Managing Data Protection Risks Using the Code of Conduct

Contents

1. Introduction

Many Federations started out with most of the member Service Providers being commercial content providers; at some point that plateaued (ie all the likely publishers had joined the Federation) and Federations began to see other types of Service Providers joining the Federation. The second wave seemed to have two types of Service Providers: a) non-publisher commercial Service Providers (eg outsourced or cloud-based services), and b) campus-based Service Providers supporting research. In virtually all situations involving commercial Service Providers of any sort there will be a contract betwen the campus and commercial entity. That contract should assign responsibilities and address risk-relaed issues.

However, it seems likely that the last category ("campus-based Service Providers supporting research" and Virtual Organizations) will be a big growth area in coming years, and perhaps the most problematic with respect to the data protection directive. It will be very difficult to get a signed contract between those Service Providers and every Home Organisation with a researcher that wants to access them; many researchers will be unwilling to tolerate the delays involved in moving a set of such contracts through the legal process at their campus.

This will likely result in a situation where all parties are facing some unmanaged risks and liabilities. This document describes what happens and who suffers if someone fails to fulfill their requirements. This document also suggests an approach (the Code of Conduct) that can be used by Home Organisations and Service Providers to minimize the risk that arises from depending on each other. Acting without an absolute assurance creates risk and potential liability; the suggested approach atempts to minimize that risk.

2. Goals

The goal is to facilitate easy sharing of appropriate end users' Attributes by his/her Home Organization with remote Service Providers in a manner that is consistent with law and accepted practice, and minimizes the risk for all parties.

1. Create an environment where campus users can expect to successfully login and enter destination Service Provider sites that use Attribute values asserted by their Home Organization
2. Allow all parties to remain sufficiently compliant with regional and national laws and regulations guarding personal privacy in order for the risk of non-compliance to be acceptable to all the parties. Find an appropriate balance between risk and value for all parties.
3. Provide suggestions to Federations, Home Organisations and Service Providers on Business Practices that are believed to be consistent with the EU data protection directive and its interpretations.
4. Provide suggestions that would allow Attribute release to a Service Provider in EU/EEA.

3. Approach

This paper is most definitely NOT a legal opinion, and should not be relied on as such. A recommendation with no guarantee is the best we can ever have.

3.1. The Highly Collaborative Research and Higher Education Environment

The standard approach to achieving minimum risk under the EU Data protection directive would expect contracts between a Home Organisation and the entities responsible for every Service Provider accessed by every member of its community. Those contracts could, among other things, identify and assign responsibility for all the remaining risks so the risk to each organisation could be determined in advance.

For some situations in the Higher Education/Research environment, however, this approach is totally impractical. Campuses are not collaborating -- individual researchers are. Legal staffs at campuses would not have the time to review contracts with every Service Provider that every researcher wants to access; researchers would not wait (and put their work on hold) while legal staffs reviewed contracts. In some cases, the organization operating the Service Provider may not be a legal entity, and will have problems in finding a proper signer for an agreement.

In addition, in essentially all collaborative research situations, the participants have NO interest in hiding their identity. Instead, a researcher wants his/her name attached to his/her contribution, because it is a merit for him/her as a researcher and benefits his/her academic career. The EU guidelines were developed to protect people from unwarranted pressure to share too much information. These two incentives need to be balanced.

The approach suggested in this document for research situations is based on balancing the legal risks arising out of non-compliance against the risks to scholarship by hindering access to important resources. Service Providers that follow the recommendations should find it easier to persuade Home Organisations that the risk of releasing Attributes is justified by the benefits that the services can provide. Of course, this process is made simpler if a Service Provider decides to accept lower risk kinds of data.

Operating with less than perfect compliance means that there will be non-zero risk. Responsibility for failure will fall wherever the legal system assigns it, which may not be the "obviously guilty" party. For example, the EU Data protection directive may assign responsibility to the Home Organisation if a Service Provider spills data due to poor practice.

3.2. Using Contracts to Further Minimize Risk

The EU Data protection directive does not explicitly require a contract between a Home Organisation and Service Provider. However, a contract would always be the safest and most predictable way to achieve Minimum risk. According to the UK Information commissioner, *"A decision to share personal data with another organisation does not take away your duty to treat individuals fairly. So before sharing personal data, you should consider carefully what the recipient will do with it, and what the effect on individuals is likely to be. It is good practice to obtain an assurance about this, for example in the form of a written contract."*

When a bilateral contract is in place it should a) assign roles, b) assign responsibility for the various responsibilities and risks, and c) define the role of the Service Provider as a data controller or processor. Without a bilateral contract, it will generally be assumed that the Service Provider is acting as a Data Controller.

However, it is not uncommon that even if there is a contract already in place that it completely ignores data protection issues. See, for instance, the JISC model licenses on digital contents for education and research.

3.3. EU Data Protection Law as the Starting Point

In developing these recommendations the working group has proceeded on the assumption that the combination of the EU Data protection directive and the European national laws that implement it will present the most challenging environment within which these recommendations will have to operate. Consequently, this document will frequently reference EU concepts and models. The assumption is that no other country or region will present scenarios that cannot be met by following these recommendations.

Therefore, the reader needs to notice that the jurisdiction has a significant impact to the application of this Code of Conduct. This Code of Conduct does not introduce new obligations to a Service Provider in European Union and European Economic Area (EEA), because they are already bound by law to most requirements imposed in the Code of Conduct. The role of the Code of Conduct is

1. to signal, that the Home Organisation and Service Provider are aware of the legal requirements, and
2. where appropriate, make a practical division of responsibility between the Home Organisation and Service Provider to ensure the legal requirements are met in a scalable and user-friendly way.

However, for a Service Provider in a jurisdiction outside EU/EEA, this Code of Conduct actually proposes new responsibilities which extend the requirements in local laws. Therefore, releasing Attributes from a Home Organisation in EU/EEA to a Service Provider outside EU/EEA (and outside countries with adequate data protection like Switzerland) is likely to require stronger guarantees (For instance, the model contracts of European Commission) than what the Code of Conduct currently offers.

3.4. A Global Approach Needed

The ultimate goal of this effort is to develop a framework that would allow interoperation between parties around the world, not just within the EU. As we collectively edge toward an inter-federated mesh-like world, most federations will have to adopt a set of practices compatible with those Federations which have adopted the strictest set of rules. That means that Home Organisations in some countries may be releasing Attributes to Service Providers in countries with much looser privacy laws. The approach described by this effort would require Home Organisations and Service Providers to signal to each other their compliance with a specific set of operating rules.

It is likely that there are other approaches to addressing these risks that would be judged to be acceptable. However, global inter-operation will succeed only by adopting a single approach. There is a need for broad consensus around a deployment profile that describes the technical mechanisms to address these requirements. Partial implementations of the agreed upon profile are unlikely to inter-operate (either technically or legally). Federations, Home Organisations, and Service Providers must work out their preferred balance of following the common recommendation as opposed to bilateral hacks.

4. When Does Risk Arise?

The Introduction to Data protection directive document, in Section 13, provides a summary of specific requirements from the Data protection directive for both Home Organisations and Service Providers. Clearly a party is at risk if it does not directly address the requirements associated with its Role.

In an ideal world, 1) all the parties would meet their respective privacy-related requirements, and 2) all parties can assume that all the other parties are also meeting their privacy-related responsibilities. There would be no security incidents; no end users would think that their privacy had been injured.

In practice, that world does not exist. Because each party is dependent on correct behavior by the other party, it is necessary to develop a design that 1) provides all parties with sufficient assurance that other parties with which they are interoperating are meeting their privacy-related responsibilities, and 2) is able to tolerate and recover from incidents and misbehaving entities.

In situations lacking a contract, each Home Organisation must determine its risk appetite. The regulations assume that each Home Organisation will assess the risk with each Service Provider. In the absence of any additional information, suggestions, or hints, it is reasonable to assume that a) very few Home Organisations would be able to assess every potential Service Provider, and b) the set of Home Organisations that do assessments will produce a variety of answers. From the Service Providers perspective this approach is not scaleable; it will result in too much uncertainty and variation. The problem for Service Providers in this environment is that they cannot know how many Home Organisations are going to be willing to release, so they will always have to cope with less than 100% coverage of its users.

4.1. Summary of Home Organisation and Service Provider Responsibilities

Both the Home Organisation and the Service Provider have specific responsibilities.

Introduction to Data protection directive, section 13, Provided a complete list of concrete design requirements for Attribute Release. The responsibilities of the Home Organisation include but are not limited to:

1. MUST take necessary measures to protect personal data, in particular when it is transmitted over a network.
2. MUST have confidence that all of the Attributes requested by the Service Provider are relevant to the service.
3. The user MUST be INFORMed when Attributes are being released.
4. The user MUST give his/her CONSENT when Attributes can be released due to the user's consent legal grounds.
5. There are a number of specific requirements around the CONSENT interaction.
6. There are additional requirements if the Service Provider is located outside the EU/EEA.

The responsibilities of the Service Provider include but are not limited to:

1. MUST take necessary measures to protect personal data, in particular when it is transmitted over a network.
2. MUST only process personal data when there is a good reason to do so.
3. MUST publish the list of Attributes that are **adequate, relevant and not excessive** to the Service.
4. If it needs just one or some particular value(s) of an Attribute, it MUST indicate which value(s) (for instance, eduPersonAffiliation="student").
5. MUST specify the legal grounds for the processing of each Attribute that it requests.
6. MUST provide their **Service Provider's Privacy Policy**.

Clearly, both the Home Organisation and the Service Provider have specific responsibilities which they must meet.

4.2. Description of the Risks

In addition to their own responsibilities, however, both the Home Organisation and the Service Provider must be assured that that the other party is also meeting its responsibilities. Some examples:

1. A Home Organisation cannot release information to a third party without "implement(ing) appropriate ... organizational measures" to ensure that it does not result in unlawful processing (Article 17(1)). There are several different items that the Service Provider must address before the Home Organisation can release attributes.
2. If an Home Organisation releases Attributes using the CONSENT legal basis, then the Service Provider MUST KNOW that the user has given his /her consent before (not after) the release takes place (Working Party 29's opinion on consent, page 9). The Service Provider could present a CONSENT dialog before transferring the user to the Identity Provider, or it could use a signal from the Identity Provider that convinced it that the Home Organisation had presented a CONSENT dialog. Without one of those options, the Service Provider does not know that there is a legitimate grounds for their processing; in this case the Service Provider may be in breach of Article 7(a).
3. A Service Provider cannot process received personal data unless it is confident that the Home Organization has met its privacy related responsibilities. (For CONSENT Article 7(a) implies these responsibilities; for INFORM, Article 11 defines the responsibilities if the Service Provider is a Data Controller; for INFORM there are no Service Provider responsibilities if the Service Provider is a Data Processor.)
4. If the Service Provider is a data controller, Article 11 requires it to inform the end user on processing his/her personal data. A normal practice is to present a link to the service's Privacy policy in the service's landing page. However, Article 11 also allows "except where [the data subject] already has [been informed]". Consequently, if the Service Provider is sure that the user has been INFORMed then the Service Provider does not risk breaching Article 11 by not doing the INFORMing itself.

Without a mutually agreed upon framework, the Home Organisation and Service Provider may each take steps that duplicate actions taken by the other party; the result will surely negatively impact the user experience, possibly causing confusion.

Alternatively, a Service Provider may be willing to process Attributes without any contract or signal, concluding that if the Home Organisation *does not* do its part then the Home Organisation will actually have committed a more serious breach of the law. Unfortunately the difference in national interpretations and enforcement means you cannot rely on both Home Organisation and Service Provider coming to the same risk assessment.

4.3. Legal Description of the Risk

In EU countries, enforcement of the relevant national laws is done by courts and the appointed Data Protection Authorities. The authorities' approaches and powers are different in the different countries, and in some countries their powers are actually changing in time as well (e.g. UK Information Commissioner's maximum penalty has gone up from £5K to £500K and there is a proposal that it should also include imprisonment).

If a Service Provider is hacked and personal data is leaked to the Internet, it is natural to assume that the Service Provider is responsible for the inadequate security and protection of its systems. However, in addition to that, it is also possible that the Home Organisation has neglected its responsibilities because it has decided to release personal data to the poorly maintained Service Provider.

Two different risks can be identified in Attribute sharing situations:

- **Regulatory Risk**
  - The regulator could penalize the Home Organisation for an unlawful disclosure of personal data.
  - Using the wrong basis for processing (consent vs necessity as defined in Article 7) or not complying with the requirements of the chosen basis could get a party penalized by the regulator.

    - Some regulators are likely to consider that some kinds of personal data should not be disclosed unless there's a contract between the parties. In this case there's a risk that the regulator will order that the disclosure stop until there is a contract.

- **Harm to Users**
    - If the release of Attributes causes harm to a person he/she can sue the Home Organisation, possibly even if the harm is the Service Provider's fault.
    - If a Home Organization is clearly not taking care of personal data they could be penalized by the regulator even before any harm occurs.
    - Potentially, a contract between the Home Organisation and the Service Provider could transfer the "Harm to Users" risk from the Home Organisation to the Service Provider (e.g. who bears the cost of the court case and paying the damages). Without a contract, the Home Organisation alone bears this risk. Presumably, before signing such a contract, the Service Provider needs to have both a reason to accept the risk and some ability to control the level of risk it is accepting.

Article 17 of the EU Data protection directive recognises risk-based decisions around Attribute release. It introduces the idea that the measures required to protect personal data can be lower for low-risk-attributes:

Article 17. Security of processing. 1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

5. Managing Risk with the Code of Conduct

The Code of Conduct assumes that the Service Provider is acting as a Data Controller. It then explicitly assigns specific responsibilities to the Home Organisation and the Service Provider, and declares that certain mechanisms are out of scope (eg user consent as a legal basis for attribute release). As a result, Service Providers are in no way dependent on the actions of an Home Organisation. Lastly, it defines a mechanism that Service Providers can use to state that they are operating in compliance with the CoC.

The Service Provider publishes a unilateral statement that it operates in conformance with specified rules and practices (which are derived from the directive). The intent is to reassure Home Organisations that the Service Provider is operating in a lawful manner and that the risk of disclosing Attributes to this Service Provider is acceptably low.

The specific text of the generally approved Code of Conduct can be found in Code of Conduct for Service Providers. These are the statements that a Home Organisation would ask to be included in a contract, if there were a contract. Minimally, the Home Organisation must be assured that all the processing being done by the Service Provider is lawful and provides appropriate privacy safeguards.

A Home Organisation could conclude that the risk of releasing Attributes to an Service Provider which has published such a statement is acceptably low, even though the two parties have not signed a bilateral contract.

If Attribute release is not based on consent, the Home Organisations do not need to make a unilateral statement to the Service Providers. Otherwise, the model must include also a way that an Identity Provider signals to a Service Provider that user CONSENT processing has been performed.

BENEFIT

The model scales well. The model is not limited to a particular (inter)federation deployment, such as eduGAIN.

RISKS

The law that the regulator(s) will be concerned with talks about a "contract *between* the parties", not a declaration by one of them. Consequently, the Declaration should have some "standing" in order for courts to consider this as a viable approach. Care should to be taken, though, to understand where liability is placed as a result of the approach taken to establish some standing for the text of the Declaration.

Without a contract, it is difficult to impose penalties on misbehaving parties. The Handling non-compliance document that is a part of the CoC recommends several approaches when a party suspects that another party is not operating in compliance with the CoC.

VARIATION

In a slightly modified approach, the declaration had provisions both for the Home Organisations and Service Providers and both the Home Organisations and Service Providers could commit to it. As an outcome, each Home Organisation and Service Provider who has committed to the the declaration would have a direct contractual relationship, without a need to sign bilateral contracts. This approach would translate the unilateral declaration into a multilateral agreement, but adds some complexity by requiring commitment also from the Home Organisations.

6. Other Possible Models to Manage Risk

Two other deployment models have been identified to manage risk and improve overall manageability. They create different relationships among the parties, and have different characteristics with respect to the EU Data protection directive.

1. Home Organisation and Service Provider have a bilateral contract
2. Home Organisations and Service Providers sign a contract with the same third party

Note that the term "deployment model" refers to each Home Organisation and Service Provider combination. A single Home Organisation could use different models with different Service Providers.

6.1 Home Organisation and Service Provider have a bilateral contract

MODEL In this model there is a bilateral contract between the Home Organisation and the Service Provider. The contract is the proper place to define responsibilities between the Service Provider and Home Organisation. An appropriate contract can remove the risk of regulatory action. This approach reduces uncertainty for all parties, and hopefully results in no or very few uncontrolled risks. Both parties should ensure that the contract addresses

- contains language similar to the Code of Conduct for Service Providers
- the role(s) of the Home Organisation and Service Provider (data controller, data processor, shared role in some fashion)
- which party assumes which aspects of liability,
- identifying which user Attributes and values are shared, and what processing is performed on them,
- require that the Home Organisation agree to perform user INFORM/CONSENT processing
- require that the Home Organisation and Service Provider follow the Metadata recommendations.

BENEFITS

This situation is the best fit with the common interpretation of the EU Data protection directive.

RISKS

However,

- this approach scales poorly, because it expects bilateral negotiations and agreements
- unfortunately, practice has shown that even where contracts do exist (i.e. contracts for the content licensed by the libraries), they rarely cover data protection issues.

VARIATION

This and the model presented in section 5 can be used in parallel. The unilateral declaration signed and published by a Service Provider can act as a baseline. Those Home Organisations which are not satisfied by the quarantees provided by the unilateral declaration can enter into a bilateral contract with the Service Provider.

6.2 Home Organisations and Service Providers sign a contract with the same third party

MODEL

The assumption is that the third party is a Federation, and that the Home Organisation and Service Provider have both signed the Federation's Participation Agreement (PA). Language in the PA could impose specific responsibilities on both Home Organisations and Service Providers. This language could address risk situations. For example, it might require certain specific practices by Service Providers with respect to Attributes that it receives, and impose requirements on how Service Providers process and handle Attributes. (This language could be similar to the eduGAIN Code of Conduct for Service Providers.) The PA might also require Home Organisations to obtain user consent before releasing any Attributes described as optional in the Service Provider's metadata entry.

This kind of language in a Participation Agreement could help Service Providers to persuade Home Organisations that the risks of releasing Attributes to member Service Providers without a bilateral contract are low enough to be acceptable. The Service Provider needs to make the case that the benefit to the Home Organisation of its users accessing the service outweighs the risks to the Home Organisation of uncontrolled Attribute release.

However, this situation is different from a bilateral contract between a Home Organisation and Service Provider. While they both have a contractual relationship with a third party, they do not have any direct legal relationship. Neither can sue the other for breach of contract. The existence of these contracts does not reduce, alter, or change the responsibilities of Home Organisations and Service Providers. The third party may take actions to help Home Organisations and Service Providers manage their service (eg use the metadata to produce Attribute Release Filters for all of the Identity Providers); however, it is still the Home Organisation's choice as to whether or not to use these files (these suggestions from a third party).

Research on how the PAs map data protection issues are made in Federation Policy Mapping.

BENEFITS

Attribute release is based on a contract, not on a unilateral declaration.

RISKS

1. There is no direct contract between an Home Organisation and an Service Provider. It is unlikely that either party could take the other to court and demonstrate injury since there is no contract. The Federation could take a Service Provider to court, but, since it had not been harmed directly, would have to argue that it had suffered other kinds of harm as a result of the Service Providers actions.
2. The addition of a third party complicates the evaluation process when the Home Organisation and Service Provider are in different Federations.

VARIATION

In a more centralised model, the third party does not provide just suggestions but actually negotiates the attribute release policy with the Service Provider on behalf of the Home Organisations and takes legal responsibility of the outcome.

7. Alternative approach: Service Provider categories

The assumption above has been that the reason why Home Organisations hesitate to release Attributes to Service Providers is that they are worried about their data protection related responsibilities. Another, complementary way to ease Attribute release for Home Organisations is to introduce categories for Service Providers.

Service Provider categories wouldn't describe the Service Provider's privacy related practices but indicate the "type" of the service it provides. For instance a service belonging to "Research and Scholarship" category might be relevant for researchers doing their job, and Home Organisations who have a profile as a research institution could consider letting their employees access those services.

In addition, each category might have associated with it a list of suggested possible Attributes. These lists could help both Service Providers and Home Organisations in their thinking about which Attributes might be relevant and useful for a Service Provider.

7.1 The Renater and InCommon model

Renater, the French Federation for higher education and research, has created a process to aid Home Organisations in making their Attribute release decisions. The federation has defined a set of categories (e.g. e-learning resource, groupware service, business application, etc). Each category has associated with it a set of "possible" Attributes for release. The Federation investigates each Service Provider and places them into an appropriate category. In addition, for each Service Provider, the Federation recommends a set of Attributes to be released (which can be narrower than the set associated with the category). The Home Organisation can then decide whether or not to accept the Federation's advice.

Also InCommon has started with one category (research and scholarship) but expects to extend the list. The federation inserts a particular EntityAttribute to the Service Provider's SAML 2.0 metadata to indicate it has been approved to the category.

7.2 Discussion

The approach does not cause the Home Organisations data protection liability to disappear, but may result in a Home Organisation being more comfortable releasing Attributes.

Purpose of processing

According to the EU Data protection directive, Home Organisations have an obligation to ensure that the purpose of processing personal data in the Service Provider does not conflict with the purpose of processing in the Home Organisation. Service Provider categories would enable the Home Organisations to filter out those Service Providers whose purpose is conflicting with that of the Home Organisation.

Data minimisation

It must be clear that all attributes associated with a category are not required by all Service Providers, but are merely a starting point, a potential aid, for evaluating each Service Providers actual requirements. Even with such a structure, it remains clear that:

- Home Organisations may have different views on both the risk and the benefit of releasing a particular Attribute set to a particular Service Provider, so a Service Provider cannot assume that every Home Organisation will be happy to release the Attribute bundle even once they are adopted into the scheme.
- that Service Providers should still endeavour to minimise the subset of attributes they request, as that should increase the likelihood of a Home Organisation being willing to release those attributes.

Those two points are important expectation-setting messages for participants. In addition, it would be important to have those statements made explicitly in case a regulator reviews the situation. If the documentation were to suggest that all Home Organisations were releasing all the suggested attributes to all the Service Providers in a category, whether or not they needed them, then that situation would raise an immediate red flag as it is a clear breach of the data minimisation principle. But if the documentation does recommend/require data minimisation then the discussion should at least move past those and onto the principles that use words like "adequate" and "appropriate", where there is a better chance of making a case that what we are doing is indeed sufficient.

RISKS

1. The Federation is not assuming the Home Organisation's risk; it is merely providing advice.

8. Sources of Information

1. The OECD privacy principles (from Part 2 of the Annex to the OECD Privacy Guidelines), which have been the basis for the EU data protection directive. The benefit is, that OECD is not limited just to the UK or Europe.
2. The EU Data Protection Directive 95/46/EC (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)
3. Additional material is provided by the Article 29 Data Protection Working Party
    a. Opinion on the Concept of Personal Data
    b. Opinion on the concepts of "controller" and "processor"
    c. Opinion on Consent
4. In addition, while the legal principles are buried in the Directive, the UK law provides a different presentation, which may be more readable
5. An ~~opinion from the European Court~~ that a member state cannot further limit the power to process data, by adding an additional qualification to their equivalent of Art 7f. There are comments that this is a reminder that the Directive is supposed to *promote* the flow of data at the same time as protecting the privacy of individuals.
    a. A related blog posting
6. A memo from DLA Piper to the eduGAIN project
7. The REFEDS paper on data protection in Federated Access Management
8. The eduGAIN Policy Framework Data Protection Good Practice Profile ver 1.0 ~~pdf~~