DLA PIPER

MEMORANDUM

TO	**:**	Dai Davies, Josh Howlett (DANTE)
FROM	**:**	Patrick Van Eecke, Maarten Truyens (DLA Piper)
DATE	**:**	29 June 2011
SUBJECT	**:**	Data protection analysis eduGAIN project

Based on our meeting of 9 February 2011, we understand that Dante is currently investigating the data protection aspects of the eduGAIN project. More in particular, Dante would like to receive legal guidance on exchanging certain user data – typically pseudonymous identifiers – between home organisations and service providers, not only in the context of national federations, but especially in a cross-border context between entities belonging to separate federations.

This memo is based on the document available on www.edugain.org/policy[1], the sample UK federation agreement[2], the good practices documents for federations[3], and the answers to a few follow-up questions sent by Dante on 21 March 2011. Furthermore, the memo also integrates the additional information and questions contained in the two emails of Mr. Howlett of 25 and 26 June 2011.

Please note that the content of this memo is "jurisdiction-agnostic": it is developed on the basis of the EU Data Protection Directive (95/46/EC), as well as EU-level case law, legal doctrine, and opinions from EU-level bodies such as Working Party 29. As pointed out below, the content of this memo should also be legally screened at the Member State level in order to receive more legal certainty about the viability of what we propose in this memo.

1. Our understanding of the facts

1.1 Home organisations, service providers, federations and eduGAIN

In the context of the Géant network, research institutions and education institutions (together "**home organisations**") need to provide their **end-users** (students, staff, alumnus, affiliate or library walk-in) with access to various electronic services that are of interest to the end-users (typically, but not exclusively, scientific information services). Instead of asking end-users to directly provide login credentials to each **service provider**, the home organisations and service providers are grouped into "**federations**", which provide structured data structures and data flows in this regard. For example, the

---

[1] Introduction to the eduGAIN Policy Framework, the eduGAIN Declaration, the eduGAIN constitution, and the eduGAIN Data Protection Good Practice Profile.

[2] www.ukfederation.org.uk/library/uploads/Documents/rules-of-membership.pdf

[3] www.terena.org/activities/refeds/data-protection.html: Federated Access Management, Pseudonymous Identifiers, Good Practice for Federated Access Management, and the presentation "Federations and Data Protection".

UK Access Management Federation for Education and Research has over 850 members (home organisations)[4], and connects these home organisations to over 225 services from more than 85 different service providers[5]. Typically, the service providers offer access to various kinds of electronic libraries[6].

The federations standardise the login procedures and the data exchange between the home organisations and the service providers, and allow end-users to rely on a "single sign on" (SSO) to connect to the various services available. The federation publishes a "**federation agreement**", in which basic liability, dispute resolution and data protection provisions are set forth.

Historically, federations have been implemented nationally. In order to foster cross-border cooperation and research, and allow end-users to access the resources of service providers associated with other federations, **eduGAIN** was created as an "inter-federation" that connects the national federations, solves various technical constraints and provides a policy framework. eduGAIN has adopted an **eduGAIN policy declaration** and an **eduGAIN Constitution**, and its members consist of the various federations. Currently, there are over 19 federations, representing thousands of home organisations and service providers, with over ten million end-users.

The data that is actually being exchanged by the parties involved, is twofold:

- On the one hand, data with respect to the end-users (so-called "**attributes**" — e.g., name, e-mail address, status, unique identifier) is directly exchanged between the home organisations and the service providers.

  Note that, although the eduGAIN and the federations define *how* and *which* attributes are exchanged, they are not involved in the actual exchange of the attributes, because the attributes do not pass through the computer systems of the federations or eduGAIN.

- On the other hand, data with respect to the computer systems of the home organisations and service providers (the so-called "**metadata**") is exchanged, in order to allow these computer systems to find and authenticate each other within or across federations, and to find out which attributes are available. eduGAIN recommends the Security Assertion Mark-up Language (**SAML**) technology for exchanging metadata between federations. In this regard, eduGAIN also provides a central "**Metadata Service**", which periodically fetches the available metadata from the participating federations and publishes this metadata to the other participating federations in the form of a combined confederation document containing all of those entities published by each federation.

  It is important to note that eduGAIN only regulates the exchange of metadata *between* federations, and does not attempt to regulate the exchange or distribution of metadata *within* the federations. For example, eduGAIN does not regulate how the metadata that is made available to each federation, is distributed by this federation to the associated home organisations and service providers.

[4] Listed on www.ukfederation.org.uk/content/Documents/MemberList
[5] Listed on www.ukfederation.org.uk/content/Documents/AvailableServices.
[6] A few example services include "Archival Sound Recordings" from the British Library, "English Drama" from Proquest, LexisNexis, NewsBank, SAGE Journals Online, Elsevier ScienceDirect, Westlaw UK, etc.

It is also important to note that the eduGAIN policy framework explains that participating federations and eduGAIN merely exchange metadata, and do not take any responsibility on the content of the metadata, the service the metadata describes or the attributes that are being exchanged (for which the home organisations and service providers are assumed to be responsible).

1.2 Data flows

The data flows described above are intended to protect the privacy of the end-users and minimise the disclosure of end-user data. From the documents at our disposal, we understand that only the strictly necessary information is exchanged (as attributes), and that attributes will be pseudonomised where possible. We assume that pseudonomisation implies in this context that, instead of exposing the actual attributes (e.g., the end-user's name), some code or reference number is made available that is not known to the service provider, but is internally known by the home organisation.

eduGAIN has published technical guidelines built on the SAML technology, which outlines the types of attributes that should be communicated by participating entities. Federations are recommended to at least provide the following attributes about their end-users: the display name, common name (typically first name and last name), email address, affiliation (such as faculty, student, alumnus, affiliate or library walk-in), home organisation and home organisation type. Where relevant for the service considered (e.g., when an end-user's configuration settings must be saved across sessions), a persistent identifier may also be communicated.

In a typical scenario, metadata regarding the availability of these attributes will be provided by the home organisation of the source federation, after which it will be collected by eduGAIN's Metadata Service, and then made available to the target federation. The target federation will, finally, make the relevant metadata available to the service provider considered[7]. As explained above, the scope of eduGAIN's rules does not extend to the distribution of metadata *inside* a federation. Furthermore, neither eduGAIN nor the federations are involved in the actual exchange of attributes between home home organisations and service providers.

The eduGAIN rules also specify that service providers must publish in their metadata the following information:

- the service provider's category, i.e. the indication whether or not the service provider processes personal data from end-users;
- all required attributes from end-users;
- the URL of the service provider's privacy policy; and
- the legal ground for processing the end-user's personal data (either consent or necessity).

[7] In a few specific scenarios, the end-user will directly provide his credentials to the service provider (e.g., where a resource is licensed to particular individuals or where e-mail is used to send results or notices). However, we understand that these situations will be limited.

2. Data protection concepts

2.1 Personal data

The Data Protection Directive defines "**personal data**" in a very broad way, covering any type of data that can be (directly or even indirectly) linked to natural persons. It can therefore be assumed that all attributes that are exchanged between home organisations and service providers qualify as personal data – even when they would be pseudonomised – because the end-user's home organisation can always link the attributes back to the actual end-user[8]. Only attributes that would be completely anonymised (i.e., when even the home organisation can no longer trace them back to the actual end-user) will fall outside the scope of the Data Protection Directive.

Conversely, it can be assumed that most metadata does not qualify as personal data, because it relates to the home organisations and service providers, and not to the actual end-users (a few exceptions apply[9]. As a result, from a data protection point of view, the exchange of metadata *itself* is not subject to specific data protection rules.

2.2 Controllers and processors

2.2.1 Introduction

Almost all of the obligations imposed by the Data Protection Directive apply to the so-called "**data controller**", which is defined as the party that (alone or jointly) determines the purposes and the means of the processing of personal data. Data controllers can, however, delegate data processing duties to one or more "**data processors**", which process personal data on behalf of the data controller.

The qualification of a party as either a data controller or a data processor, is of paramount importance in any data flow. In practice, however, this qualification is often difficult to make. While Working Party 29[10] has clarified the distinction between data controllers and data processors to some extent[11],

[8] In deciding whether or not information qualifies as personal data, Recital 26 of the Data Protection Directive holds that *"account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person"*. Although the home organisations and the service providers are separate entities, we consider them to be sufficiently close to each other in the context of the (inter)federation to decide that it is indeed *reasonable* to assume that a service provider will be able to identify a pseudonomised end-user, if necessary with the help of the home organisation (as the home organisation can internally trace back the pseudo-code to the actual end-user attributes). According to the current position of Working Party 29, one can only assume in strict conditions with strict barriers (e.g., when deontological rules prevent a doctor from sharing patient data with a pharmaceutical company) that Recital 26 will not apply. See Opinion 4/2007 on the concept of personal data, p. 15 (example nr. 13).

[9] For example, when the contact details of a home organisation's or service provider's system administrator would be published as part of the metadata (see also footnote 34). Also note that a few jurisdictions (such as Austria) not only protect data relating to *natural* persons, but also data relating to *legal* persons. For such jurisdictions, obtaining additional local legal guidance is advisable.

[10] Working Party 29 is an EU-level advisory body that consists of representatives of each national data protection authority, as well as a representative from the European Commission and the Community institutions and bodies. The opinions of the Working Party are not binding as such, but have great authoritative value in practice (as there are few other sources of data protection interpretation at the EU level), and are followed by many national data protection authorities.

there remains a significant amount of uncertainty and interpretation issues, with very little legal guidance or case law available. This legal uncertainty should be borne in mind when reading the analysis below. It should also be taken into account that the opinion of the Working Party is not binding as such (although most data protection authorities follow these opinions, if only because the Working Party is mainly composed of representatives of the various national data protection authorities).

2.2.2 Position of Working Party 29

According to Opinion 1/2010 of the Working Party 29, *"being a controller is primarily the consequence of the factual circumstance that an entity has chosen to process personal data for its own purposes"* [12], while the *"determination of the 'purpose' of processing is reserved to the 'controller' – (w)hoever makes this decision is therefore (de facto) controller"*. Throughout the opinion of the Working Party, it becomes clear that defining the purpose of the processing is the most important criterion for assessing whether a party qualifies as a data controller, even though the Data Protection Directive requires that data controller also define the means of the processing.

As regards the "means" criterion, Working Party 29 distinguishes between essential and non-essential aspects. Essential aspects include questions such as *"which data shall be processed?"*, *"for how long shall they be processed?"* and *"who shall have access to them?"*[13]. Conversely, non-essential aspects relate to operational aspects on how the data will be processed — for example, which hardware and software will be used. The decision on non-essential aspects of the means can be delegated by a data controller to a data processor, without any impact on the data controller's qualification.

2.2.3 Applied to eduGAIN

In the context of eduGAIN, we deem the following aspects to be relevant for determining the qualification of the parties involved:

- **Home organisations** initially collect end-users' information for their own purposes (such as staff administration, student management, internal IT management, etc.).

  Home organisations must provide their end-users with certain facilities to enable them to execute their duties or tasks — such as performing research, preparing papers and studying for exams. To this end, home organisations enter into contracts with commercial service providers. In this context, the home organisations will pass on some of the end-users' information they collected to service providers in the form of attributes.

- **Service providers** use the end-user's attributes primarily to check whether access can be granted to the service provider's platform and commercial content. Secondarily, some personal data is also used to deliver the service to the end-user (e.g., to store a user's preferences or send him/her an email).

[11] See Opinion 1/2010 on the concepts of "controller" and "processor" of 16 February 2010.
[12] Opinion 1/2010, page 8
[13] Opinion 1/2010, page 14

- The **federations** define and streamline the relations between the home organisations and the service providers with respect to the exchange of attributes (and metadata). They define the general technical and policy framework that provides authentication to multiple service providers using a single password. However, in the context of this framework, the decision which attributes to actually exchange is ultimately taken by the service providers and the home organisations (whereby the service providers will indicate which data they need, and the home organisations will / will not grant this request).

- Similarly, **eduGAIN**, as an inter-federation, defines a framework for exchanging attributes (and metadata) between home organisations and service providers of different federations. While eduGAIN only recommends a certain technical baseline, the decision which metadata will be exchanged is ultimately taken by each federation.

In our opinion, all four parties simultaneously exhibit both data controller and data processor characteristics. For example, home organisations need to provide their staff and students with certain facilities and therefore enter into contracts with third parties (= defining purpose), and ultimately decide to which attributes access will be granted or denied (= defining which data will be processed). Service providers, meanwhile, use the attributes to protect their own commercial content (= defining purpose), whereby it could be argued that the home organisations fetch attributes from end-users to pass on to the service providers. However, when looked at from a higher level perspective, it could also be argued that service providers act as subcontractors (= data processing) towards the home organisations, because the attributes are ultimately exchanged for the purpose of enabling staff and students to get access to required content. As regards eduGAIN and the federations, they consider themselves as mere facilitators between the home organisations and the service providers, which only transfer metadata on behalf of the home organisations and service providers (= data processing task). However, it would not be correct to really minimize the role of eduGAIN and the federation in the entire data exchange, because they actually define the policy and the technical characteristics of the data exchange, and regulate the rights, obligations and liability of the home organisations and service providers. Such tasks lean towards a qualification as data controller, because they can qualify as "essential means".

Taking into account the interconnections and interdependence between the parties, whereby no party decides on all aspects of the data processing (which data to process, who will have access, etc.), and both the home organisations and the service providers have their own data processing purposes, we think that the home organisations and the service providers (but possibly also the federations and eduGAIN) will qualify as joint data controllers.

Our analysis is supported by the fact that the Working Party seems to lean towards joint controllership in complex cases where the data processing responsibilities of the various parties involved are not clearly delineated at either the macro or the micro level[14] [15]: *"joint control will arise when different parties determine with regard to specific processing operations either the purpose or those essential elements of the means which characterize a controller. However, in the context of joint control the*

[14] See page 17 of Opinion 1/2010: *"Indeed, there are an increasing number of cases in which different actors act as controllers and the definition laid down by the Directive caters for this."*

[15] The Working Party makes an exception for scenarios where the various parties process data in a chain with clear subdivisions. However, in our opinion this exception is not relevant for this memo.

participation of the parties to the joint determination may take different forms and does not need to be equally shared." [16]. Among the few and very heterogeneous examples of joint controllership provided by the Working Party, the following seem relevant for the eduGAIN project:

- **Example nr. 10**[17]: A bank uses a financial messages carrier in order to carry out its financial transactions. Both the bank and the carrier agree about the means of the processing of financial data. The processing of personal data concerning financial transactions is carried out at a first stage by the financial institution and only at a later stage by the financial messages carrier. However, even if at micro level each of these subjects pursues its own purpose, at macro level the different phases and purposes and means of the processing are closely linked. Both the bank and the carrier therefore qualify as joint data controllers.

- **Example nr. 15**[18]: A public authority establishes a national switch point regulating the exchange of patient data between healthcare providers. The public authority is responsible for the actual design of the processing and the way it is used. The plurality of controllers - tens of thousands - results in such an unclear situation for the data subjects (patients) that the protection of their rights would be in danger. According to the Working Party, joint controllership arises.

In light of these examples, we would not agree with eduGAIN's current assumption[19] that only home organisations typically qualify as data controllers, while the service providers will usually qualify as data processors (depending on the service considered)[20]. Even if joint controllership (which we think is the most likely qualification) would not be upheld, we are of the opinion that most service providers will qualify as a data controller, and not as a mere data processor, because the end-user attributes are primarily used to protect the service provider's commercial content.

2.2.4 Consequences

The consequence of the joint controllership is that the four parties involved will be jointly responsible for fulfilling the obligations of a data controller (providing information to users, granting requests for access or correction, notifying the data processing to authorities, etc.). Moreover, each party can be held responsible for the actions and omissions of the other parties. In case of a data breach, for example, joint liability could arise, unless it would be very clear that the responsibility lies with just one specific party (e.g., the service provider).

We would, however, advise not to exaggerate the possible exposure of the federations and eduGAIN due to their possible joint controllership. As we understand that their tasks are essentially limited to defining the overall data flows and governance aspects, we would expect that liability will most likely be limited to cases where actual errors were committed when defining the data flows or undertaking the governance tasks. Taking into account that, based on the information we have at our disposal, both

[16] Page 19 of Opinion 1/2010
[17] *Ibid.*
[18] Page 21 of Opinion 1/2010
[19] See page 15 of the eduGAIN policy framework.
[20] *"when the Service Provider is a subcontractor of the Home Organisation, the Service Provider is a data processor processing personal data on behalf of the Home Organisation. An example of this is if the Service Provider provides licensed content, such as library content or Software as a Service (SaaS), to the Home Organisation"*

the federations and eduGAIN aim to minimize the amount of personal data being exchanged and try to respect the requirements of the Data Protection Directive throughout all operations, the risk for being held liable for basic errors in the data flows seems reasonable.

It remains unclear, however, how courts will deal with this joint controllership in practice, and to which extent a party will really be held jointly liable for responsibilities attached to the other parties. To the best of our knowledge, we are not aware of any case law in this regard to provide further guidance.

2.3 Lawful ground for processing

2.3.1 Overview

According to article 7 of the Data Protection Directive, personal data can only be processed if the data controller can rely on at least one lawful ground. Article 7 provides six different grounds[21] on which personal data can be processed, of which only the following three grounds are relevant in the context of eduGAIN:

- the consent of the end-user (the "data subject");
- necessity in order to execute a contract to which the end-user is a party;
- legal obligation for the data controller to process the personal data;
- the legitimate interests pursued by the data controller (or the other parties to whom the data is disclosed).

2.3.2 Current legal grounds

Based on the documents at our disposal, we understand that eduGAIN currently considers "consent", "contractual necessity" and (to a lesser extent) "legal obligation" to be the relevant legal grounds to process personal data[22]. For example, the Data Protection Good Practice Profile explains on page 5 that service providers should assume that *"a service that is related to an employee doing his work is usually based on necessity"*, while *"a service that is related to a student taking his courses and otherwise being educated is usually based on necessity"*. In our opinion, reliance on these three legal grounds is difficult and presents various practical and legal issues:

- Assuming that the service provider would qualify as an independent (instead of a joint) data controller, we believe that the "contractual necessity" legal ground cannot be invoked in the relation between the service provider and the end-user, because the end-user is not a party to the contract between the home organisation and the service provider.

[21] Please note that other legal grounds for processing apply in case so-called "sensitive personal data" would be processed (such as information relating to someone's health, philosophical beliefs, sex life, etc.). However, based on the information at our disposal, we have no reason to believe that any end-user metadata would qualify as sensitive data.
[22] See, for example, page 3 of the Terena Federated Access Management document.

Accordingly, this legal ground can only be used in case the service provider enters into a separate contract with each end-user, for example when the service provider would impose separate terms & conditions.

However, even in such cases, reliance on this legal ground may be doubtful, because the service provider will not likely qualify as an independent data controller. When joint controllership would apply between the home organisations, service providers, federations and eduGAIN, reliance on this legal ground becomes uncertain.

In addition, it must be investigated whether all of the attributes are truly necessary for the service provider in order to execute the contract. In general, the necessity requirement is interpreted quite strictly.

- The consent of the end-user must be *"freely given, specific and informed"* [23]. It is questionable whether an end-user can really be deemed to have given his/her free consent in cases where the use of the service is a necessity for the end-user (e.g., to receive access to certain resources).

  Furthermore, according to Working Party 29[24], consent is only freely given when it can be withdrawn by the end-user[25]. Accordingly, either the service provider itself or the other parties involved in the data exchange should provide facilities to allow an end-user to withdraw his/her consent for the processing.

  Moreover, reliance on the legal ground of consent has the drawback of administrative overhead: in general, end-users will need to be presented with an "I accept" button or checkbox (which must not be pre-checked), and service provider will need to store each end-user's consent (because the burden of proof lies with the data controller). Based on our meeting, we understand that many service providers do not currently impose mandatory acceptance of their terms & conditions.

- It is difficult to envisage situations in which the "legal obligation" legal ground can be invoked. This may, for example, be the case when local legislation would require a service provider to store certain user data in order to allow the user to access certain types of information (e.g., confidential data). However, from our understanding of the eduGAIN project, these situations will be very exceptional. In addition, this legal ground may present difficulties in case of joint controllership, because even if a legal obligation applies, it will likely only be relevant for one single party.

2.3.3 "Legitimate interests" legal ground

Taking into account the various issues associated with the legal grounds of consent, necessity and legal obligation, and considering Dante's desire to find a more practical solution, we are of the opinion that in most cases the "legitimate interests" legal ground can be used (article 7.(f) of the Data Protection Directive). This legal ground can be invoked when the processing is necessary for the

[23] Article 2.(h) of the Data Protection Directive
[24] Working document on a common interpretation of Article 26(1) of Directive 95/46/EC, p. 11.
[25] Working document on a common interpretation of Article 26(1) of Directive 95/46/EC, p. 11.

purposes of the legitimate interests pursued by the data controller (or by the third party or parties to whom the data are disclosed).

This legal ground has the advantage that no formalities must be fulfilled, and that it can also be used when joint controllership would apply. The drawback of this legal ground is, however, that it involves some legal uncertainty: article 7.(f) of the Data Protection Directive explains that it cannot be used when the legitimate interests of the data controller are overridden by the interests for fundamental rights and freedoms of the data subject.

It must indeed be acknowledged that data protection authorities often frown upon the use of this legal ground, because it is frequently used by data controllers to justify dubious processing for which no of the other legal ground is applicable. For eduGAIN, however, we think that this legal ground would be justified. (For the avoidance of doubt: even when eduGAIN would rely on this legal ground, all the other obligations of the Data Protection Directive would continue to apply, such as the information obligation towards data subjects, access and correction rights, security of processing, etc.)

Working Party 29 explains that article 7.(f) requires a balance to be struck between the rights and interests of the data controller and the data subject, which should take into account issues of proportionality, subsidiarity, the consequences for the data subject[26], as well as the risks posed for the data subject's privacy[27]. The Working Party also stresses that compliance with the other obligations of the Data Protection Directive is important, and that in some situations additional safeguards may be necessary to justify reliance on article 7.(f). Similarly, the European Commission[28] refers to the nature of the data, the nature of the processing, and the measures which the controller has taken to protect the interests of the data subject.

While the Working Party has not yet provided any extensive explanations on article 7.(f), the following examples can serve as useful illustrations. According to the Working Party, article 7.(f):

- can be used as a legal ground by search engines to store user queries for system security and fraud prevention purposes;
- cannot be used as a legal ground for sending spam to email addresses found in a public on the internet (e.g., on a forum)[29];
- can be used as a legal ground by a financial transaction processor such as SWIFT to grant a foreign government access to financial transactions from European citizens[30], when faced with subpoenas. However, due to the "hidden, systematic, massive and long-term" manner in which SWIFT gave access to the US government, the Working Party considered that article 7.(f) could not be relied upon by SWIFT.
- can be used as a legal ground to justify the transfer of personal data to the United States, in order to be used in US pre-trial disclosures[31]. The Working Party recommends that data controllers

[26] See Opinion 4/2006 (14 June 2006), page 6.
[27] See opinion 5/2000, page 5.
[28] First report on the implementation of the Data Protection Directive, COM (2003) 265 final, Analysis and impact study on the implementation of Directive 95/46/EC in Member States, page 10.
[29] Opinion 1/2000, page 4.
[30] Opinion 10/2006, pages 18-19.
[31] Working document 1/2009, page 10.

should anonymise or pseudonomise the data in a first step. However, after filtering the irrelevant data, a limited set of personal data could e disclosed as a second step.

- can, in principle, be used as a legal ground for video surveillance[32]. However, the Working Party nevertheless recommends to investigate whether there would be interests that deserve protection that may be in conflict with the installation of the video surveillance system.

Legal doctrine also provides a few examples where reliance on article 7.(f) would be justified[33], for example for company-wide internal employee contact databases or company database with assessment information of high-ranking employees[34].

In light of these examples, we believe that reliance on article 7.(f) is generally justified for the eduGAIN project, for the following reasons:

- The main purpose of federated identity management, as implemented in the eduGAIN project, is to protect the privacy of end-users and to minimise the amount of data being exchanged. Instead of having users directly provide credentials to service providers, the home organisations will channel the data exchange through identity providers.

- Based on the documents we have reviewed, we understand that the current policies and frameworks fully support the aims of privacy protection and data minimisation. For example, service providers must explicitly indicate through the SAML protocol which end-user attributes are required, and will not receive any additional information. Furthermore, pseudonomisation will be used whenever possible.

- While it should be assumed that all attributes qualifies as personal data, we consider the actual information being exchanged (name, affiliation, email address) and the types of services and content accessed by the end-users (mainly scientific) to be rather innocuous, in particular when this metadata would be (partially) pseudonomised. A completely different assessment would apply when health-related data would be exchanged, or when the federations would give access to personal banking services.

- As a result, we think that, in general, there are no overriding fundamental rights of end-users that would prevent reliance on the legitimate interests legal ground. We would, nevertheless, advise to take some additional safeguards, as explained below.

3. Conclusions

1. All attributes exchanged between the home organisations and the service providers qualifies as personal data, to which the requirements of the Data Protection Directive apply. As a result, the

[32] Working Document on the processing of personal data by means of video surveillance, adopted on 25 November 2002, pages 15-16.
[33] C. KUNER, *European data protection law – corporate compliance and regulation*, second edition, page 247.
[34] In our opinion, this example would also apply to the contact details of the system administrators that are included in the metadata that is exchanged through the federations and eduGAIN (which can be considered a closed user group). While it is advisable to additionally obtain each system administrator's consent (and to at least to duly inform him/her about the fact that the contact details are included in the metadata), it should be

"data controller" must comply with the various obligations imposed by the Directive, such as duly informing end-users, giving them access and correction rights, adequately protecting the attributes, anonymising attributes that are no longer necessary, etc. Most importantly, however, the data controller must find at least one legal ground to rely on for processing the attributes.

2. The metadata that is made available by the federations and by eduGAIN, does not generally qualify as personal data, because it does not relate to actual natural persons. Only limited exceptions seem to apply (e.g., when the contact details of an IT administrator would be included in the metadata).

3. In the context of the eduGAIN project, it is difficult to pinpoint which of the parties involved (home organisations, service providers, federations or eduGAIN) qualify as "data controller", i.e. a party responsible for the data processing. However, taking into account the fact that all of these parties contribute to the data flows and the data structure, we lean towards the assessment that **at least the home organisations and the service providers, but possibly also the federations and eduGAIN qualify as data controllers**. Moreover, in light of the interdependence of the parties and the current tendency of advisory bodies such as Working Party 29 towards joint responsibility, we think that **it is likely that the controllers will be considered joint data controllers**. This results in a situation where each controller may be held responsible for the acts and omissions of the co-controllers. However, because the role of the federations and eduGAIN in the entire set of operations is fairly limited and delineated (mostly defining data structures and general governance), their risk for being held co-responsible should not be exaggerated. Nevertheless, it should be noted that little legal guidance is currently available in this regard.

4. As regards the legal grounds for processing, we understand that "consent" and "contractual necessity" (and, to a lesser extent, "legal obligation") are currently used by eduGAIN and reflected in its data structures. However, **both "consent" and "contractual necessity" are difficult to rely on** in the eduGAIN project:

- As for consent, it is doubtful whether the end-user's consent is always freely given when a user would be obliged to use the service for his/her research or studying purposes. In any case, managing consent can be difficult because an additional steps must be taken towards the end-users, and records of consent and withdrawal must be kept.
- As for contractual necessity, it is doubtful whether there is really a contract between the data controller and the end-users, even when only the home organisation or the service provider would qualify as a data controller. Moreover, "necessity" is interpreted quite strictly, so that it may not be the case that all attributes that are currently exchanged between the parties, pass the test.

5. Instead of relying on "consent" or "contractual necessity", **we recommend to generally rely on the "legitimate interests" legal ground**. While this legal ground involves a balancing exercise (and, therefore, some level of legal uncertainty), reliance on this legal ground seems justified for the eduGAIN project, taking into account the general privacy-protecting setup of the data flows in the project, the low level of risk posed by the personal data being exchanged, and the innocuous (mainly scientific) types of services access by the end-users. Reliance on this legal ground has the advantage

---

noted that consent is often contested in the context of an employee / employer relationship; hence the reliance on the "legitimate interests" legal ground.

that no administrative overhead is involved, and that it can be applied regardless of how the qualification as (joint) data controller would turn out. Irrespective of the legal ground that would be used, all the other obligations of the Data Protection Directive must also be complied with, such as the information obligation towards data subjects, access and correction rights, security of processing, etc.

4. Recommendations and next steps

- While we are convinced that there are sound legal arguments why the "legitimate interests" legal ground is appropriate for the eduGAIN project, its viability should be further assessed at the level of each EU Member State. As discussed during our meeting, we would be happy to involve the colleagues from our network in this regard.

- While the documents we investigated point out that the parties involved in the eduGAIN project must take appropriate measures to comply with the various data protection obligations (such as right of information, right of access / correction, etc.), it should be investigated whether this is effectively the case. As pointed out above, in assessing whether the legitimate interests legal ground applies, data protection authorities attach great importance to the fact that the interests and fundamental rights of the data subjects are actually guaranteed.

- While we assume that the attributes that are currently exchanged is strictly limited to what we described in section 1.2 above, and while we understand that the types of services that are currently made available are mainly scientific, it should be further investigated at the level of the individual federations whether there are no exceptions for which the balance of interests would turn out differently. For example, if for some services sensitive data would be exchanged, then reliance on other legal grounds may be necessary for such cases.

- The documents we investigated provide a basic understanding of EU data protection legislation. However, taking into account the fast evolution of this field of law, we would recommend to have the current documents screened and updated. Considering the consequences of joint controllership, we would also recommend to reconsider the rights and obligations agreed in the eduGAIN Constitution and policy documents, in order to minimise the consequences of joint liability issues. Please let us know whether we can provide any assistance in this regard.

* *

*