan-European e-infrastructure for authentication, authorisation and single sign-on for researchers (or "End Users") in research and education organisations in Europe.

The e-infrastructure provides researchers with easy access to cross-national research infrastructures without the use of extra credentials, such as usernames and passwords. Accessing the research e-infrastructure requires sharing some of a researcher's personal data from his/her research or education organisation (or "Home Organisation") to the service provider he/she is accessing in another member state or beyond (or "Service Provider").

For Home Organisations to share End Users' personal data with Service Providers, they must comply with relevant data protection legislation. However, the lack of scalable, practical compliance guidelines has caused e-infrastructures in different member states to adopt fragmented practices for personal data release, which is hindering cross-national access to services.

Discomfort about data protection compliance has also led to an approach where, to be cautious, Home Organisations do not share End Users' personal data with the Service Provider. As a consequence, End Users need to register and create separate credentials for each service, undermining the reliability of the credentials, inhibiting access to services, causing administration overheads and resulting in less efficient pan-European academic research.

GÉANT, as a cross-border European academic research and education e-infrastructure, drafted a pan-European Code of Conduct to facilitate the application of the data protection principles stemming from the Data Protection Directive, taking account the specific characteristics of the processing carried out in the academic sector, and respecting the national provisions adopted by member states.

The attached GÉANT Data Protection Code of Conduct proposes a scalable approach to protect the End User's personal data when he/she logs in to a service provided by another organisation. 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.

A formal endorsement of the pan-European Code of Conduct by the Article 29 Working Party would enhance the credibility of the Code of Conduct.

1. Context

1.1. Who we are

GÉANT[1] is the pan-European research and education backbone network that interconnects Europe's National Research and Education Networks (NRENs). Together with its national partners (the NRENs), the GÉANT network offers network connectivity and associated services (such as, an e-infrastructure for electronic identity) to over 10 000 research and education institutions in 42 countries, including all EU member states.

The GÉANT network is developed and operated by the GÉANT project (GN3plus), which receives funding from the Seventh Framework Programme of the European Commission. The project is coordinated and the network is operated by GEANT Limited (formerly Delivery of Advanced Network Technology to Europe (DANTE)[2]), a limited liability company and a not-for-profit organisation that is part of the GÉANT Association[3], the leading collaboration on network and related infrastructure and services for the benefit of research and education.

As the coordinator of the GÉANT project, GEANT Limited has submitted this Code of Conduct to the Article 29 Working Party, on behalf of the GÉANT project partners.

1.2. Access to research infrastructures

The success of the European economy is increasingly dependent on scientific and technological innovation. The European Research Area (ERA) was launched at the Lisbon European Council in March 2000. The development of ERA is needed to overcome the fragmentation of research in Europe along national and institutional barriers.

According to the EC's vision of the ERA, *major infrastructures should be built and exploited in the form of joint European ventures. They should be accessible to research teams from across Europe and the world, with researchers working in Europe having access to international infrastructures and equipment in other parts of the world. These research infrastructures should be integrated, networked and accessed*

[1] http://www.geant.net/

[2] http://www.dante.net/

[3] http://www.geant.org/

through the concomitant development of new generations of electronic communication infrastructures (also known as "e-infrastructures")*, both in Europe and globally.*[4]

In the strategy report on the European Research Infrastructure roadmap,[5] ESFRI identified 44 research infrastructure projects from the broad disciplines of social sciences and humanities, environmental science, energy, biological and medical sciences, materials and analytics facilities, and physical sciences and engineering. The construction costs of the individual projects are between EUR2 M and EUR2100 M, and annual operation costs range from EUR2 M to EUR120 M. In 2010, ten projects had entered the implementation phase. Many of the research infrastructures rely on the availability of secure and reliable e-infrastructures.

For security reasons, researchers usually need electronic identities for authentication and verification of access rights before they can access the research infrastructure. In its communication on the ERA[6] in 2012, the European Commission invites the member states to *adopt and implement national strategies for electronic identity for researchers giving them transnational access to digital research services* and research stakeholder organisations, to *implement and promote the uptake of electronic identity and digital research services.* The ERA communication also reflects the 2010 Digital Agenda for Europe, whose Key Action 3 calls for a framework for *cross-border recognition and interoperability of secure eAuthentication systems.*[7]

Without a proper e-infrastructure for electronic identities, the ERA researchers need to manage credentials for thousands of services, inhibiting effective co-operation and research and creating administrative burdens. To provide an e-infrastructure for secure authentication, authorisation and single sign-on of researchers and other End Users, a new approach, **Federated Identity Management**, has been introduced, which is described in the next section.

---

[4] European Commission. The European Research Area: New perspectives. Green Paper 4.4.2007.

[5] European Strategy Forum on Research Infrastructures. Strategy Report on Research Infrastructures. Roadmap 2010.

[6] European Commission. A Reinforced European Research Area Partnership for Excellence and Growth. COM(2012) 392, 17.7.2012.

[7] European Commission. A Digital Agenda for Europe. COM(2010) 245, 26.8.2010.

1.3. Federated Identity Management

Federated Identity Management is crucial to the ability of e-Infrastructures to operate in a scalable, secure manner. In order to operate, however, Federated Identity Management requires a trust framework to exchange some of the researcher's personal data.

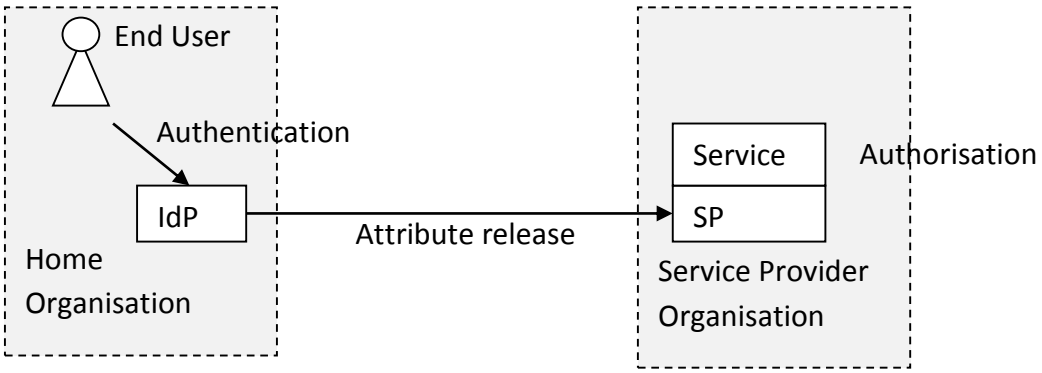

Figure 1. The basic actors in Federated Identity Management and their division of responsibility.

The basic division of responsibility is presented in Figure 1. **End Users** are researchers, teachers, students and other natural persons affiliated to a university, research institution or other Home Organisation. **Home Organisations** (such as universities and research institutions) are responsible for managing their End Users' personal data (called *Attributes*, such as name, e-mail address and role/position in the Home Organisation) and for delivering credentials (such as usernames and passwords) to allow identified access to local and federated services. At the moment when an End User accesses a Service Provider, his/her Home Organisation authenticates him/her using such credentials. The authentication is performed by an **Identity Provider** server (IdP) that the Home Organisation operates.[8] After authenticating the End User, the Identity Provider delivers the End User's Attributes to the **Service Provider** server (SP) the End User is accessing. The Attribute delivery takes place at the time when the End User accesses the service. Based on the Attributes, the Service Provider decides if the End User is entitled (authorised) to use the **Service**, and assigns him/her to his/her existing profile in the Service, if any.

[8] The Identity Provider server can be operated by the Home Organisation or the Home Organisation can outsource it. In some countries, the federation operator operates a centralized Identity Provider for the Home Organisations.

By virtue of the Federated Identity Management, the End User only needs a single set of credentials to access all Service Providers, and can enjoy a single sign-on experience. Service Providers do not need to maintain End Users' credentials, and are able to receive End Users' up-to-date and reliable attributes from their Home Organisations. When an End User departs, the Home Organisation closes his/her account, and access to the research infrastructures ceases.

1.4. The relationship triangle

From a data protection perspective, there are three parties and three relationships involved (see Figure 2).

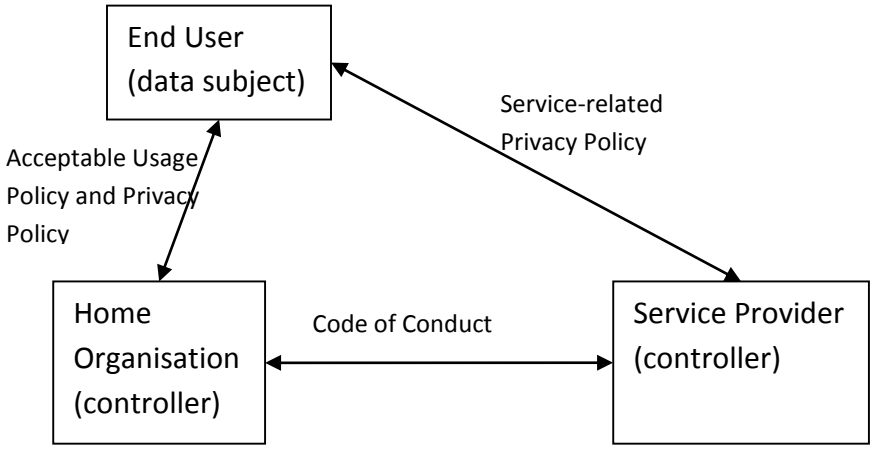

Figure 2. The triangle of relationships involved in Federated Identity Management.

The Home Organisation processes the End User's personal data to carry out its duties as an employer, to provide teaching to a student, or to fulfil other tasks of the institution. The relationship between the End User and the Home Organisation is governed by an **Acceptable Usage Policy** (typically including or linked to a privacy policy), to which the End User commits at the start of his/her employment, studies, or other relationship in his/her Home Organisation, and receives his/her username and password from the Home Organisation.

The Home Organisation delivers the End User's Attributes to the Service Provider to enable the researcher or student to conduct research, take courses, etc. The relationship between the End User and the Service Provider is set by the Service Provider's purpose of data processing and is documented in the Service Provider's service-related **Privacy Policy**.

In some circumstances, the Home Organisation and Service Provider may have a bilateral agreement that also addresses protection in the End User's personal data.

However, to guarantee a baseline for data protection in the instances where there is no bilateral agreement, the **Code of Conduct** helps the Service Provider to engage with the Home Organisations on data protection practices.

1.5. Academic Identity Federations

The federated approach to identity management presented above suffers from scalability problems when End Users from thousands of Home Organisations need to access thousands of Service Providers. To address this issue with scalability, e-infrastructures called *Identity Federations* have been established in the research and higher education sector since 2005.

Today, academic Identity Federations are nationally focused and typically organised by NRENs, the non-profit organisations providing Internet connectivity and associated services to researchers, teachers and students in the institutions. Currently, there are 23 academic Identity Federations[9] in EU member states. In November 2014, those federations had a total of 2738 IdP and 3395 SP servers registered.[10]

The role of the **Identity Federation** (Figure 3) is to set the rules for its **Members** (i.e. Home Organisations and Service Provider Organisations), such as the eligibility to join the federation, minimum requirements for strength of End User authentication, liability, technical specifications, etc. The Identity Federation also nominates an organisation to be responsible for operations of the federation. The **Federation Operator** (typically, the NREN) takes care of day-to-day issues, such as registering Members' Identity and Service Provider services to the federation, providing technical support to the Members, etc.

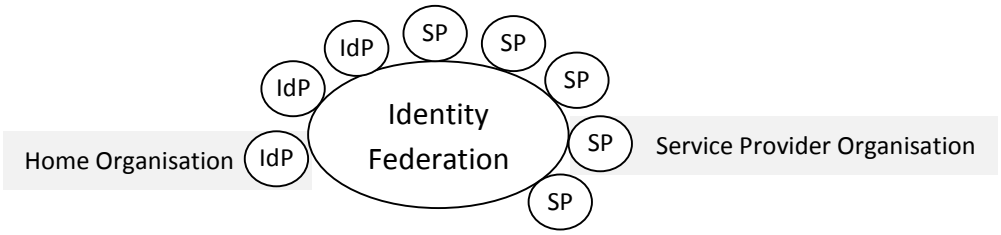

Figure 3. An Identity Federation is an e-infrastructure service that allows Identity Provider (IdP) servers (managed by End Users' Home Organisations) and Service Provider (SP) servers (managed by SP organisations) to exchange Attributes on authenticated End Users.

[9] TERENA Compendium of National Research and Education Networks in Europe, 2014 edition https://compendium.terena.org/reports

[10] https://met.refeds.org/met

Typical services to which academic Identity Federations provide authentication and authorisation are scientific journals and other licensed content (such as university libraries' electronic magazine subscriptions for researchers), e-learning (teachers' virtual learning tools to support their teaching), collaboration (wikis and fileshares for cross-organisation workgroups) and SaaS services (universities' outsourcing of administrational services to the private sector). Recently, however, Identity Federations have started to face increasing demand to support multinational research infrastructures. This has created the need to bridge the formerly national federations into a cross-national interfederation service called eduGAIN.

1.6. eduGAIN interfederation service

The eduGAIN service[11] (delivered by the EC-funded GÉANT GN3plus project) connects the national academic federations into an interfederation service (see Figure 4). Within their Home Organisation, End Users can use their local usernames and passwords to access Service Providers in another Participant Federation (countries).

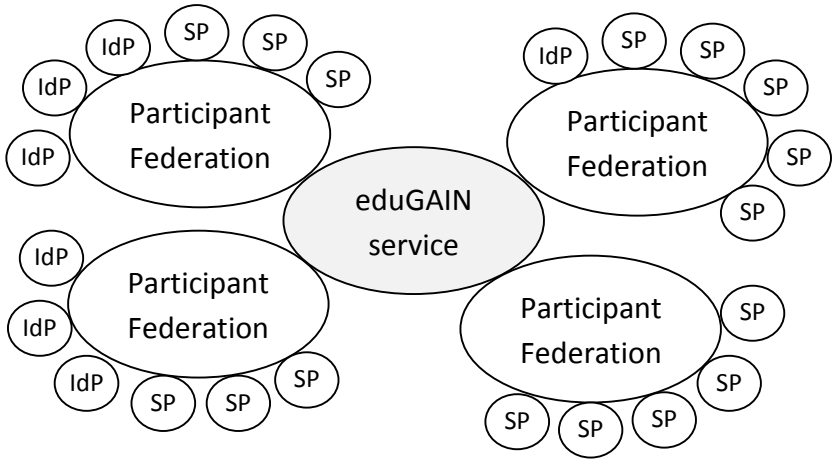

Figure 4. eduGAIN interfederation service connects its participants and allows a direct exchange of Attributes between Identity Providers (IdP) and Service Providers (SP).

The technical architecture is distributed as shown in Figure 4. eduGAIN mediates IdPs' and SPs' technical descriptions (such as the address of the server endpoints and their trusted certificates) between the Participant Federations. There is no single proxy server that channels the entire message exchange in eduGAIN. Any release of personal data takes place directly between the IdP and SP.

[11] http://www.edugain.org/

The eduGAIN interfederation service establishes a pan-European e-infrastructure for electronic identity in the ERA. It eases co-operation of researchers and other End Users throughout Europe and reduces the administrative burden needed to access research infrastructures. eduGAIN also supports the European single market introduced in Article 3 of the Treaty on European Union, and is interconnected with similar e-infrastructures in other parts of the world.

2. Data protection directive requirements

This section summarises the interpretation of service-specific requirements that eduGAIN derives from Directive 95/46/EC.

2.1. Personal data (Article 2.a)

Typical Attributes released to the Service Provider by a Home Organisation include: the End User's online identifier (if possible, pseudonomised), name and email address. It is often necessary to also release Attributes describing the End User's relationship to the Home Organisation, such as the name of the Home Organisation and the organisational unit the End User is affiliated to, and his/her role in the Home Organisation (e.g. student, researcher, member, library walk-in, etc). In some cases, there is a requirement to exchange more sophisticated Attributes, e.g. those based on a person's entitlement to use a specific resource. Such Attributes, alone or together, qualify as personal data.

2.2. Data controller/data processor (Article 2.d,e)

At least the Home Organisations and Service Providers, but also possibly the federations and eduGAIN, qualify as data controllers. It is possible that the Home Organisation and Service Provider are considered joint data controllers.

2.3. Purpose of processing (Article 6.b)

In the context of Federated Identity Management, the purpose of processing personal data is to share necessary (but not excessive) personal data on the End User from his/her Home Organisation to the Service Provider, in order for the Service Provider to be able to provide access to the service for eligible End Users.

2.4. Informing the End User (Article 11)

According to the Code of Conduct, Service Providers are obliged to publish a prominent link to the service's privacy policy in the service's landing page. End Users have an opportunity to study the privacy policy before they log in and their Attributes are released from the Home Organisation to the Service.

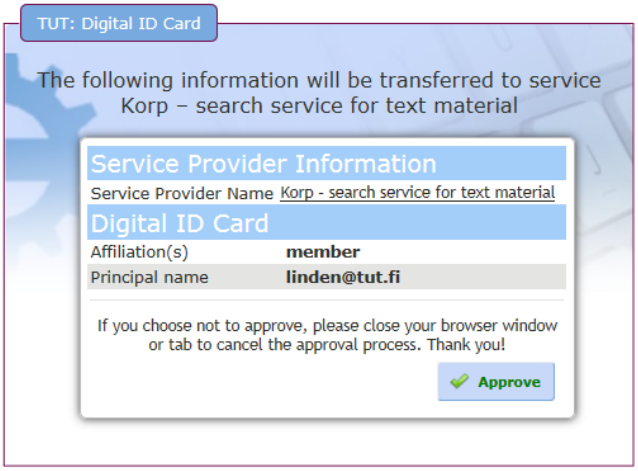

Figure 5. Example of how a Home Organisation should inform End Users and provide an opt-out opportunity before Attributes are released to a new Service Provider. Clicking the Service Provider Name leads to its Privacy policy page.

Additionally (see Figure 5), it is recommended that the Home Organisations ensure that their duty to inform the End User is fulfilled by providing End Users with the service's name, description, clickable privacy policy link and requested Attribute names and values before the Attribute release takes place for the first time.

2.5. Relevance of Attributes (Article 6.c)

The Service Provider has service expertise as well as understanding of the Attribute requirements of the service. For reasons of scalability, the Code of Conduct proposes an approach where the Service Provider publishes a list of its Attribute requirements and takes full responsibility to ensure Attributes are adequate, relevant and not excessive, in relation to the purpose of processing. Alternatively, the Service Provider can assign the service to a category of similar services, such as, "Research and Scholarship", with an associated list of Attributes typical for those services. Home Organisations are expected to respect that list.

2.6. Keeping Attributes up-to-date (Article 6.d)

It is assumed that the Home Organisation, which has a close relationship to the End User, is well placed to ensure that End Users' Attributes are kept up-to-date. Therefore, the Attributes are periodically refreshed from the Home Organisation to the Service Provider, commonly every time the End User logs in to the service. The End User should contact his/her Home Organisation to rectify these Attributes, if necessary.

However, many Service Providers also want to maintain some additional personal data in the service (for example, the End User's preferences in that particular service). The Service Provider's Privacy policy instructs the End User how to rectify this data.

2.7. Legal grounds (Article 7)

Controller legitimate interests

Reliance on the notion of legitimate interests legal grounds (Article 7.(f)) is generally justified for both Home Organisations and Service Providers.

Taking into account the WP 29 Opinion 06/2014 on the notion of legitimate interests of the data controller, we note the following:

Home Organisations and Service Providers both have an interest in ensuring the services offered by Service Providers are available and accessible to all End Users in a way that limits the administrative burden for End Users. Indeed, Home Organisations and Service Providers have an interest in avoiding a situation where the procedure to gain access to the services becomes an impediment to the actual use of the service.

We note that this interest (i) is lawful and not contrary to applicable EU and national laws; (ii) is clearly articulated; and (iii) represents a real and present interest for the Home Organisations and Service Providers; and as such, **constitutes a "legitimate interest"** in the sense of article 7.f of the Directive.

Furthermore, we note that the Attribute-release mechanism, as described above, is indeed **necessary** to achieve the interest pursued. There are no reasonably workable, less-invasive means to reach the identified purpose of the processing.

In general, it is believed that there are **no overriding fundamental interests or rights** of End Users that would prevent reliance on the legitimate interests legal ground, because a.o.

- The interest of the controllers, providing the End User with the service he/she has requested in an easily accessible manner, coincides with a wider, public interest, i.e. fostering scientific and technological innovation.
- Without the processing taking place, Service Providers would not be able to provide access to the service for eligible End Users.
- While it is assumed that all Attributes qualify as personal data, we consider the actual information being exchanged (name, role, email address) and the types of services and content accessed by the end uses (mainly scientific) to be innocuous, in particular, when Attributes would be (partially) pseudonomised.
- The impact on End Users is very limited, compared to the benefit the system brings to End Users as well as Home Organisations and Service Providers.

- Furthermore, **additional safeguards** will be implemented, including the following: A design goal of Federated Identity Management and the Code of Conduct is to protect the privacy of End Users and to minimise the amount of data being exchanged. Instead of having End Users directly provide credentials to Service Providers, the Home Organisations will channel the data exchange through Identity Provider servers.
- The Code of Conduct fully supports the aim of privacy protection and data minimisation. For example, Service Providers must explicitly indicate which End User Attributes are required through the technical infrastructure, and will not receive any additional information. Furthermore, pseudonymisation will be used, when possible.

Data subject consent

In addition to the release of *necessary* attributes based on the legitimate interests grounds, in future, there are plans to extend the Code of Conduct, to provide an End User with an opportunity to provide informed consent (Article 7.(a)) to the release of *necessary* Attributes for additional purposes, and to the release of *extra* Attributes in exchange for added value services. For instance, if the End User wants to subscribe to a regular newsletter on service updates, he/she can consent to the Home Organisation's release of his/her e-mail address to the Service Provider.

2.8. Security of processing (Article 17)

The technical specifications used in federations[12] recommend that message or transport layer encryption is used to ensure the confidentiality of the Attributes when transmitted over the network to the Service Provider. The integrity of the Attributes is guaranteed by mandatory digital signatures created by the Identity Provider server. Confidentiality and integrity is supplemented by registering the Identity and Service Provider servers' trusted certificates. Additionally, the Service Providers are expected to ensure the security of their software installations and configurations.

The distributed architecture of eduGAIN has no central points that would be able to examine the Attribute exchange between the Identity and Service Provider.

[12] Currently, most federations make use of the SAML 2.0 standard (Security Assertion Mark-up Language) and the SAML2int profile derived from it.

3. Requirements from the research and education sector

This section presents the requirements for the GÉANT Data Protection Code of Conduct from the Research and Education (R&E) sector in Europe and beyond.

3.1. Scalability

The Code of Conduct should scale to the size where hundreds or thousands of Service Providers and Home Organisations exchange End User Attributes. Bilateral negotiations and/or contracts between each Home Organisation and Service Provider will not adequately fulfil this requirement.

3.2. Balance risk with the ease of collaboration

The Code of Conduct should find an appropriate balance between minimising the data protection risks and enabling easy collaborations for End Users in different Home Organisations.

However, the Code of Conduct does not preclude a Home Organisation entering bilateral negotiations with a Service Provider in the case where the safeguards offered by the Code of Conduct are not sufficient e.g. for particularly sensitive work.

3.3. Sustain and recover from incidents and misbehaving entities

In an ideal world, all parties would meet their respective data-protection-related requirements, and all parties would be able to assume that all other parties will also meet their data-protection-related responsibilities. There would be no security incidents; no End Users would think that their privacy has been breached. In practice, however, that world does not exist. It is necessary to develop a design that provides all parties with sufficient assurance that other parties with which they interoperate are aware of and meet their data-protection-related responsibilities, and that all parties are able to tolerate and recover from incidents and misbehaving entities.

3.4. Minimise the risk of a Home Organisation's liability for a Service Provider's misbehaviour and vice versa

In general, it is the role of a Home Organisation to release Attributes to a Service Provider when the Attribute release supports its End User's research, teaching and study-related activities. However, if it turns out that the Home Organisation may become liable for a data protection problem caused by a Service Provider, the Home Organisations may become hesitant and refrain from their role as an Identity Provider (and *vice versa*). Instead, the End Users would need to self-register and learn local

usernames and passwords, which would defeat the benefits of Federated Identity Management.

Thus, it is important that the Code of Conduct clearly allocates responsibility for compliance with data protection rules and responsibility for possible breach of these rules to Home Organisations and Service Providers. It must be avoided that there is (a) a loophole where not all obligations imposed by the Directive are covered by a party; or (b) a situation where a party can be held liable for another party's misbehaviour.

The Code of Conduct must therefore provide a clear and effective allocation of obligations and responsibilities between all parties.

3.5. Suggest good practices to the Home Organisations

The intention of the Code of Conduct is to reduce Home Organisations' hesitation to release Attributes to the Service Providers by providing a tool to support risk analysis. This is achieved by clearly documenting behavioural rules for Service Providers. The rules enable the Home Organisation to decide whether it is safe to release personal data to the Service Provider. It should be noted that this only applies to the Home Organisation's release of data to the Service Provider. The Code of Conduct is a Code of Conduct for *Service Providers*, not for Home Organisations. The Code of Conduct may introduce good practices that can help a Home Organisation to reduce its data-protection-related risks, but if the Home Organisation decides to ignore them, it is first and foremost the Home Organisation, not the Service Provider, that is exposed to risk.

3.6. Minimise the Federation Operator's role

The Attribute exchange takes place between the Home Organisation and the Service Provider. In most academic Identity Federations, the Federation Operator is not involved in the transaction.[13] The Code of Conduct therefore does not cover the federation operator's liability for data protection issues caused by the Home Organisation or the Service Provider.

[13] In some countries, the Federation Operator operates a centralised Identity Provider on behalf of the Home Organisations. In those countries, the Federation Operator is involved in the transaction as a data processor.

3.7. The importance of a global approach

The R&E community is global, and research collaborations cross national and federation borders. The approach adopted should be applicable globally, or at least as widely as possible.

4. GÉANT Data Protection Code of Conduct

This section presents how the approach presented in the previous section is put into practice in the GÉANT Data Protection Code of Conduct, and describes the framework developed to supplement its use. The proposed Code of Conduct may be found in Appendix A.

4.1. Goal and approach

The EU member states' 20 academic Identity Federations have been developed independently, with fragmented approaches to data protection issues often primarily embedded in specific national laws. A goal of the Code of Conduct is to

(i) Seek for a pan-European interpretation and good practice approach for the issues related to data protection in Federated Identity Management in research and education, and
(ii) Promote pan-European interpretation and practice to eduGAIN Participant Federations, in order to reduce obstacles hindering cross-national access to research infrastructures.

These requirements do not seek to replace or reduce requirements of specific data protection regulation for e-Infrastructures and parties involved in federated identity. Rather, the aim of the Code of Conduct is to identify and highlight key aspects for the R&E community in a scalable way.

The Code of Conduct covers issues related to the protection of the End User's personal data received from his/her Home Organisation when he/she accesses the service. The Code of Conduct does not cover data protection issues related to the content of the service, such as, how biological research data can be shared for research purposes if it contains potentially sensitive patient data.

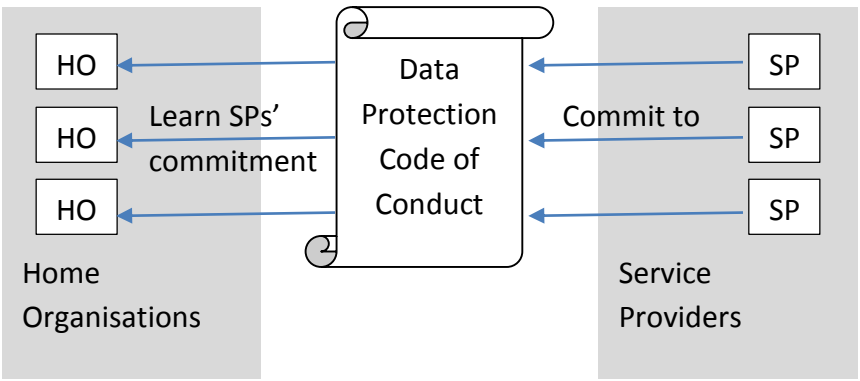

Figure 6. Service Providers (SP) commit to the Data protection Code of Conduct. Home Organisations (HO) learn the Service Providers' commitment by the indications relayed by the Identity Federation(s).

The intention (depicted in Figure 6) is that the Service Provider commits to the Code of Conduct, the Identity Federations (and the eduGAIN interfederation service) relay an indication of the commitment to the Home Organisations, who then make the decision about releasing Attributes to the Service Providers.

A pilot on the Code of Conduct has been started within the eduGAIN community. In November 2014, 37 Service Providers have expressed their commitment to the Code of Conduct, most of them in the disciplines of linguistics, the arts and humanities.

Although designed for the eduGAIN interfederation service, it is intended that the Code of Conduct can also be used locally within the national Identity Federations.

4.2. Supporting documents

The eduGAIN project has developed extensive additional material[14] to support Service Providers, Home Organisations and Identity Federations in adopting the Code of Conduct.

The normative documents consist of the Code of Conduct (Appendix A) and technical specifications on how to use the SAML 2.0 standard to convey information on Service Providers' commitment to the Code of Conduct to the Home Organisations in the most reliable way. The technical specifications also describe how the Service Provider server presents to the Identity Provider server the link to its privacy policy page and the list of Attributes it requests from the Home Organisation. This information is sufficient for the Home Organisation to configure its Identity Provider server to inform the End User of

[14] https://wiki.refeds.org/display/CODE

the Attribute release, and to release a limited Attribute set to Service Providers without administrational involvement, for each Service Provider.

In addition to the Code of Conduct, the normative documents are complemented with guidelines and good practice:

- **How to develop a privacy policy document.** Although obliged by the directive and national laws, practice has shown that many Service Providers have problems in developing an appropriate privacy policy document for their service. A practical template is provided to assist the Service Providers.
- **How to assess what Attributes are relevant for a Service Provider.** This guideline assists Service Providers' decision-making process regarding what Attributes they can reasonably request from the Home Organisations under the Code of Conduct.
- **Good practices for a Home Organisation to release Attributes.** Good practice, for instance, suggests that a Home Organisation informs the End User before the Attribute release (see Figure 5 on page 13) and proposes that a Home Organisation develops a maximum list of Attributes to release under the Code of Conduct, based on risk assessment.
- **Guidelines for Identity Federations.** The guideline describes how the Identity Federations are expected to record a Service Provider's commitment to the Code of Conduct and to convey it to the Home Organisations.
- **How to handle Service Provider's non-compliance to the Code of Conduct**. This guideline suggests enforcement actions if someone (such as, an End User, Home Organisation or Federation operator) believes a Service Provider is not complying with the Code of Conduct, even though it has committed to it.
- **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 (see Figure 5 on page 13).
- **A Code of Conduct cookbook** with recipes for Service Providers, Home Organisations and federation operators. The recipes provide step-by-step guidance on how to deploy the Code of Conduct.

4.3. Supplementary tools

As the operator of the eduGAIN interfederation service, the GÉANT project runs a monitoring service[15] of all Service Providers that have expressed commitment to the

[15] http://monitor.edugain.org/coco

Code of Conduct. The monitoring tool performs some technical basic checks to the Service Providers to make sure they have published a privacy policy document and the list of necessary Attributes that Home Organisations need to release. The tool provides a page where Service Provider administrators can check their technical conformance (see Figure 7).

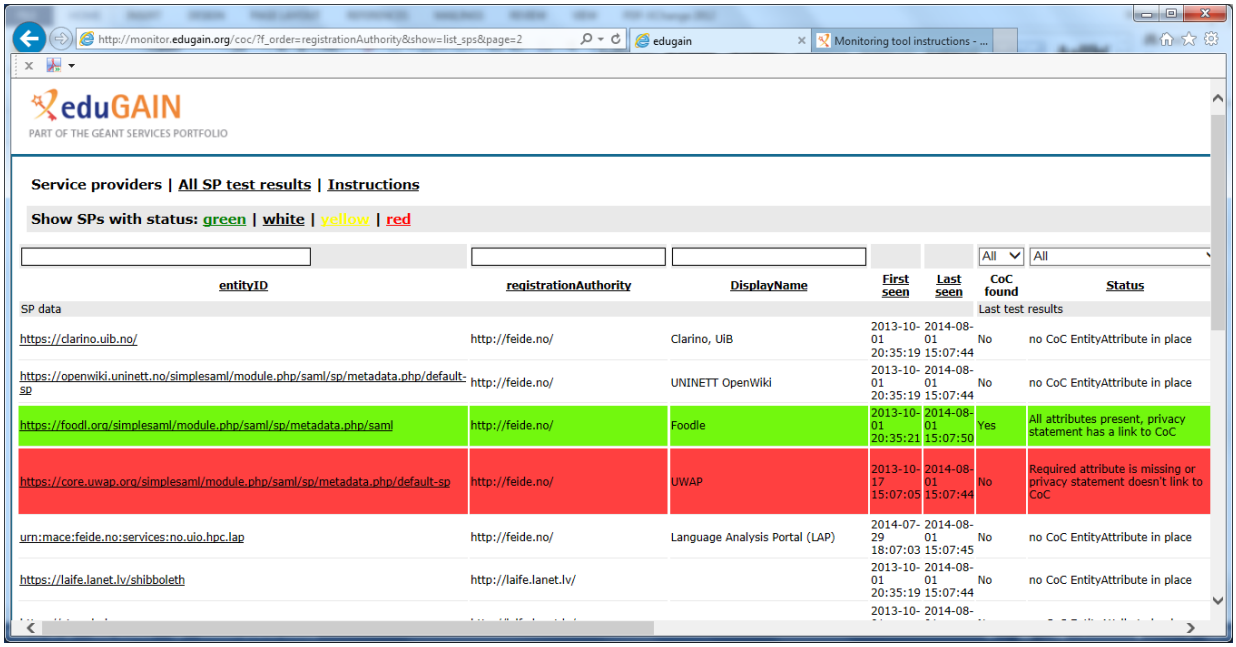

Figure 7. A Code of Conduct monitoring tool helps Service Provider administrators to ensure their technical conformance. Green line indicates the SP is OK, red indicates a problem. White SPs have not committed to the Code of Conduct.

The monitoring tool also periodically archives the monitoring results and the Service Providers' Privacy policy documents for audit trail, in case of a later dispute.

5. Geographical/jurisdiction considerations

Initially, eduGAIN only provided interfederation services to federations in Europe. However, as mentioned in Section 1 and 3.7, research is global, and there is a need to exchange Attributes with data controllers outside the EU/EEA.

5.1. Attribute release to EU/EEA or country with adequate protection

According to the basic scenario, both the Service Provider and Home Organisation are established in an EU/EEA country or in a country or arrangement that ensures adequate protection, as defined in Article 25 of the Directive. In this case, the Code of Conduct is a binding document which:

- indicates the Service Provider is aware of its legal obligation to protect personal data,
- limits the data protection risks of the Home Organisation that releases Attributes to the Service Provider, and
- divides responsibility between the Home Organisation and the Service Provider in a scalable manner.

The Code of Conduct can be seen as a unilaterally binding declaration the Service Provider makes as part of its data protection practices towards all Home Organisations whose End Users are welcome to use the service.

5.2. Attribute release to a third country

If the Service Provider resides in a country which does not ensure adequate protection ("third country"), the Code of Conduct should be used together with the Standard Contractual Clauses.[16] In that scenario, the Service Provider (outside EU/EEA) and the Home Organisation (in EU/EEA) commit, respectively as a data importer and as a data exporter, to the Code of Conduct combined with the Standard Contractual Clauses (Figure 8).

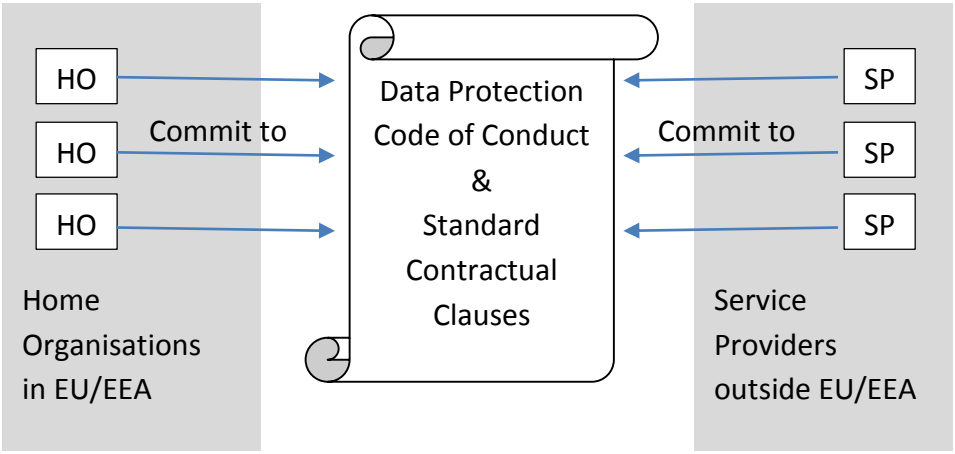

Figure 8. Code of Conduct in combination with Standard Contractual Clauses to enable Attribute release to third countries.

The proposed approach would form a multilateral agreement, where several Home Organisations and several Service Providers are committed to the same contractual terms. Via the multilateral agreement, each Home Organisation and Service Provider

[16] Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

has a direct contractual relationship with each other. However, each Service Provider and Home Organisation needs to commit to the charter only once, fulfilling the scalability requirement presented in Section 3.1.

GÉANT Data Protection Code of Conduct

For Service Providers established in European Union, European Economic Area and countries with adequate data protection pursuant to Article 25.6 of the directive 95/46/EC

GN3-12-215

Document URI:
http://www.geant.net/uri/dataprotection-code-of-conduct/v1

Version 1.0, 14 June 2013

Purpose and Context

Without prejudice to the provisions as set forth in the agreement between the Home Organisation and 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 providing access to their services. This Code of Conduct is a binding community code for the Service Providers that have committed to it.

The work leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007-2013) under Grant Agreement No. 238875 (GÉANT).

1 Definitions

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

b) Service Provider (SP): An organisation that is responsible for offering the End User the service he or she desires to use.

c) 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.

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

e) Attributes: The End User's personal data as managed by the Home Organisation or its Agent, such as (but not limited to) name, e-mail and role in the Home Organisation.

f) 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.

g) Personal Data: any information relating to an identified or identifiable natural or legal person, if applicable.

2 Principles of Attributes Processing

The Service Provider agrees and warrants:

a) **[Legal compliance]** to only process the Attributes in accordance with the relevant provisions of the Personal Data protection law applicable to the Service Provider;

b) **[Purpose limitation]** to only process Attributes of the End User that are necessary for enabling access to the service provided by the Service Provider;

c) **[Data minimisation]** 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;

d) **[Deviating purposes]** not to process the Attributes for any other purpose (e.g. selling the Attributes or selling the personalisation such as search history, commercial communications, profiling) than enabling access, unless prior consent has been given to the Service Provider by the End User;

e) **[Data retention]** to delete or anonymise all Attributes as soon as they are no longer necessary for the purposes of providing the service;

f) **[Third parties]** not to transfer Attributes to any third party (such as a collaboration partner) except

   a. if mandated by the Service Provider for enabling access to its service on its behalf, or

   b. if the third party is committed to the Code of Conduct or has undertaken similar duties considered sufficient under the data protection law applicable to the Service Provider or

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

g) **[Security measures]** to take 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.

h) **[Information duty towards End User]** to provide to the End User, at least at first contact, in an easily, directly and permanently accessible way a Privacy Policy, containing at least the following information:

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

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

   c. a description of the Attributes being processed;

   d. 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;

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

   f. the retention period of the Attributes;

   g. a reference to this Code of Conduct;

i) **[Information duty towards Home Organisation]** 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 updates or changes in the local data protection legislation, which are less strict than the principles set out in this Code of Conduct;

j) **[Security Breaches]** to, without undue delay, report all suspected privacy or security breaches (including unauthorized disclosure or compromise, actual or possible loss of data, documents or any device, etc.) concerning the Attributes to the Home Organisation or its Agent;

k) **[Liability]** 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;

l) **[Transfer to third countries]** when Attributes are being transferred outside the European Economic Area and countries with adequate data protection pursuant to Article 25.6 of the directive 95/46/EC, to ensure an adequate level of protection of the Personal Data by taking appropriate measures pursuant to the law of the country in which the Home Organisation is established, such as requesting End User consent or entering into agreements with the Home Organisation based on EU model clauses;

m) **[Governing law and jurisdiction]** to have this Code of Conduct governed by the national material law of the country in which the Service Provider is established with the exclusion of its international private law and to have any disputes regarding the validity, the interpretation or the implementation of this Code of Conduct definitively decided by the competent court of the country in which the Service Provider is established;

n) **[Eligibility to execute]** to have this Code of Conduct executed by a duly authorised representative of the Service Provider;

o) **[Termination of the Code of Conduct]** to only terminate adherence to this Code of Conduct in case of

a. it being replaced by a similar arrangement or

b. termination of the service provisioning to the Home Organisation;

p) **[Survival of the clauses]** 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;

q) **[Precedence]** 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 Service Provider and Home Organization, the provision of the agreement concluded between Service Provider and Home Organization takes precedence over the provision of this Code of Conduct.

GEANT

GEANT - Code de Conduite concernant la protection des données de

Pour les Fournisseurs de Services établis dans l'Union européenne, l'Espace Economique européen et les pays assurant une protection des données adéquate conformément à l'article 25§6 de la Directive 95/46/CE

GN3-12-215

Document URI:
http://www.geant.net/uri/dataprotection-code-of-conduct/v1

Version 1.0, 14 juin 2013

Objectif et Contexte

Sans préjudice des dispositions reprises dans le contrat entre l'Organisme d'Origine et le Fournisseur de Service qui primeront en toutes circonstances, ce Code de Conduite détermine les règles auxquelles les Fournisseurs de Services adhèrent lorsqu'ils veulent recevoir des Attributs concernant leurs Utilisateurs Finaux de la part des Organismes d'Origine ou de leur Agent afin de rendre leurs services accessibles. Ce Code de Conduite est un code communautaire contraignant pour les Fournisseurs de Services qui se sont engagés à le respecter.

Le travail qui a mené à ces résultats a reçu un financement du Septième programme-cadre (7ème PC 2007-2013) de la Communauté européenne en vertu du Contrat de subvention n° 238875 (GEANT).

1. Définitions

a) Fournisseur d'Identité (FId): le composant du système qui émet des assertions sur les Attributs au nom des Utilisateurs Finaux qui les utilisent afin d'accéder aux services du Fournisseur de Service.

b) Fournisseur de Service (FS): Un organisme chargé de proposer à l'Utilisateur Final les services qu'il ou elle souhaite utiliser.

c) Organisme d'Origine: L'organisme à lequel un Utilisateur Final est affilié gérant le Fournisseur d'Identité par lui-même ou via un Agent. Il est en charge de la gestion des données d'identité des Utilisateurs Finaux et de leur authentification.

d) Agent: L'organisme gérant, le cas échéant, le Fournisseur d'Identité au nom de l'Organisme d'Origine.

e) Attributs: Les données à caractère personnel de l'Utilisateur Final, gérés par l'Organisme d'Origine ou son Agent, tels que notamment le nom, l'e-mail et le rôle au sein de l'Organisme d'Origine.

f) Utilisateur Final: toute personne physique affiliée à un Organisme d'Origine, par exemple un chercheur ou un étudiant utilisant le service d'un Fournisseur de Service.

g) Données à caractère personnel: toute information relative, le cas échéant, à une personne physique ou morale, identifiée ou identifiable.

2. Principes du Traitement des Attributs

Le Fournisseur de Service accepte et s'engage à:

a) [**Respect de la législation**] ne traiter les Attributs que conformément aux dispositions pertinentes de la législation relative à la protection des Données à caractère personnel applicable au Fournisseur de Service;

b) **[Limitation des finalités]** ne traiter que les Attributs de l'Utilisateur Final qui sont nécessaires pour permettre l'accès au service fourni par le Fournisseur de Service;

c) **[Réduire au maximum les données]** limiter les Attributs demandés à l'Organisme d'Origine à ceux qui sont adéquats, pertinents et raisonnables en vue de permettre l'accès au service, et, lorsque plusieurs Attributs peuvent être utilisés pour fournir un accès au service, utiliser les Attributs les moins intrusifs possible;

d) **[Objectifs détournés]** ne pas traiter les Attributs à des finalités autres (par exemple,

la vente des Attributs ou la vente d'éléments d'identification, tels que l'historique des recherches, les communications à caractère commercial, les profils) hors ceux destinés à permettre l'accès, sauf si un consentement préalable a été donné par l'Utilisateur Final au Fournisseur de Service;

e) **[Conservation des données]** supprimer ou mettre sous forme anonymisée tous les Attributs dès que ceux-ci ne sont plus nécessaires aux fins de la fourniture du service;

f) **[Parties tierces]** ne pas transférer les Attributs à aucune autre partie tierce (telle qu'un partenaire) sauf

   a. s'il a été mandaté par le Fournisseur de Service pour permettre l'accès à son service en son nom, ou

   b. si la partie tierce s'est engagée à respecter le Code de Conduite ou a pris des engagements similaires jugés suffisants en vertu de la législation relative à la protection des données applicable au Fournisseur de Service ou

   c. en cas de consentement préalable de la part de l'Utilisateur Final;

g) **[Mesures de sécurité]** prendre les mesures, techniques et organisationnelles, appropriées afin de protéger les Attributs contre toute destruction accidentelle ou illicite ou une perte accidentelle, une modification, une divulgation ou un accès non-autorisés. Ces mesures doivent garantir un niveau de sécurité adapté aux risques liés au traitement et à la nature des données à protéger, eu égard au niveau technologique et au coût de leur mise en œuvre.

h) **[Obligation d'information vis-à-vis de l'Utilisateur Final]** fournir à l'Utilisateur Final, au moins lors du premier contact, une Politique de Confidentialité accessible facilement, directement et en permanence, et contenant au moins les informations suivantes:

   a. le nom, adresse et pays du Fournisseur de Service;

   b. la ou les finalités du traitement des Attributs;

   c. une description des Attributs traités;

   d. les destinataires tiers ou les catégories de destinataires tiers à qui les Attributs peuvent être divulgués, et les transferts proposés d'Attributs vers des pays en dehors de l'Espace Economique Européen;

   e. l'existence des droits d'accès, de rectification et de suppression des Attributs conservés concernant l'Utilisateur Final;

   f. la durée de conservation des Attributs;

   g. une référence à ce Code de Conduite

i) **[Obligation d'information vis-à-vis de l'Organisme d'origine]** : fournir à l'Organisme d'Origine ou à son Agent au moins les informations suivantes:

   a. un lien lisible par une machine vers la Déclaration de Confidentialité;

   b. indication de l'engagement pris de respecter ce Code de Conduite;

   c. toute mise à jour ou modification de la législation locale relative à la protection des Données, qui sont moins stricts que les principes énoncés dans ce Code de Conduite;

j) **[Atteintes à la sécurité]** : signaler, sans délai indu, à l'Organisme d'Origine ou à son Agent tout soupçon d'atteinte à la vie privée ou à la sécurité (notamment les divulgations ou atteintes à l'intégrité non-autorisées, la perte, réelle ou possible, de données, documents ou appareils) en rapport avec les Attributs;

k) [**Responsabilité**]: indemniser l'Utilisateur Final, l'Organisme d'Origine ainsi que l'Agent de tout préjudice subi à la suite d'une violation de ce Code de Conduite par le Fournisseur de Service comme établi dans une décision judiciaire contraignante et exécutoire;

l) [**Transfert vers des pays tiers**] assurer, lorsque des Attributs sont transférés en dehors de l'Espace Economique Européen et des pays assurant une protection des données adéquate conformément à l'article 25§6 de la Directive 95/46/CE, un niveau de protection adéquat des Données à caractère personnel en prenant les mesures appropriées conformément à la législation du pays dans lequel l'Organisme d'Origine est établi, par exemple en demandant l'accord de l'Utilisateur Final ou en concluant des contrats avec l'Organisme d'Origine sur base des clauses type de l'Union européenne;

m) **[Droit applicable et juridiction compétente]** faire en sorte que ce Code de Conduite soit régi par les règles nationales de droit matériel du pays dans lequel est établi le Fournisseur de Service, à l'exclusion des règles de droit international privé, et que tout litige concernant la validité, l'interprétation ou l'application de ce Code de Conduite soit définitivement tranché par la juridiction compétente du pays dans lequel est établi le Fournisseur de Service;

n) **[Pouvoirs pour conclure]** faire signer ce Code de Conduite par un représentant dûment autorisé du Fournisseur de Service;

o) **[Résiliation de ce Code de Conduite]** ne mettre fin à son adhésion à ce Code de Conduite que:

   a. si celui-ci est remplacé par un accord similaire ou

   b. en cas de fin de la fourniture de services à l'Organisme d'origine;

p) **[Survie des clauses]** être tenu par les dispositions de ce Code de Conduite qui, en raison de leur sens et portée, sont conçues pour subsister après la fin, l'expiration ou la

nullité de ce Code de Conduite;

q) **[Primauté]** respecter la disposition selon laquelle, en cas de conflit entre une disposition contenue dans ce Code de Conduite et une disposition de la convention conclue entre le Fournisseur de Service et l'Organisme d'origine, la disposition du contrat conclu entre Fournisseur de Service et l'Organisme d'Origine l'emportera sur la disposition de ce Code de Conduite.