Guidance on justification for attribute release for RandS

Please note this is a summary of the reasoning behind approaches taken to attribute release by federations, with particular reference to the REFEDS Research and Scholarship Entity Category. It does not constitute legal advice but does point to legal documentation that can be used to support the ideas in this process. All federations and organisations should take appropriate legal advice but are free to use this information to support arguments and processes. For more information see: https://refeds.org/research-and-scholarship

A. Useful Information Sources

Pre-May 2018

- **DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995** on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- **ARTICLE 29 DATA PROTECTION WORKING PARTY Opinion 06/2014** on the notion of legitimate interests of the data controller Under Article 7 of Directive 95/46/EC.
- **ARTICLE 29 DATA PROTECTION WORKING PARTY Opinion 15/2011** on the definition of consent.

From 25th May 2018

- **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).

General Advice

- "Consent, the Last Resort?" Blog post by Andrew Cormack.
- "Legitimate Interests and Federated Access Management." Blog post by Andrew Cormack.
- Data Protection Code of Conduct for Service Providers: Guidelines on "necessary" attributes.

With thanks to Andrew Cormack for allowing REFEDS to use his material for this advice piece.

B. Justification for Processing Data in Europe

Any organisation that processes personal data needs to have a legal justification for doing so. Personal data is defined in GDPR as "information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a **name, an identification number, location data, an online identifier** or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Practically speaking this may mean government id card information, computer IP address, social media account name as well as personal name, telephone, address etc. The Research and Scholarship Entity Category recommended by REFEDS supports minimal disclosure of a few elements of personal data to support access to resources (an identifier, name, email address).

There are 6 use-cases in which you can share personal data within the EU. These remain the same from the pre-GDPR Directive and within the GDPR (Article 6).

Reason	Short Name used by REFEDS	Issues

The data subject has **unambiguously** given his consent.	**CONSENT**	Consent must be unambiguous – forcing people to tick boxes for access can be seen as forced consent.
Processing is necessary for the **performance of a contract** to which the **data subject is party** or in order to take steps at the request of the data subject prior to entering into a contract.	**CONTRACTUAL**	Limited cases where the data subject is legitimately required by contract to provide personal data.
Processing is necessary for compliance with a legal obligation to which the data controller is subject.	LEGAL OBLIGATION	Unlikely to apply in REFEDS scenarios.
Processing is necessary in order to protect the **vital interests** of the data subject.	VITAL INTEREST	Unlikely to apply in REFEDS scenarios.
Processing is necessary for the performance of a task carried out in **the public interest** or in the exercise of **official authority** vested in the controller or in a third party to whom the data are disclosed.	PUBLIC INTEREST	Unlikely to apply in REFEDS scenarios.
Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by the third party or parties to whom the data are disclosed.	**LEGITIMATE INTEREST**	Can be claimed that legitimate interest exists where users need to give certain pieces of data to use a tool for their study / work.

Only three of these options would have bearing in the typical exchanges within a research and education identity federation: **consent, contractual and legitimate interests**.

C. Consent Justification

Work has been done on consent modules for access management workflows and it is now easier to build this functionality in to user screens, but there are concerns that in many scenarios consent could be seen as forced as the subject has no choice but to pass the information if they want to use the resource. The Article 29 Working Party warn that consent may be a "false good solution". This is strengthened in the text of the GDPR, which is clear that consent must be freely given (Article 7).

> *"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." (Recital 32).*

D. Contractual Justification

The important text here is that release must be in line with the performance of a contract to which the data subject is a party. It could be argued that for some staff members, accessing services using federated identities could be seen as a function that is required by their job role but this is difficult to assert for all scenarios. The argument would be much more difficult for students and researchers.

E. Legitimate Interests Justification

The Research and Scholarship Entity Category relies on the legitimate interest approach. This is supported by the Article 29 WP Opinion on Legitimate Interests documentation. There has been some concern expressed that Legitimate Interests cannot be used for Public Authorities as in some countries universities and colleges are deemed Public Authorities, but this limitation is only related to activities that directly relate to work that directly relates to the "public" aspects of the worn undertaken by that organisation. A student accessing a scholarly article or the typical day to day work of a researcher would not fall under the "public" aspects of the organisation. There is a useful article detailing how this has been addressed in the UK.

Use of Legitimate Interests under 1995 Directive

The Article 29 WP recognises that:

> "The current text of Article 7(f) of the Directive is open ended. This flexible wording leaves much room for interpretation and has sometimes as experience has shown led to lack of predictability and lack of legal certainty. However, if used in the right context, and with the application of the right criteria, as set out in this Opinion, Article 7(f) has an essential role to play as a legal ground for legitimate data processing."

The Article 29 WP states that:

> *"...an appropriate assessment of the balance under Article 7(f), often with an opportunity to opt-out of the processing, may in other cases be a valid alternative to inappropriate use of, for instance, the ground of 'consent' or 'necessity for the performance of a contract'. Considered in this way, Article 7(f) presents complementary safeguards - which require appropriate measures - compared to the other pre-determined grounds. (p10)".*

Use of Legitimate Interests under GDPR

The text of the GDPR makes a stronger case for the use of Legitimate Interests. This is described in Recitals 47 - 49.

F. Research and Scholarship Entity Category and Legitimate Interests

In outlining the use case for using Legitimate Interests, the GDPR states that:

> *"Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller." (Recital 47)*

This description applies well to most transactions carried out by services within Identity Federations, particularly with the added safeguard of R&S. However, the GDPR insists that there must be a careful assessment of legitimate interests before that purpose is used. The following table shows some areas that should be used to make this assessment, and demonstrates how the R&S Entity Category can help organisations make this determination. The GÉANT Code of Conduct also has some useful information on good practice for home organisations.

Issue	Discussion	Review of R&S
Put in Place Safeguards	Data minimisation (necessary), privacy enhancing technologies (for example pseudonyms), transparency and a right to opt-out.	R&S addresses all of these areas. The Code of Conduct also has information on necessary attributes. We'd also recommend reviewing the Privacy Notice of an SP and encouraging them to populate privacy statement URL in metadata.
Balance the Rights of Data Subjects and the Rights of Data Controllers	Ensures the necessary flexibility for data controllers for situations where there is no undue impact on data subjects, while at the same time providing sufficient legal certainty and guarantees to data subjects that this open-ended provision will not be misused. The stronger the legitimate interest being pursued by the data controller and the less harm the processing does to the interests of the data subject, the greater the likelihood that the activity will be lawful.	R&S addresses this by limiting the types of services that are allowed to claim this category and focusing on low-risk services that have a clearly identifiable need for personal information such as wikis etc.
Impact Management	Impact on the individual will depend on the nature of the personal information, how it is processed and what the individual would reasonably expect.	Controlled in the R&S use case by minimal attribute sets and stress on the concept that attribute must not be asked for if it is not needed.
Define the "legitimate" reasons?	Norms in the community concerned falls in to this definition, as does the idea of both parties wishing to provide and receive access. Those claiming legitimate interest should be able to explain their interest and how it satisfies this balancing test	R&S provides this reason in its definition to support the process and to ensure that release is happening against an agreed set of criteria.
Ensure Transparency	Relying on legitimate interests still means users have to be informed about what their personal information is being used for. Privacy notices should still be put in place by IdPs and SPs.	Transparency is provided by keeping lists of SPs in this category and clear descriptions of what is being released.
Case-by-Case	Legitimacy must be ensured for each service.	Each SP is considered on a case-by-case basis by the federation in question and reviewed annually.

G. The "Balance" Test

In order to meet the requirements of the Legitimate Interests, the Article29WP suggests using the following balance test. The onus is on each home organisation / identity provider to carry out the balance test, but using R&S effectively helps organisations "pre-fill" this in. Whilst legitimacy must be ensured for each service, we suggest that organisations only need to carry out the balance test once for all R&S services as the services are vetted both at Federation level and in an annual audit by REFEDS.

Step One

Assessing which legal ground may potentially apply under Article 6.

- Review the six processes above to ensure that legitimate interests is the best model for moving forward.
- Federations should not allow Service Providers to use the R&S tag unless they can prove a legitimate interest in the minimal data set used by R&S.

Step Two

Qualifying an interest as 'legitimate' or 'illegitimate'.

- Is it lawful (i.e. in accordance with EU and national law)?
- Is it sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e. sufficiently concrete)?
- Does it represent a real and present interest (i.e. not be speculative)?

Federations should pre-check these criteria when allowing a Service Provider the R&S tag.

Step Three

Determining whether the processing is necessary to achieve the interest pursued.

- Is there a less invasive means to reach the identified purpose of the processing and serve the legitimate interest of the data controller?

Given the minimal data allowed to flow as part of R&S, it is unlikely that a less invasive approach would be found.

Step Four

Establishing a provisional balance by assessing whether the data controller's interest is overridden by the fundamental rights or interests of the data subjects.

- Consider the nature of the interests.
- Evaluate any possible prejudices.
- Take into account the nature of the data requested (how sensitive?).
- Take into account the nature of the data processing (how stored, profiled, where shared).
- Consider the data subjects' reasonable expectations.
- Evaluate the impact on the data subject.

As Service Providers must meet the definition of an R&S entity as described in the entity category, these conditions should be met.

Step Five

Establishing a final balance by taking into account additional safeguards.

- Identify possible safeguards that are in place (data minimisation, technical and organisation design, pseudonyms, transparency).

The design of identity federations and the privacy-by-design and data minimisation processes used in R&S meet these requirements.

Step Six

Demonstrate compliance and ensure transparency.

- Document the process (i.e. pages on your wiki about the R&S Entity Category and members).

Federations, Service Providers and Identity Providers are encouraged to document their usage of R&S in an appropriate public space.

Step Seven

What if the data subject exercises his/her right to object?

- Have a process to address opt-out.

Identity Providers need to be able to demonstrate a mechanism for users to opt-out of data release. This can include scenarios where users lose access to the service.

H. Use of R&S Outside of Europe

The GDPR claims that it should be followed by "controllers and processors in the Union" (Recital 22) and controllers and processors "processing the data of data subjects who are in the Union" (Recital 23), although it is not clear how organisations outside of the EU will be made to comply with the requirements. This means the requirements of the GDPR impact nearly all participants in Identity Federation, as most will have some users accessing services within the EU. Where transfers are happening outside of the EU, the GDPR allows for this to happen under one of three possible headings:

- On the basis of an adequacy decision (Article 45).
- Subject to appropriate safeguards (Article 46).
- Subject to a derogation (Article 49).

Adequacy Decision

Countries and processes covered by an adequacy decision are clearly defined and documented. At the time of writing these countries are: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the ~~US (limited to the Privacy Shield framework)~~. Transfers to these countries can be made using the same criteria as any EU country. Since July 2020, the US Privacy Shield has been determined invalid for international transfers.

Safeguards

Article 46 sets out a series of safeguards that can be used to permit transfer to a third country or international organisation. These are:

- A legally binding and enforceable instrument between public bodies.
- Binding Corporate Rules.
- Standard data protection clauses adopted by the Commission. The wording for these contracts can be found here.
- An approved Code of Conduct.
- An approved Certification mechanism.

Of these, only the Code of Conduct approach is used significantly at this point in time in our community. Guidelines are being developed for the use of Binding Corporate Rules and Certification but it may be some time before they can be practically used by organisations.

GÉANT is exploring a Code of Conduct that can be used at international scale. This could be used in conjunction with R&S to support data transfer to third countries and international organisations. As things currently stand, the Dutch Data Protection Authority has declared that it will not be possible to have a Code of Conduct for GÉANT that covers both EU transfers and non-EU transfers.

REFEDS is actively following guidelines on Certification to see if R&S can be consider a certification approach in the future. This is likely to be a lengthy process.

Derogation

The Article 29 Working Party have provide guidelines for the use of derogation under Article 49. The Article lists a series of potential derogations that could be used for transfer, but many of these will not prove adequate for federated access management.

- **Consent can be used**, but this must fulfil all the usual GDPR requirements ***plus*** "explicit" rather than just "unambiguous" and "informed" must include "about the specific risks" arising out of the transfer. The Article 29 Working Party points out that this "might prove not to be a feasible long terms solution for transfers to third countries".
- **Contract with Data Subject is permitted** but only for "occasional" transfers, must be a "direct and objective link" between the data and the performance of the contract (i.e. works for travel agent telling hotel you're coming, but not for choosing to host your personnel system in another country).
- **Compelling legitimate interests** can be used, but this must demonstrate that no other option works. Data controller's interests must be "compelling" (example is "to protect organisation or systems from serious immediate harm") and balanced against any risk to the data subject's rights and freedoms. Must only apply to a subset of data subjects, and must apply additional safeguards.
- One of the outstanding issues for use of legitimate interests as a derogation is that the controller is required to inform the supervisory authority of the transfer. This is not scalable at any level and is recognised as problematic in the Working Party document.

Use of legitimate interests as a derogation for federated access management exchanges to third countries does meet many of the obligations:

- There is no access on a general basis to a database of users.
- The access only covers minimised data of the single user who has chosen to authenticate that way and should already have been informed of the consequences.
- There are individual safeguards: we minimise, pseudonymise, encrypt and put in place rules for which the data can be used.
- Retaining data is actively counter-productive – the main benefit for the data importer is that they can get fresh data every time the individual logs in.
- There isn't a "stable relationship between the exporter (IdP) and importer (SP)": each has a relationship only with its own federation. Where there are such relationships (e.g. site licenses) then there's already a contract to put the necessary safeguards in.

It is likely that this area will be subject to much debate and discussion in coming months as GDPR is implemented. Given the lack of maturity of approaches under Article 46 (safeguards), the demonstrable application of safeguards and privacy via R&S and the high-risk impact of other solutions by the user (using commercial logins) there is a strong case to continue using R&S in these scenarios.