26-09-2017

Milestone M9.2
Assessment of DP Legislation Implications

Milestone M9.2

Contractual Date:	28-02-2017
Actual Date:	26-09-2017
Grant Agreement No.:	731122
Work Package/Activity:	9/JRA3
Task Item:	Task 1
Nature of Milestone:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	NORDUnet
Document ID:	GN4-2-17-8C75D
Authors:	P. Axelsson (SUNET)

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

Abstract
This white paper assesses and summarises the implications of the new European Union General Data Protection Regulation (GDPR) for the eduGAIN interfederation service and its different parts.

Table of Contents

Executive Summary

This white paper assesses and summarises the implications of the new European Union General Data Protection Regulation (GDPR) for the eduGAIN interfederation service and its different parts. It aims to provide information about the effect of the new regulation on the academic identity federation landscape and give suggestions on how to address different issues. The white paper is limited to identity federation/interfederation service membership and personal data transferred between users' home organisations and the service provider organisations with federated protocols. The new regulation will come into effect on 25 May 2018.

The GDPR affects all organisations that process personal data of anyone in the European Union (EU) and in non-EU members of the European Economic Area (EEA), resident or not. This holds no matter where you are, or where the processing takes place, even if the processing organisation is located outside the EU/EEA. Furthermore, if the organisation is based in the EU/EEA or the processing takes place in the EU/EEA, the organisation is always subject to the GDPR for all processing, wherever the data subjects are located. International organisations, such as CERN and ESA, are handled in the GDPR the same way as countries outside the EU/EEA.

1 Introduction

eduGAIN interconnects higher education and academic Identity Federations around the world, simplifying access to content, services and resources for the global research and education community. eduGAIN enables the trustworthy exchange of information related to identity, authentication and authorisation.

eduGAIN:

- Helps students, researchers and educators access online services while minimising the number of accounts users and Service Providers have to manage – reducing costs, complexity and security risks.
- Gives Service Providers access to a larger pool of users internationally, and allows users to access resources of peer institutions or commercial or cloud services using their one trusted identity.

With eduGAIN participants from more than 2,500 Identity Providers accessing services from more than 1,700 Service Providers [eduGAIN Tech], eduGAIN is the primary mechanism to interfederate for research and education collaboration around the world.

Ensuring the safe, secure and proportionate exchange of personal data between end points that are in eduGAIN is a key benefit of the service to End Users and Service Providers. By design, neither the eduGAIN interfederation service nor member Identity Federations carry personal data or information about End Users at any point and the principles in use in many cases exceed the requirements of current and future legislation. Operational contact information for individual administrators of infrastructure is held in the eduGAIN database and in federation metadata.

Personal data is only exchanged in a federated identity environment such as eduGAIN when an End User logs in to a service using a federated Identity Provider. At this point, a minimal set of personal data (attributes) about the End User is transferred securely and encrypted from the End User's Home Organisation to the Service Provider Organisation so that the Service Provider can judge eligibility to access a service. This is called Attribute Assertion. Where it takes place within the European Union (EU) and within non-EU members of the European Economic Area (EEA) or involving these citizens, this transfer of information will be subject to the General Data Protection Regulation (GDPR) [GDPR] from the effective date 25 May 2018. The exception to this is when the Identity Provider, Service Provider and the citizen are all located outside EU/EEA at time of transfer of personal data.

This document aims to give Home Organisations, Service Provider Organisations and Federation Operators information about most of the known implications of the General Data Protection Regulation in the eduGAIN interfederation environment so that organisations can prepare for

compliance within their environments. It is expected that detailed guidance from regulatory authorities on the implementation of the Regulation and on national derogations will be provided in the next few years. Those guidelines may affect the information in this document.

For a general introduction to the new European General Data Protection Regulation, information is available on the website of your national data protection agency. If you cannot find an introduction based on your country's legal culture or if you are situated outside the EU/EEA, the British Information Commissioner's Office has a good overview of the new legislation [ICO GDPR].

All terminology used in this document is based on the most commonly used identity federation technology today, SAML2. The resulting document is reusable for other federation technologies, i.e. eduroam and the forthcoming OpenID Connect Federation, with customisation for those operational contexts. For example, the analogue of a federation in eduroam is a National Roaming Operator (NRO), and a Service Provider is called a Relying Party (RP) in other identity federation technologies.

2 Analysis of GDPR Impact

The new European General Data Protection Regulation [GDPR] is a European Union regulation that must be implemented without any local adaptions in national law by all member states within the European Union and by agreement in all non-EU-member states of the European Economic Area (Iceland, Lichtenstein and Norway) with an effective date of 25 May 2018. Unlike previous Data Protection Directives (DPDs) [DPD], which gave member states some leeway in interpretation and implementation, as a regulation the GDPR is a binding legislative act and must be applied in its entirety. This means that the personal data protection laws within most of Europe will be harmonised. However, it is possible for some national derogations in certain situations: member states can introduce exemptions from the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in safeguarding a democratic society. Within the GDPR there is also scope for some national adjustments and complementary national legislation. The United Kingdom will still be a member of the European Union in the spring of 2018 and therefore the UK will adopt the new legislation.

Within the GDPR, Personal Data is defined as any information, single or in combination, that can identify a person directly or indirectly. This includes online identifiers such as pseudonymised persistent or non-persistent identifiers, IP addresses and cookies if they are capable of being linked back to the person.

The most important changes between the old Data Protection Directive and the new General Data Protection Regulation are in the areas of Increased Territorial Scope, Penalties, Consent, Breach Notification, Right to Access, Right to be Forgotten, Data Portability, Privacy by Design and Data Protection Officers.

2.1 Impact on General Aspects of eduGAIN

2.1.1 Description of eduGAIN and Identity Federations

In an Identity Federation, and in an interfederation service such as eduGAIN, it is not the federation itself that controls or processes personal data but the end points. Identity Providers (IdPs) and Attribute Authorities (AAs) are known as "data controllers" and Service Providers (SPs) are called "data processors" if bilateral data processing agreements are in place between the parties, as they process the data supplied by Identity Providers and Attribute Authorities. When there is no data processing agreement between the Identity Provider Home Organisation and the Service Provider Organisation, the Service Provider becomes the data controller over the asserted attributes. In these cases, the End Users, or "data subjects" in the GDPR, should be informed with transparency and in a

user-friendly language of what attributes are released by the Identity Provider to the Service Provider.

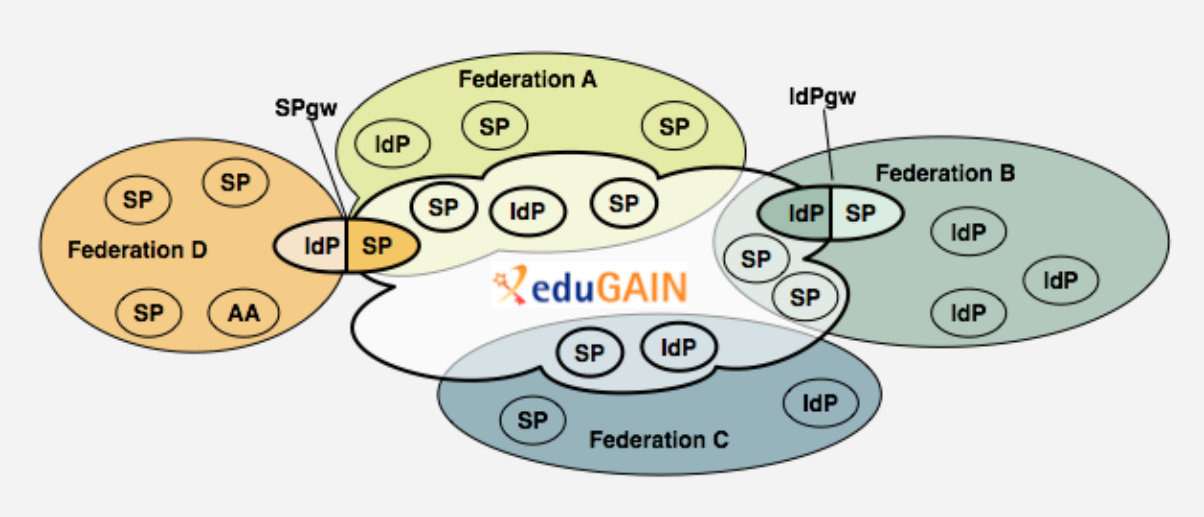

Figure 2.1: Identity federation technical architecture

The most common type of Identity Federation is when all Identity Providers and Service Providers communicate directly between each other and the Federation Operator provides metadata on all parties in the federation (Federation A and C in Figure 2.1). This is called a full-mesh federation.

There may be more complex entities in Identity Federations that act like a gateway, or proxy, between the federation and a cluster of one or more Identity Providers or Service Providers.

For a cluster of Identity Providers this is called an Identity Provider Gateway (IdPgw) and may be seen as an "Identity Provider only" federation with a single Service Provider that acts like a common Identity Provider for all the individual Identity Providers towards the federation (Federation B in Figure 2.1). In its most pure form, where all Identity Providers within the Identity Federation are hidden behind an IdPgw, then the Identity Federation is called a hub-and-spoke federation. In a hybrid federation, you find a combination of a full-mesh federation and a hub-and-spoke federation where some Identity Providers are behind the Identity Provider Gateway and some not. The most important implication for GDPR adoption is that the IdPgw is a data processor that acts on behalf of the actual Identity Providers on the inside of the gateway.

Some research organisations/projects aggregate all their Service Providers behind a Service Provider Gateway (SPgw) and the whole research organisation/project acts like one Service Provider in the federation (Federation D in Figure 2.1). This means that the Service Provider acts on behalf of the actual Service Providers on the inside of the gateway. If the SPgw adds, stores and asserts data about the End User, e.g. specific authorisation information, it is a data controller for that personal data.

In an Identity Federation, there can be a form of specialised service that acts as an attribute store for one or more Service Providers. These services are called Attribute Authorities (AAs) and they are data controllers for the information they store. Where there is a contractual relationship between

an Attribute Authority and the Service Providers it serves, there should be a data processing agreement appended to the contract.

The federation exports some or all of these entities to the academic interfederation eduGAIN, according to national policies.

2.1.2 Impact of GDPR

The General Data Protection Regulation is an EU/EEA regulation that regulates the core business of Identity Federations, i.e. release of personal information from an Identity Provider to a Service Provider. Therefore, it is important for all parties within a federated environment to understand the impact of the new regulation.

All Identity Providers, Service Providers, Attribute Authorities and Federation Operators within the EU/EEA are directly within the scope of the GDPR. The increased territorial scope of the new regulation also makes all Service Providers that accept End Users from within the EU/EEA affected by the GDPR, even if they operate outside the EU/EEA. Depending on the federation architecture, the Federation Operator may not have significant involvement in the transfer of End User data. However, even for full-mesh federations, the policies and practices that govern how Identity Providers and Service Providers participate should be reviewed based on the GDPR.

2.1.3 Recommendation

The Identity Federations, together with the eduGAIN interfederation service and the identity federation community REFEDS, need to review their best practices regarding Attribute Assertions to ensure they adhere to the new legislation.

To do minimal Attribute Assertions at scale is one of the greatest challenges for Identity Federations. It is important to keep the balance between minimal data exchange and enabling the users to access the services that they need for research and education. The identity federation community must continue to work on scalable minimal Attribute Assertions and adapt them to the GDPR. The following section focuses on those practices currently in use and how they are impacted by the GDPR. However, Identity Federations, or National Research and Education Networks (NRENs) more widely, also need to help Home Organisations and Service Provider Organisations identify where those scalable models do not apply so that the contracting parties can make bilateral Data Processor Agreements where necessary. The eduGAIN interfederation service should consider developing a sample bilateral Data Processor Agreement as an exemplar in the eduGAIN interfederation service Best Common Practice (BCP) package, with the caveat that implementation must be at the risk of the contracting parties.

2.2 Impact on Recommended Practices and Profiles

While it is the approach that minimises risk most fully, it is not feasible to handle bilateral Data Processor Agreements between every Home Organisation and every Service Provider Organisation without dramatically altering the cost/benefit relationship for all parties involved. In addition, due to

the highly diverse and scattered nature of research geographically, it is unlikely that any central brokering function would be recognised and adopted. More importantly, due to the principles of data minimisation and privacy that have always been inherent in identity federation, it is not necessary to adopt this approach to deliver the GDPR's objectives. Additional barriers to use of service deter the user from using these privacy-preserving mechanisms and drive them towards use of private identities from providers with less stringent data minimisation principles, thereby also undermining the spirit of compliance with the GDPR, which is to provide citizens with a firmer privacy foundation for their data.

The recommended approach to minimise risk within the GDPR, but to avoid the opposite risk of hindering the End Users in using the Service Providers they need, is to create and implement standardised classifications for Attribute Assertion. These standardised classifications are called Entity Categories and they sort the different Service Providers into different, larger use cases with particular attribute or data management aspects so that Identity Providers can automate Attribute Assertion decisions in a scalable manner. Internationally within eduGAIN there are two entity categories in use today: GÉANT Data Protection Code of Conduct and REFEDS Research and Scholarship (described in Section 2.2.1 and Section 2.2.2 below). When entity categories are used the Service will take ownership of the personal data that is transferred from the Identity Provider to the Service Provider via Attribute Assertion.

All academic Identity Federations, and the interfederation service eduGAIN, publish within their technical metadata names, email addresses and sometimes telephone numbers for administrative, technical, support and security contacts. These contacts should not be personal but rather refer to functions.

2.2.1 GÉANT Data Protection Code of Conduct

2.2.1.1 *Description*

The current version of the GÉANT Data Protection Code of Conduct (GÉANT CoCo) [GÉANT CoCo] describes an approach to meet the requirements of the EU Data Protection Directive in federated identity management. The GÉANT Data Protection Code of Conduct defines behavioural rules for Service Providers that want to receive attributes from Home Organisation Identity Providers about the user that logs in to the service. It is expected that Home Organisations are more willing to release attributes to Service Providers who manifest conformance to the GÉANT Data Protection Code of Conduct.

2.2.1.2 *Impact of GDPR*

The GÉANT Data Protection Code of Conduct is being updated to reflect the changes between the new GDPR and the old Data Protection Directive (DPD), both to update requirements for the GDPR and also to deprecate aspects no longer needed from the former DPD.

The work on a new version of GÉANT CoCo commenced in the GN4-2 project and is being carried out by a small team of identity federation specialists with support from data protection legal specialists at the global law firm DLA Piper. The draft GDPR version has been substantially completed and has at the time of writing been sent out to consultation within the international identity federation community. The new version of GÉANT CoCo is more detailed than version 1 as the new legislation is

more prescriptive and takes into consideration the areas of Increased Territorial Scope, Penalties, Consent, Breach Notification, Right to Access, Right to be Forgotten, Data Portability, Privacy by Design and Data Protection Officers. The interim working draft was published in June 2017 on the REFEDS Wiki [GÉANT CoCo-v2]. An explanatory memorandum is being prepared in parallel.

2.2.1.3 *Recommendation*

The small working group shall complete the work on the new GDPR version of the GÉANT Data Protection Code of Conduct, including aspects such as jurisdiction and arbitration clauses for international organisations. After completion, the new version must be submitted to the EU GDPR competent supervisory authority of approved codes of conduct as described in GDPR Article 40. After the submission of GÉANT CoCo v2.0. GÉANT shall work together with the competent supervisory authority to get GÉANT CoCo v2.0 approved as an official GDPR Code of Conduct, effective after 25 May 2018.

In parallel with the approval process, adoption and use of GÉANT CoCo v2.0 within eduGAIN will be formalised as Best Practice for both Service Providers and Identity Providers. Federations should therefore prepare their tools and processes to enable adoption and use by Identity Providers and Service Providers. They can be supported in this by GÉANT, with training and best practice documentation.

2.2.2 REFEDS Research and Scholarship Entity Category

2.2.2.1 *Description*

The target Service Providers for the REFEDS Research and Scholarship Entity Category (REFEDS R&S) [REFEDS R&S] are those operated for the purpose of supporting research and scholarship interaction, collaboration or management, at least in part. REFEDS R&S is intended for global use by a wide range of different Service Providers, commercial, campus or research, providing they fulfil the above condition. REFEDS R&S is designed to allow data to flow to providers that have a legitimate interest in the data. It is important to note that the GDPR is not only intended to protect personal data, but also to “remove the obstacles to flows of personal data”. This second area is often overlooked in the analysis of the GDPR.

The attributes supported in REFEDS R&S are chosen to represent a privacy baseline such that further minimisation achieves no particular benefit. The attribute bundle contains a shared unique user identifier, personal name, mail address and, optionally, a user affiliation. The shared unique identifier can be narrowed down to a unique identifier between the Identity Provider and Service Provider or a global unique identifier based on the need. The optional affiliation attribute can have one or more of the values faculty, staff, employee, student, member, affiliate, alum and library-walk-in.

2.2.2.2 *Impact of GDPR*

Little has changed in the application of the REFEDS Research and Scholarship Entity Category under the GDPR. REFEDS R&S was designed to ensure the processing was explicit, legitimate and limited, and with safeguards and risk assessment built in to the process. REFEDS R&S provides both technical and organisational measures to ensure the requirements of the Regulation are met.

The EU/EEA use of REFEDS R&S is based on "legitimate interests", as described in Article 6 of the GDPR: "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party". This legitimate interest is based on the fact that the End User is accessing the service to fulfil their work duties or studies, i.e. a relevant and appropriate relationship between the End User and the Home Organisation exists and the fundamental rights and freedoms [CFREU] of the End User are not violated. The impact of the GDPR is low due to the fact that REFEDS R&S is based on necessary use of the service and utilises the minimal Attribute Assertion (shared user identifier, person name, email address and the optional organisational affiliation).

2.2.2.3 *Recommendation*

Service Provider Organisations outside the EU/EEA must comply with the GDPR for their European End Users and if they cannot fulfil this requirement they should not offer the services to federated users from within the EU/EEA. As such, international use of the REFEDS R&S process is recommended for federations, although further work is required to support the requirements of Article 45 and 46 of the GDPR. It is noted that many of the processes identified in this section do not yet exist.

As REFEDS R&S is based on necessary use by legitimate interest of the Home Organisation or the Service Provider Organisation, if the Home Organisation's Identity Provider uses consent for Attribute Assertions before GDPR comes into effect, then it is advisable to remove the consent question. It is possible to use a transparent privacy notice in which the Identity Provider explains to the End User which attributes are released and why it is necessary to release them for REFEDS R&S Service Providers. Such a transparent privacy notice must be implemented so as to have a minimum impact on the workflow of the End User. For more information on the use of consent in GDPR, see Section 2.3.1.

REFEDS is carrying out an assessment of the GDPR on REFEDS R&S. Areas addressed will be the use of consent with REFEDS R&S, the use of REFEDS R&S outside the EU/EEA and the applicability of REFEDS R&S as an appropriate certification mechanism. The incorporation of REFEDS R&S as eduGAIN Best Common Practice will take these factors into account.

Furthermore, REFEDS R&S requires Federation Operators to implement a lightweight audit before applying the tag to ensure that the data in the attribute bundle is legitimately required by the Service Provider. This is supported by a risk management toolkit to help organisations make effective decisions when supporting REFEDS R&S. This process means that REFEDS R&S is a candidate for a Certification approach for demonstrating compliance as described in the GDPR, and REFEDS and eduGAIN will be exploring the potential of this route as Certification bodies emerge.

2.2.3 Security Incident Response Trust Framework for Federated Identity – SIRTFI

2.2.3.1 *Description*

Within a federated community there is a need to handle different security incidents. The Security Incident Response Trust Framework for Federated Identity (SIRTFI) [SIRTFI] aims to enable the coordination of incident response across federated organisations. This assurance framework

comprises a list of assertions which an organisation can attest in order to be declared SIRTFI compliant. The SIRTFI framework was finalised in late 2016, and adoption of SIRTFI throughout the eduGAIN membership is underway.

2.2.3.2 *Impact of GDPR*

Security incidents involving breach of personal data are in scope for SIRTFI. In GDPR Chapter IV Section 2 the security practices for data breach of personal data are defined.

There are different practices depending on whether the organisation with the data breach is the data controller or is the data processor of the personal data involved in the breach. Identity Providers and Attribute Authorities are always data controllers but a Service Provider can be either a data processor or a data controller based on whether or not there is a Data Processing Agreement with the Identity Home Organisation, as described in Section 2.1.1.

A data processor must inform the national supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of the data breach. Article 33 defines the minimal steps for a data controller with regard to handing the data breach and the need for documentation. A data processor is required to inform the data controller about a personal data breach without undue delay. The data processor should assist the data controller with the documentation of the data breach; this behaviour should be defined in the Data Processing Agreement.

Article 34 defines how the End User should be informed by the data controller of a data breach. If the personal data breach is likely to result in a high risk to the rights and freedoms of the End User the data controller should inform the End User without undue delay. If the data controller has met certain conditions defined in Article 34 there is no need to inform the End User until the national supervisory authority requires it.

2.2.3.3 *Recommendation*

In the event of a data breach the GDPR only stipulates communication between a data processor and the national supervisory authority and between a data processor and the data controller. In a federated environment, more than one data controller can be affected by the data breach and therefore it is recommended that other affected data controllers are informed in an appropriate way. It may be hard for a data controller to evaluate which data controllers could be affected and there is need for a central function within eduGAIN to help the data controllers with this identification process. This central function should also handle data breach reporting.

The recommended way to meet the requirement of the GDPR with regard to handling communications around data breaches within the federated environment is to use the SIRTFI framework. SIRTFI Best Practice will therefore be positioned formally within eduGAIN as recommended practice, and supported by the central function for data breaches. SIRTFI has also been included in the GÉANT CoCo v2.0 specification to address GDPR requirements on incident response. SIRTFI states that the use of the Traffic Light Protocol (TLP) must be used to facilitate such information sharing.

Information around the data breach may be very sensitive and the identity of the End User should only be communicated directly between the End User Home Organisation and the affected Service Provider Organisations or the rights and freedoms of the End User may be breached.

2.2.4 Contact Information within Federation and Interfederation Metadata

2.2.4.1 *Description*

To run an effective academic Identity Federation, or an interfederation service as eduGAIN, all of the different parties involved must be able to communicate directly with each other on operational matters. To enable this communication, contact information for Identity Providers, Service Providers and Attribute Authorities is published for administrative, technical, support and security contacts maintained in the federation technical metadata.

2.2.4.2 *Impact of GDPR*

The contact information in the technical metadata consists of name, email address and potentially a telephone number for each of the contact types. If these contacts relate to identifiable humans they are subject to the GDPR.

The eduGAIN interfederation service publishes contact information for the eduGAIN Steering Group delegate and deputy of all member federations on the technical website These contacts are for individuals and therefore subject to the GDPR.

2.2.4.3 *Recommendation*

Each academic Identity Federation should recommend that their Identity Providers, Service Providers and Attribute Authorities use non-personal contact information in the metadata to avoid having personal data in the technical metadata. If personal information is unavoidable, Article 15 on the rights of access by the data subject applies. This includes aspects such as the right to information about data processing, information about how the data is sourced, the right to lodge a complaint and other aspects of personal data management.

The eduGAIN interfederation service operators should inform eduGAIN member organisations that information about their Steering Group delegate and deputy is published on their technical website. Processes in eduGAIN Operations should ensure that the individuals mentioned have the appropriate ability to ensure this information is accurate and to understand how it is used (as described in Article 15 Rights of access by the data subject).

2.3 Impact on Other Aspects and Practices

2.3.1 Use of Consent

2.3.1.1 *Description*

In the local adaptions of the Data Protection Directive, the use of consent was defined differently in the legislations of the European countries. As a result, it was not easy to give a general recommendation on the use of consent as a risk management strategy for attribute release.

2.3.1.2 *Impact of GDPR*

In the General Data Protection Regulation, requirements around consent have been clarified in a Recital.

"(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data.

Silence, pre-ticked boxes or inactivity should not therefore constitute consent.

Consent should cover all processing activities carried out for the same purpose or purposes.

When the processing has multiple purposes, consent should be given for all of them.

If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."

Where consent is applicable, all consent should always be given freely, and be specific, informed and unambiguous. This means that when Attribute Assertion is based on one of the defined necessary processing models in Chapter II Article 6, End User consent is not considered applicable. Furthermore, negative consent cannot be used for users affected by the GDPR, i.e. you cannot ask the user to uncheck a box in order to stop information being shared. Negative consent is often used outside the EU/EEA and therefore the expanded territorial reach of the GDPR has a de facto impact on the use of consent globally.

2.3.1.3 *Recommendation*

It is possible to interpret from the legislation that an End User should not be asked for consent when necessary Attribute Assertion takes place between an Identity Provider and a Service Provider. Consent should only be used when the Attribute Assertion is not necessary. This would imply that when one of the entity categories GÉANT Data Protection Code of Conduct or REFEDS Research and Scholarship is used for Attribute Assertion, Identity Providers should not ask for consent. This may

have a significant impact on the use of Identity Provider consent mechanisms, such as uApprove and Consent-Informed Attribute Release (CAR), and requires further investigation by federations where use of consent is common under existing legislation. Further, specific investigation of the relationship between use of consent and other attribute release mechanisms is therefore recommended, including seeking specific legal opinion when preparing Best Common Practice (BCP).

The Identity Provider can and maybe should inform the users what personal data is released to the service. Therefore, consent mechanisms may be adapted and extended to change the consent button from "I agree" to "OK" or "I understand" to support the requirement for transparent privacy notices rather than consent. It is important that this information is provided in a user-friendly fashion so the user is informed, not misinformed, and does not see it as a consent request.

In addition, the End User should be able to look up what personal data about the user is available at the Service Provider Organisation. This is not a question of consent but of the End User's rights to transparency of and control over their personal data. This information would not be shown at time of logon but should rather be easily available within the service.

2.3.2 Interoperability with Jurisdictions outside the EU and EEA

2.3.2.1 *Description*

One of the largest changes in the GDPR is the extended territorial scope of the legislation regarding both Home Organisations and Service Provider Organisations. In Chapter V of the GDPR, international transfer of personal data outside the EU/EEA is defined. The definition is applicable to both third countries, i.e. countries outside the EU/EEA, and international organisations, i.e. an organisation established by a treaty or other instrument governed by international law and possessing its own international legal personality. Some research organisations within Europe are defined as international organisations, e.g. CERN and ESA.

2.3.2.2 *Impact of GDPR*

The increased territorial scope in the GDPR makes all Service Providers that supply services to End Users within the EU/EEA affected by the GDPR even if they operate in a third country or within an international organisation. In the old Data Protection Directive, this was ambiguous and referred to "in context of an establishment".

Processing or transfer of the control of personal data for End Users using an Identity Provider within the EU/EEA to log in to a Service Provider outside the EU/EEA or into an international organisation where personal data is transferred via an Attribute Assertion continues to be subject to the GDPR.

2.3.2.3 *Recommendation*

Service Provider Organisations outside the EU/EEA must comply with the GDPR for their European users and if they cannot fulfil this requirement they should not offer the services to federated users from within the EU/EEA. There may be a need for a metadata jurisdiction marking to help Service Provider Organisations with filtering based on the GDPR. This provides an opportunity for simplification, as separate regional mechanisms and tools do not need to be developed to cover SPs outside the EU/EEA.

The entity categories GÉANT Data Protection Code of Conduct and REFEDS Research and Scholarship should be used to handle Attribute Assertions from Identity Providers within the EU/EEA to Service Providers outside.

2.3.3 Rights of the Data Subject

2.3.3.1 *Description*

Chapter III of the General Data Protection Regulation contains a set of defined rights for the End User based on the fair processing principle, i.e. all data processing must be fair, lawful and transparent. These rights are defined to create a possibility for the data subject to exercise the right to transparent information, communication and modalities.

In short, the rights for the End User are:

- The right to information on data processing.
- The right to access personal data.
- The right to rectification.
- The right to erasure ("right to be forgotten").
- The right to restriction of processing.
- The right to data portability[1].
- The right to object.
- The right not to be subject to automated individual decision-making.

Fair processing requires the applicable organisation to:

- Be open and honest about the identity of the organisation.
- Describe to End Users how the organisation intends to use any personal data it collects about them (unless this is obvious).
- Only process End Users' personal data lawfully.
- Handle End Users' personal data only in ways they would reasonably expect.
- Above all, not use End Users' personal data in ways that unjustifiably have a negative effect on them.

2.3.3.2 *Impact of GDPR*

The rights of the data subject are fundamental to the GDPR and therefore it is important for organisations to fully understand these rights. All parties within an Identity Federation, and the interfederation service eduGAIN, shall respect End Users' rights, including the right to access to personal data, the right to request correction of any inaccurate information relating to them and the right to request deletion of any irrelevant personal data the Identity Provider, Service Provider or Attribute Authority holds about him or her.

[1] The right to data portability only applies if the basis for processing is either consent or necessary for contract.

2.3.3.3 *Recommendation*

The best way to fulfil the right to information on data processing is to create a privacy policy that describes what and how personal data is used in the service. It is recommended that appropriate privacy policies are published for all levels of identity federation services, from eduGAIN centrally to federations to Identity Providers and Service Providers, to demonstrate transparency of compliance to the GDPR.

One notable effect of the right to erasure is that personal information, such as personal data within logs, should not be saved longer than needed. The privacy policy shall contain information on how long personal data is kept.

The upcoming version 2 of the GÉANT Data Protection Code of Conduct will contain information on how to uphold the rights of the End User that can be adapted to provide a framework for such privacy policies.

3 Conclusions and Next Steps

The new European legislation makes us all think about how we can design applications to take better care of personal privacy. The data protection rights of the End User are central to this change. In the research and education environment, this means ensuring that individuals in their roles as researcher, staff member or student are not hindered in their daily use of federated services but at the same time their privacy as an individual is preserved. Research and education federations have always led the way in adopting these principles for End Users, and are therefore well placed to comply with the GDPR and to go beyond in the spirit of it.

Although the effective date of the Regulation is in 2018, it must be noted that consistent and detailed implementation advice and concrete examples on the implementation of GDPR compliance are scarce as there is as yet no real body of experience. Initiatives within the GÉANT community such as the proposed Task Force on Data Protection Regulation (TF-DPR) will enable eduGAIN and federations to track state of the art in this area and refine compliance plans as the date for implementation approaches.

However, from the existing level of information, it appears that existing research and education federation practice already supports most of the aims of the GDPR, and that only minor changes are likely to be required. As with every legislation change, national research and education Identity Federation Operators need to actively review recommendations they give Home Organisations and Service Provider Organisations so that the General Data Protection Regulation is mirrored in the recommendations. The work within REFEDS and eduGAIN can help the federations with this work, covering federation and interfederation practice to ensure we can continue to support international research and education, but the spirit of the design of these services already strongly enforces individual privacy and the ability to support the work of research and education.

Within eduGAIN, in the current workplans, Best Common Practice on CoCo, R&S and SIRTFI will be positioned to make implementation more consistent and well understood, supported by the harmonisation opportunity presented by the GDPR. GÉANT will develop privacy policies scoped for eduGAIN central infrastructure and provide support and guidance to the community in the preparation of policies at federation level and IdP/SP organisation level. Best Common Practice on the use of consent will also be considered in an additional phase. GÉANT and eduGAIN will continue to support work at REFEDS and AARC2 to ensure policies and practices are adapted for the GDPR environment as needed, and will support federations in their adoption with documentation and training.

The European Union is working on a draft for a new regulation on Privacy and Electronic Communications [ePR]. This regulation is focused on the protection of fundamental rights and

freedoms of natural persons in the provision and use of electronic communications services. Depending on definitions, it may have a future impact on federated login and Attribute Assertions.

Acknowledgements

In the work on this white paper the author was helped by a lot of people both directly, in terms of contributions, and indirectly. The author would like to particularly mention the following people:

- David Foster, CERN
- David Groep, Nikhef
- Ann Harding, SWITCH
- Nicole Harris, GÉANT Association
- Lukas Hämmerle, SWITCH
- Mikael Linden, CSC
- Valter Nordh, SUNET
- Hannah Short, CERN

The discussions within different mailing lists in the identity federation community have been a source of what needs to be discussed in this white paper. Thank you all for indirectly directing me to where the challenges are.

The legal advice from DLA Piper for the next version of the GÉANT Data Protection Code of Conduct has been very valuable in the writing of this white paper.

Special thanks go to Andrew Cormack, Jisc, for his interesting and informative blog [Cormack] and regular community updates about regulatory developments.

References

[CFREU]	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
[Cormack]	https://community.jisc.ac.uk/blogs/regulatory-developments
[DPD]	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046
[eduGAIN Tech]	https://technical.edugain.org retrieved September 2017
[ePR]	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CONSIL:ST_11995_2017_INIT
[GÉANT CoCo]	http://www.geant.net/uri/dataprotection-code-of-conduct/v1
[GÉANT CoCo-v2]	https://wiki.refeds.org/display/CODE/Code+of+Conduct+ver+2.0+project
[GDPR]	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
[ICO GDPR]	https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
[REFEDS R&S]	http://refeds.org/category/research-and-scholarship
[SIRTFI]	https://refeds.org/sirtfi

Glossary

Acronym	Term / Name	Description
–	Attribute Assertion	Transfer of personal data from End User Identity Provider to the requested Service Provider, i.e. gives the service information about the End User to authenticate and authorise and when needed the End User's personal data.
AA	Attribute Authority	An Attribute Authority is a service within an Identity Federation that only acts like an attribute store for one or more Service Providers.
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. In GDPR the End User is called a data subject.
–	Entity Category	Entity categories are classifications of Service Providers in metadata that makes it possible to group different Service Providers based on different criteria. It is possible to base Attribute Assertions on entity categories.
EU	European Union	
GDPR	General Data Protection Regulation	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).
–	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. In GDPR the Home Organisation is called a data controller.
–	Identity Federation	An association of Home Organisations and Service Providers typically organised at national level, which collaborate for allowing cross-organisational access to services.
IdP	Identity Provider	The system component that issues Attribute Assertions on behalf of End Users who use them to access the services of Service Provider Organisations.

Acronym	Term / Name	Description
IdPgw	Identity Provider Gateway	A special type of Identity Provider that acts as a proxy for one or more Identity Providers. The proxy could be a protocol conversion proxy from one identity technology on to another or it could be a harmonising proxy that makes it easier to administrate attribute release policies.
–	Interfederation	An interfederation is best described as a federation of Identity Federations that share a common goal. The interfederation makes it possible for End Users within one Identity Federation to use services within another Identity Federation.
–	Personal Data	Any information, single or in combination, that can identify a person directly or indirectly. This includes online identifiers such as pseudonymised persistent or non-persistent identifiers, IP addresses and cookies if they are capable of being linked back to the person.
–	Recital	Recitals are used by the Court of Justice of the European Union in order to establish what any Directive or Regulation means in the context of a particular case before the Court. With regard to the GDPR, Recitals will also be used by the European Data Protection Board when it exercises its role of ensuring the Regulation is consistently applied across Europe.
REFEDS	Research and Education FEDerationS	
SIRTFI	Security Incident Response Trust Framework for Federated Identity	
SP	Service Provider	A system component that receives Attribute Assertions from Identity Providers, to authenticate the End User to the service and provide the Attribute Assertion to the service about the End User.
SPgw	Service Provider Gateway	A special type of Service Provider that acts like a proxy that enables Service Providers with a common use case to act like one Service Provider into an Identity Federation. The proxy could be a protocol conversion proxy from one identity technology on to another or it could be a harmonising proxy that makes all Service Providers behind the proxy subject to the same attribute release policy.
–	Service Provider Organisation	An organisation that is responsible for offering the End User the service he or she desires to use. In GDPR the Service Provider Organisation may be called both data processor and data controller. Data processor over the personal data received from the Home Organisation and data controller over the personal data that originates at the Service Provider Organisation.