eduGAIN GDPR Impact Assessment

As part of the GN4-2 project, an assessment of the GDPR implications on the eduGAIN constituency was conducted and the results are presented in the A ssessment of DP legislation implications document.

Based on this assessment, the following action points have been attributed to eduGAIN central operational team (in table only eduGAIN), REFEDS, Identity Federation Operators, Service Providers (SP) and Identity Providers (IdP).

We recognise that there are differences in legal requirements for Identity Federations within the European Union (EU) / European Economic Area (EEA) and in the rest of the world, but believe this advisory represents best current practice for all Identity Federations so have not distinguished our advice to different regions.

Action Topic	Who	Description	Advisory	Status
Publishing contacts in metadata	eduGAIN	Operational contact information for individual administrators IdPs, SPs, AAs and Identity Federations is collected in the metadata published by Identity Federation Operators. In this case, eduGAIN is data processor for this information. The information is held and published in the eduGAIN database and in the eduGAIN metadata. The current eduGAIN Metadata Profile says: that if present, <md:EmailAddress> SHOULD not be a personal address but a role address to get in contact with the entity's responsible persons.	Identity Federations should register functional role contact information intended for publication in metadata. Publication of personal data in metadata for publication is not recommended. eduGAIN will publish guidelines and recommendations to the eduGAIN Steering Group (SG). eduGAIN will update the wiki.edugain.org with such examples and practices, and in future Best Current Practice (BCP) guidelines. Since at the moment, there are no strict requirements regarding contact information in metadata, and substantial number of entities are publishing personal contacts, eduGAIN will adapt the (new) eduGAIN Privacy Notice accordingly. Where personal data does exists, all the usual rights of the user under GDPR will apply.	Best Current Practice for eduGAIN will be developed from March 2018 - December 2018. Areas impacted by GDPR will be prioritised.
	Identity Federations	Operational contact information is registered for administrative purposes and published in metadata for administrators of IdPs, SPs and AAs. Different contact details will be held for internal authorisation purposes and as contact points for public consumption.	For metadata that is published, Identity Federations should adapt its entity metadata registration practice to request functional role contacts rather than personal contacts. For internal administration processes, Identity Federations will need to manage personal data for authorisation processes and should adapt Privacy Notices accordingly.	
	REFEDS		When registering entities, Identity Federations will gather several different types of contact data. Some of this will be for internal administrative purposes and some will be to publish in metadata. The REFEDS Metadata Registration Practice Statement should be updated to include guidance on what type of contacts should be gathered for each role.	
SG members contacts	eduGAIN	Contact information for the eduGAIN Steering Group delegate and deputy of all member federations is collected and published on the technical website.	Inform member federations that information about their SG delegate and deputy is collected. This information should be added in the (new) eduGAIN Privacy Notice. Consult with the SG if keeping this information publicly is needed.	Consultation started with the eduGAIN Steering Group.
Data Processor Agreements - DPA	IdPs, SPs	GDPR regulates the release of personal information from an IdP/AA to SP. Scalable minimal attribute assertions should be addressed with the use of entity categories. However, where scalable models do not apply, the contracting parties can make bilateral DPA agreements, such as those embedded in site licenses.	IdPs and SPs have the option to use a bilateral agreement where more specific agreements (not supported by entity categories) are needed or in place - such as via a specific procurement or other agreement. Other approaches that are more scalable will typically be preferred but will not always fit.	
	Identity Federations		Support the IdPs and SPs, and help them identify where scalable models do not apply.	
	eduGAIN /REFEDS		Consider developing a sample bilateral Data Processor Agreement in the BCP package, with the caveat that implementation must be at the risk of the contracting parties.	
GÉANT Data Protection Code of Conduct (CoCo)	eduGAIN	The current version of the CoCo describes an approach to meet the requirements of the EU DPD via the "Code of Conduct" function. It defines behavioural rules for SPs that want to receive user attributes from IdPs/AAs.	Update GÉANT CoCo to reflect the changes between the new GDPR and the old DPD. After completion, the new CoCo v2.0 should be submitted to the EU GDPR competent supervisory authority of approved codes of conduct as described in GDPR Article 40. After the submission of CoCo v2.0. GÉANT shall work together with the competent supervisory authority to get 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 CoCo v2.0 within eduGAIN will be formalised as Best Practice for both SPs and IdPs.	The work on a new version of CoCo is being led by a small team of identity federation specialists with support from DLA Piper. The draft version has been substantially completed and has been sent out to consultation within the international identity federation community.The interim working draft was published in June 2017 and an explanatory memorandum is being prepared in parallel. The second draft was published in January 2018 and the consultation period will finish in February 2018.
	Identity Federations		Prepare the tooling and processes to enable adoption of GÉANT CoCo v2 by IdPs and SPs. Promote usage of CoCo v2 when it's approved.	
	IdPs, SPs		Given the lack of maturity of approaches under Article 40 of the GDPR (Codes of Conduct), the demonstrable application of safeguards and privacy via CoCo and the high-risk impact of other solutions by the user (using commercial logins) there is a strong case to continue using the existing CoCo v1 until CoCo v2 is approved.	
REFEDS Research and Scholarship Entity Category - REFEDS R&S	REFEDS	REFEDS R&S is designed to allow data to flow to research and scholarship SPs, that have a legitimate interest in the data.The attributes supported in REFEDS R&S are chosen to represent a privacy baseline such that further minimisation achieves no benefit. The impact of the GDPR is low due to the fact that REFEDS R&S is based on legitimate interests and requires minimal attribute release (shared user identifier, person name, email address and the optional organisational affiliation).	Guidance on the use of REFEDS R&S and GDPR has been developed by REFEDS and published. REFEDS is considering the potential of making R&S a Certification but this will be a long process. REFEDS should develop a lightweight audit process for SPs asserting R&S entity category, to be used by Identity Federations before asserting the REFEDS R&S tag for the SP to ensure that the data in the attribute bundle is legitimately required. This should be supported by a risk management toolkit to help organisations make effective decisions when supporting REFEDS R&S.	https://wiki.refeds.org/display/ENT/Guidance+on+justification+for+attribute+release+for+RandS
	eduGAIN		Incorporate REFEDS R&S as BCP within eduGAIN.	

	Identity Federations		Implement and use the lightweight audit process for SPs asserting R&S entity category that will be developed by REFEDS.	
	IdPs		As REFEDS R&S is based on legitimate interests, the IdPs should not use consent dialogues in the workflow. A transparent Privacy Notice in which the IdP explains to the end user which attributes are released and why, can be used instead.	
Security Incident Response Trust Framework for Federated Identity – SIRTFI	eduGAIN, Identity Federations, IdPs, SPs	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. In GDPR Chapter IV Section 2 the security practices for data breach of personal data are defined. Security incidents involving breach of personal data are in scope for SIRTFI.	The SIRTFI framework is the recommended way to meet GDPR requirements with regard to handling communications around data breaches within federations. SIRTFI will therefore be positioned formally within eduGAIN as Best Current Practice (BCP) and supported by the central eduGAIN function for data breaches. End-user personal data that is necessary for resolving a security incident should only be shared between end points ie. IdP and SP affected. Identity federations and eduGAIN have a role in supporting, escalation and reporting only.	The SIRTFI framework was finalised in late 2016, and adoption of SIRTFI throughout the eduGAIN membership is underway. 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.
Use of Consent	IdPs	Where consent is applicable, all consent should always be given freely, and be specific, informed and unambiguous.When attribute release is based on one of the defined necessary processing models in Chapter II Article 6, consent is **not** considered applicable. Negative consent cannot be used, i.e IdP cannot ask the user to uncheck a box in order to stop information being shared.	When attributes are required for operation of a service, IdPs should not ask for consent for passing this information. Consent mechanisms may be adapted to support the requirement for transparent privacy notices rather than explicit consent. Do not use an accept button but a continue button.	
	Identity Federations, eduGAIN, REFEDS		Further, specific investigation of the relationship between use of consent and other attribute release mechanisms is recommended, including seeking specific legal opinion when preparing BCP.	
Interoperability with Jurisdictions outside the EU and EEA	SPs outside of EU /EEA	The increased territorial scope in the GDPR makes all SP that supply services to end users within the EU /EEA affected by the GDPR.	SPs outside the EU/EEA should comply with the GDPR, and EEA IdPs should assess the risks of releasing attributes to these services. The entity categories REFEDS R&S and the upcoming CoCo v2 should be used to handle attribute release from IdPs within the EU /EEA to SPs outside.	
Rights of the Data Subject	SPs, Identity Federations, eduGAIN	The rights of the data subject are fundamental to the GDPR and therefore it is important for organisations to fully understand and respect these rights.	Create a Privacy Notice that describes what and how personal data is used in the service. It is recommended that appropriate Privacy Notices are published for all levels of identity federation services, from eduGAIN centrally, to federations, to IdPs and SPs to demonstrate transparency of compliance to the GDPR. These notices should include guidance on which level of the service users should contact in given scenarios. The upcoming CoCo v2 will contain information on how to uphold the rights of the end-user that can be adapted to provide a framework for such Privacy Notices.	An example of how to write a Privacy Notice can be found on the InAcademia website. The Current GÉANT Code of Conduct has a template Privacy Notice as part of its document set.
Support requests to edugain-support	eduGAIN	Contact information for individuals will be received by edugain-support. This will typically only cover email address and any contact information in email signatures, but there is a risk that individuals may share sensitive data regarding the issues they face (e.g. passwords or usernames that are not working, sensitive incident information). Tickets are managed by the GÉANT OTRS system and only accessible by authorised members of the edugain-support team.	Guidance should be given where the edugain-support address is publicised encouraging users not to send personal data to the edugain-support list and describing the incident response role of eduGAIN.	