

1 **eduGAIN Policy Framework**
2 **Data Protection Good Practice**
3 **Profile**
4 **(OPTIONAL)**



5

Version	Version date	Editor	Change
1.0	29.4.2011	Mikael Linden	Approved by SA3 T3 task leader 28.4.2011

6

7 1. Introduction

8 When releasing Attributes from a Home Organisation to a Service Provider, the Data Protection Directive
9 [DPdirective] often needs to be taken into account. The directive imposes requirements, some of which are best
10 covered by Home Organisations' and Identity and Service Providers' coordinated functioning. An introduction to
11 relevant articles of the directive and their interpretation in the context of federated identity management is
12 provided in Appendix B.

13 In the eduGAIN Policy, it has been recognised as an important goal to introduce policies and practices that
14 adapt the data protection directive to the technical infrastructure. This optional Data protection good practice
15 profile of eduGAIN defines two categories for Service Providers with different positions with regards to the
16 directive. An Identity and Service Provider and their Home Federation use SAML 2.0 metadata tags defined in
17 this document to indicate their support for this profile.

18 As the controller of its end user's personal data, the ultimate responsibility for releasing personal data to a
19 Service Provider is in the Home Organisation, who makes its decision based on its local risk management
20 procedures. However, eduGAIN may have thousands of Service Providers, which has made it practical to seek
21 ways to ease the Home Organisations' burden. This profile may help the Home Organisations in their decisions
22 by mediating privacy-related information on the service from the Service Provider to the Home Organisations
23 using well-defined syntax and semantics.

24 2. Requirements and Categories for Service 25 Providers

26 Considering the data protection directive's implications, Service Providers are grouped into these two
27 categories:

- 28 • category PII: the Service Provider processes personal data
- 29 • category non-PII: the Service Provider processes no personal data

30 PII stands for 'Personally Identifiable Information'. The categories are explained further in this section and are
31 summarised as a table in Appendix A.

32 2.1. Registering to a Category

33 A Service Provider who has adopted this Data protection good practice profile registers to either of the two
34 categories. Registering to a category implies that the Service Provider is committed to the functionality which

35 this profile requires in that category. A Service Provider cannot manifest conformance to this profile without
36 registering to either of the two categories.

37 The Service Provider's Home Federation records and mediates the category to other Participant Federations
38 and their Identity Providers via the exposed eduGAIN SAML 2.0 metadata.

39 **2.2. Service Providers Manifesting No Category**

40 If a Service Provider does not manifest any category, it is assumed that the Home Organisations, Identity
41 Providers and Service Providers will fulfil the obligations set by the data protection directive using an out-of-
42 band mechanism.

43 **2.3. Category PII: SP Processes Personal Data**

44 In category PII, the Service Provider is processing personal data because it receives Attributes from the Identity
45 Provider which are considered personal data.

46 The Service Provider can be one of the following:

- 47 • A data processor, processing personal data on behalf of a Home Organisation, in which case the Home
48 Organisation and Service Provider should have a written agreement as the basis for processing
49 personal data. For example, the Service Provider provides software as a service (SaaS) or licensed
50 contents (such as. library content) to the Home Organisation, and a related contract is in place between
51 the Home Organisation and Service Provider.
- 52 • A data controller, processing personal data not on behalf of the Home Organisation. Instead, release of
53 personal data from the Home Organisation to the Service Provider initiates a new and separate
54 processing of personal data in the Service Provider.

55 Whether the Service Provider is a data processor or data controller may vary per the Home Organisation. With
56 some Home Organisations in eduGAIN, the Service Provider may have a data processing agreement and acts
57 as a data processor. For the other Home Organisations, the Service Provider may be a data controller.

58 **2.3.1. Purpose of Processing**

59 In eduGAIN service, personal data is processed to support the goal of eduGAIN as defined in the eduGAIN
60 constitution.

61 A bilateral data processing agreement signed by a data controller and a data processor is likely to be more
62 specific on the purpose of processing.

63 **2.3.2. Relevance of Personal Data Processed**

64 See section 2.5. Relevance of Attributes.

65 **2.3.3. Informing the Data Subject**

66 The Service Provider must make the service's Privacy Policy publicly available. The Service Provider's Home
67 Federation must register a URL to a place where the privacy policy can be found and expose this URL to the
68 eduGAIN metadata. The privacy policy must be available at least in English and address the issues presented
69 in Article 11 of the data protection directive:

- 70 • Identity of the controller and of his representative, if any
- 71 • Purposes of the processing
- 72 • Any further information such as;
 - 73 ○ Categories of data concerned
 - 74 ○ Recipients or categories of recipients
 - 75 ○ Existence of the right of access to and the right to rectify the data concerning him/her

76 Before releasing the end user's Attributes to the Service Provider:

- 77 • For the first time
- 78 • For the first time after an extension in the Attribute set for this Service Provider

79

80 the Home Organisation must provide the Service Provider's privacy policy URL to the end user. As an example,
81 this can be done when an end user consents, if necessary, to Attribute release (see section 2.3.4).

82 The data controller is responsible for informing the end user on processing his personal data. If the Service
83 Provider is a data processor, the Service Provider may refer to the Home Organisation in its privacy policy web
84 page.

85 **2.3.4. Criteria for Making Data Processing Legitimate**

86 Releasing personal data from a Home Organisation to a Service Provider may be based on necessity or end
87 user's consent.

88 In Category PII, the Service Provider, being an expert of the service and its use scenarios, makes a proposal
89 on the legal grounds for processing. The Service Provider's Home Federation registers the proposal to the
90 Service Provider's metadata and exposes it to eduGAIN. Based on the proposal, the Service Provider's privacy
91 policy and other information available on the Service Provider, the Home Organisation decides if Attribute
92 release is based on consent or necessity.

93 To assist Providers in decision-making, guidelines and good practice are:

- 94
- A service that is related to an employee doing his work is usually based on necessity.
- 95
- A service that is related to a student taking his courses and otherwise being educated is usually based
- 96
- on necessity.

97 The process for informing the end user (see section 2.3.3) and asking for his consent for attribute release may

98 vary. If the end user is a child, granting the consent may also involve his parents.

99 When an end user logs in to a Service Provider for the first time:

- 100
- If Attribute release is based on consent, the Home Organisation provides the end user the following or
- 101
- equivalent text "I am informed on release of my personal data to the service and consent to it <OK>
- 102
- <Cancel>"
- 103
- If Attribute release is based on necessity, the Home Organisation provides the end user the following or
- 104
- equivalent text "I am informed on release of my personal data to the service <OK>"

105 In both cases, the Home Organisation must provide the end user with a clickable link to the Service Provider's

106

107

107 privacy policy (see section 2.3.3). Section 4.5 describes how to integrate this into the login sequence in an Identity Provider.

108 If an end user wants to withdraw his consent later, he can use the contact information in the privacy policy to

109

109 submit a request to the Service Provider to remove his personal data.

110 **2.3.5. Ensuring Adequate Level of Protection in 3rd Countries**

111 The Service Provider takes the responsibility of ensuring that the Service Provider resides in an EU/EEA

112

113

114

114 country or a country which ensures adequate levels of data protection or that the Service Provider is otherwise committed to an adequate level of protection (for example, the Service Provider is committed to the US Safe Harbour privacy principles).

115 **2.4. Category non-PII: No Personal Data Processed**

116 In Category non-PII, the Service Provider does not process personal data and the directive is not applied to the

117

117 Attribute release and the Service Provider

118 **2.4.1. Ensuring the Service Provider receives no Personal Data**

119 If a Service Provider is registered to the category non-PII, the Service Provider takes the responsibility of

120

121

121 ensuring that the Attribute Requirements registered for it do not contain any personal data in the Service Provider's jurisdiction.

122 Depending on the jurisdiction, some attributes either do or do not count as personal data or, due to lack of court

123

124

124 decisions, the status is unknown. For this Data protection good practice profile, it is advised to assume that SAML 2.0 Persistent NameID (known as eduPersonTargetedID) is personal data.

125 In some jurisdictions, IP addresses are considered personal data. IP addresses are not released via eduGAIN,
126 but are collected directly from the end user. Service Providers who reside in jurisdictions where IP addresses
127 are personal data should treat them as such and have adequate legal grounds (such as consent or necessity)
128 from end users before collecting them. This also applies to other data that, with other added information such
129 as an identifier, can become personal data.

130 **2.5. Relevance of Attributes**

131 Irrespective of which category PII or non-PII the Service Provider belongs to, the Home Federation must
132 register the Attribute Requirements of a Service Provider. The Home Federation publishes the Attribute
133 Requirements in the Service Provider's SAML 2.0 metadata entry exposed to eduGAIN.

134 It is assumed that the Service Provider, which is the expert of the service, carefully balances its Attribute
135 Requirements with the data protection directive and its national implementation before registering it to the
136 Home Federation. The Home Federation and eduGAIN service takes no legal responsibility on the Attribute
137 Requirements a Service Provider has registered.

138 Additionally, the Service Provider may register one or several statements made by one or several trusted third
139 parties (TTP) on Attributes the TTP deems relevant for the service. It is up to the Home Organisation to:

- 140 • Decide if it trusts the statement.
- 141 • Make an out-of-band agreement with the TTP on any legal responsibilities the TTP takes by the
142 statement.

143 Attributes revealing data that the data protection directive defines as sensitive personal data should not be
144 released in eduGAIN.

145 **3. Registering a Home Organisation's** 146 **Conformance**

147 The Home Federation registers a Home Organisation's manifest that is has adopted this Data protection good
148 practice profile. Registering implies that the Home Organisation is committed to the functionality that this profile
149 requires from a Home Organisation. A Home Organisation can manifest support to the category non-PII Service
150 Providers, category PII Service Providers or both.

151 The Home Federation records and mediates the Home Organisation's manifest of conformance to this profile to
152 other Participant Federations and their Service Providers using eduGAIN's SAML 2.0 metadata.

153 If a Home Organisation does not manifest conformance to this profile, it is assumed that the Home
154 Organisation and the Service Providers will fulfil the obligations set by the data protection directive using an

155 out-of-band mechanism. This is the default for Home Organisations and Identity and Service Providers who
 156 have not adopted this profile.

157 4. Technical Implementation

158 This section defines how the data protection mechanisms introduced in this document are technically
 159 expressed in the Identity and Service Providers' SAML 2.0 metadata entity elements. A new XML namespace
 160 mddp is introduced with one XML element, `DataProtectionProperties`, having three child elements:

- 161 • `Category` to indicate the category an SP belongs to and the categories an IdP supports.
- 162 • `LegalGrounds` to indicate the legal grounds for processing as suggested by the Service Provider.
- 163 • `saml:Assertion` to embed any signed Trusted Third Party statements to the metadata.

164 Additionally, SAML 2.0 metadata specification is used to indicate that the attributes the Service Provider
 165 requests, and Metadata Extensions for Login and Discovery User Interface [MetadataUI] to indicate the Service
 166 Provider's Privacy Policy's URL.

167 4.1. Provider's Category Indication

168 A Service Provider uses `Category` element to indicate the category in which the Service Provider belongs. An
 169 Identity Provider uses the same element to indicate which categories the Identity Provider supports.
 170

171 The element is placed to the Provider's metadata extensions element as a child element of the
 172 `DataProtectionProperties` element. The category is expressed using the values "non-PII" and "PII" and
 173 implementations should ignore the case.

174 Example (Service Provider):

```
175 <SPSSODescriptor>
176   <md:Extensions>
177     <mddp:DataProtectionProperties>
178       <mddp:Category>PII</mddp:Category>
179     </mddp:DataProtectionProperties>
180   </md:Extensions>
```

182 Example (Identity Provider):

```
183 <IDPSSODescriptor>
184   <md:Extensions>
185     <mddp:DataProtectionProperties>
186       <mddp:Category>PII</mddp:Category>
187       <mddp:Category>non-PII</mddp:Category>
```

```

188         </mddp:DataProtectionProperties>
189     </md:Extensions>
190 
```

191 4.2. Relevance of Personal Data

192 In its eduGAIN SAML 2.0 metadata element, the Service Provider uses the RequestedAttribute element defined
 193 by SAML 2.0 Metadata standard to indicate the Service Provider's Attribute Requirements. The isRequired
 194 XML attribute should be set to "true" if the service does not open to the user (not even using some lower level
 195 of functionality) without releasing the Attribute.

196 Example:

```

197 <SPSSODescriptor>
198     <AttributeConsumingService ...>
199         <RequestedAttribute
200             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
201             Name="urn:oid:2.5.4.4" isRequired="true"/>
202         <RequestedAttribute
203             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
204             Name="urn:oid:2.5.4.42" isRequired="false"/>
205     </AttributeConsumingService>
206 
```

207 Additionally, if the Service Provider wants to register a trusted third party's statement on necessary Attributes to
 208 its metadata entry, it can place a SAML attribute assertion in its EntityDescriptor. The contents and the
 209 semantics of the assertion are out of scope for this profile.

210 Example:

```

211 <SPSSODescriptor>
212     <md:Extensions>
213         <mddp:DataProtectionProperties>
214             <saml:Assertion>
215                 ... a TTP statement here...
216             </saml:Assertion>
217         </mddp:DataProtectionProperties>
218     </md:Extensions>

```

219 4.3. Informing the Data Subject

220 In its eduGAIN SAML 2.0 metadata element, the Service Provider uses the PrivacyStatementURL element
 221 defined in Metadata Extensions for Login and Discovery User Interface [MetadataUI] to indicate where the
 222 Service Provider's Privacy Policy can be found. The element must be in place for any category PII Service
 223 Provider.

224 Example:

```

225 <SPSSODescriptor>
226   <md:Extensions>
227     <mdui:UIInfo>
228       <mdui:PrivacyStatementURL xml:lang="en">
229         http://www.example.org/privacypolicy.html
230       </mdui:PrivacyStatementURL>
231     </mdui:UIInfo>
232   </md:Extensions>
233

```

234 4.4. Criteria for Making Data Processing Legitimate

235 In its eduGAIN SAML 2.0 metadata element, the Service Provider must use a LegalGrounds element to
 236 indicate what the Service Provider proposes as the legal grounds for processing personal data in the Service
 237 Provider (see section 2.3.4). The values should be in lowercase. The implementations must ignore the case.

238 **consent** The data subject gives unambiguously his consent (see article 11 a of the directive)

239 **necessity** Release of personal information is necessary (see article 11 b-f of the directive)

240 The Home Organisations may use this information to decide if Attribute release is based on necessity or
 241 consent. The element must be in place for any category PII Service Provider.

242 Example:

```

243 <SPSSODescriptor>
244   <md:Extensions>
245     <mddp:DataProtectionProperties>
246       <mddp:LegalGrounds>consent</mddp:LegalGrounds>
247     </mddp:DataProtectionProperties>
248   </md:Extensions>
249   ...
250

```

251 4.5. Identity Provider Behaviour

252 An Identity Provider relying on the data protection mechanisms provided in this profile must, before releasing
 253 any Attributes, ensure that:

- 254 • The Service Provider manifests conformance to category PII or non-PII.
- 255 • Only Attributes a category non-PII Service Provider requests are released to it.
- 256 • Only necessary Attributes are released to a category PII or non-PII Service Provider. The Identity
 257 Provider may use the RequestedAttribute information, privacy policy URL and trusted third party
 258 statements available in the Service Provider's metadata entry to construct its Attribute Release Policy.

259 Sections 2.3.3. and 2.3.4 introduced two requirements for Home Organisations:

- 260 • Inform the end user by providing him/her with a clickable link to the Service Provider's privacy policy.
- 261 • Ask him/her to consent, if necessary, to the Attribute release.

262 The Home Organisations may use any processes, such as printed and signed documents, to fulfil these
 263 requirements. However, in the front-channel binding of SAML 2.0 web single sign-on, a practical way could be
 264 that, after authenticating the end user but before releasing his attributes to the Service Provider, he is
 265 presented with a web dialogue which covers the two steps.

266 4.6. Service Provider Behaviour

267 Relays a Service Provider on the data protection mechanisms defined in this document and belongs to
 268 category PII, the Service Provider must ensure that the Identity Provider manifests conformance to category PII
 269 before the Service Provider accepts any attributes.

270 4.7. Multi-faced Service Providers

271 It is possible that an SP's category and other properties vary, depending on which Home Organisation the
 272 end user logs into. For instance, some library content may be licensed to some Home Organisations as an
 273 expensive site license and as a cheaper per-user license to another.

274 For such Service Providers, it is suggested that:

- 275 • The Service Provider registers multiple entries (with distinct entityIDs).
- 276 • The SP is not registered to eduGAIN at all.

277 It is assumed that few SPs have this issue.

278 APPENDIX A: Summary of Service Provider 279 Categories

	No category (default) Data protection covered out-of-band	Category PII: the SP processes personal data	Category non-PII: the SP processes no personal data
1. Description			
	eduGAIN is not involved in fulfilling	The SP processes personal data, which may be released to the SP	No personal data is passed

	No category (default) Data protection covered out-of-band	Category PII: the SP processes personal data	Category non-PII: the SP processes no personal data
	the obligations imposed by the data protection directive. The providers must use an out-of-band mechanism.	from an IdP. For a Home Organisation, the SP may be: <ul style="list-style-type: none"> • A data processor, processing personal data on behalf of the Home Organisation, • A data controller, not processing personal data on behalf of the Home Organisation. 	to the SP from the IdP.
2. The directive and how the category covers it			
2.1.Purpose of processing (Directive's article 6.1(b))	N/A	"To support the goal of eduGAIN." If the Service Provider is a data processor, the data processing agreement may define a more specific purpose.	N/A. Personal data is not processed
2.2.Relevance of personal data processed (Article 6.1 c)	N/A	The SP's Home Federation registers the SP's Attribute Requirements and provides them as part of the SAML2 metadata. Additionally, the metadata may contain a trusted third party's statement on what Attributes it deems necessary for the service. Sensitive personal data should not be released.	The same as the column to the left The SP must ensure that the Attribute Requirements do not incorporate personal data.
2.3.Informing the data subject (Article 11)	N/A	The SP's Home Federation registers the SP's Privacy policy's location in the <PrivacyStatementURL> element in the SAML2 metadata. When the Attribute release from the	Not needed. Personal data is not processed

	No category (default) Data protection covered out-of-band	Category PII: the SP processes personal data	Category non-PII: the SP processes no personal data
		Home Organisation to the SP takes place for the first time, the IdP must provide this clickable link to the end user.	
2.4.Criteria for making data processing legitimate (Article 7)	N/A	The SP proposes the criteria for making data processing legitimate. Based on the proposal, the Home Organisation decides if Attributes are released based on consent or necessity. It is assumed that in most use scenarios in eduGAIN, Attribute release is based on necessity.	N/A. Personal data is not processed
2.5.Withdrawal of consent	N/A	If the Attribute release is based on consent, the end user can contact the data controller's representative, by mail for example. It is assumed that withdrawal of consent does not occur frequently.	N/A. Personal data is not processed.
2.6.Release of personal data to 3rd countries	N/A	Personal data can be released to countries with adequate level of data protection just as it is released to EU/EEA countries. The Service Provider ensures that it resides in EU/EEA or in a country with adequate level of protection.	N/A. Personal data is not processed. Attributes can be freely released to 3rd countries.
2.7. Receiving personal data from 3rd countries.	N/A	Personal data can be received from 3rd countries in a similar way they are received from Home Organisations in EU/EEA.	N/A. Personal data is not processed. Attributes can be freely received from 3rd countries.
3. Technical implementation			
3.1.How providers manifest	This is the default category which is implied if a provider	IdPs and SPs manifest their conformance to this category by	IdPs and SPs manifest their conformance to this category by adding a tag "non-PII" to

	No category (default) Data protection covered out-of-band	Category PII: the SP processes personal data	Category non-PII: the SP processes no personal data
conformance to this category	does not manifest any other categories.	adding a tag "PII" to its metadata.	its metadata.
3.2.IdP behavior during login	The IdP must use an out-of-band mechanism to ensure that the obligations imposed by the data protection directive are fulfilled.	Before releasing Attributes to a Category PII SP, the IdP must ensure that the SP manifests conformance to Category PII in the SAML2 metadata.	Before releasing Attributes to a Category non-PII SP, the IdP must ensure that the SP manifests conformance to Category non-PII in the SAML2 metadata.
3.3.SP behavior during login	The SP must use an out-of-band mechanism to ensure that the obligations imposed by the data protection directive are fulfilled.	Before accepting Attributes from a Category PII IdP, the SP must ensure that the IdP manifests its conformance to Category PII in the SAML2 metadata.	No requirements to the SP behaviour.
4. Examples			
		eduroam trouble ticketing system (TTS), eduroam wiki, CLARIN	Library contents

280 Table A.1: Service Provider Categories.

281 APPENDIX B: Selected Sections of the 282 Directive and a Federation

283 This appendix discusses the directive's articles which are particularly interesting for federated identity
284 management and the eduGAIN service. The other provisions of the directive and its implementations are

285 naturally binding as well, but the provisions presented here have been identified as those who need
286 coordinated functionality from the Home Organisations and Identity and Service Providers in eduGAIN.

287 **B.1. Objective of the Directive (Article 1)**

288 The objective of the directive is to protect a persons' fundamental rights while guaranteeing the free flow of
289 personal data between member states. Thus, the directive can be seen as an enabler, not as a disabler, of
290 eduGAIN, providing the Attribute release in eduGAIN is implemented in a way that follows the provisions of the
291 directive.

292 *1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms*
293 *of natural persons, and in particular their right to privacy with respect to the processing of personal data.*

294 *2. Member States shall neither restrict nor prohibit the free flow of personal data between Member*
295 *States for reasons connected with the protection afforded under paragraph 1.*

296 **B.2. Definition: Personal Data (Article 2a)**

297 *'Personal data' shall mean any information relating to an identified or identifiable natural person ('data*
298 *subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by*
299 *reference to an identification number or to one or more factors specific to his physical, physiological,*
300 *mental, economic, cultural or social identity;*

301 It is obvious that common Attributes such as end user's full name (cn), email address (mail) and unique
302 identifier (eduPersonPrincipalName) are personal data. However, it is questionable if Attributes such as
303 privacy-preserving bilateral identifiers (eduPersonTargetedID/SAML2 Persistent identifier) are personal data.
304 Following is a brief discussion of this question.

305 The only property the eduPersonTargetedID Attribute has is that it has the same value when the same end
306 user visits the same service again. The interpretation of the expression *relating to an identified or identifiable*
307 *natural person* seems to vary country by country. The directive seems to make no difference between
308 *identification* and *recognition*, the latter meaning that the service notices the end user is the same one who has
309 visited the service earlier, although it does not know who he is in real life.

310 This case is fundamentally similar to the use of an IP address; the end user is recognised by his IP address,
311 but an end user's identity cannot be deduced from it. Case law is available in the Member States. One German
312 court (Berlin Regional Court 23 S 3/07) decided that the IP address is personal data. Another German court
313 (Munich district court 133 C 5677/08) decided that it is not. It is obvious that it is hard to get a pan-European
314 interpretation if IP address or eduPersonTargetedID is personal data. In the eduGAIN service, it should be
315 assumed that eduPersonTargetedID is personal data.

316 It is also worth noticing that if several Attributes are coupled together (as they usually are) and one of them is
317 personal data, then all the Attributes are personal data. For instance, an end user's role (the

318 eduPersonAffiliation Attribute) in his Home Organisation is not personal data alone, but put together with his
319 unique identifier (eduPersonPrincipalName) it becomes personal data, too.

320 **B.3. Definition: Processing of Personal Data (Article 2b)**

321 *'Processing of personal data' ('processing') shall mean any operation or set of operations which is*
322 *performed upon personal data, whether or not by automatic means, such as collection, recording,*
323 *organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,*
324 *dissemination or otherwise making available, alignment or combination, blocking, erasure or*
325 *destruction;*

326 Based on the definition, it is obvious that a Home Organisation processes personal data and the directive is
327 applied to it. However, as Home Organisations in the eduGAIN service typically already maintain user accounts
328 for their end users, being a Home Organisation who has registered an Identity Provider to a federation does not
329 change their status there.

330 Service Providers are processing personal data if they collect any information (either Attributes from an Identity
331 Provider or directly from the end user him/herself) that is considered to be personal data.

332 A common interpretation of the directive is that when an Identity Provider passes Attributes carrying personal
333 data to the Service Provider, the Identity Provider disseminates an end user's personal data to the Service
334 Provider, even though technically in the front-channel binding of the SAML 2.0 authentication request protocol,
335 it is the end user who uses his web browser to carry the SAML assertion to the Service Provider. There is no
336 known case law where this assumption is verified. If an Identity Provider is not passing personal data to the
337 Service Provider, but it is the end user him/herself, then most requirements presented in this document
338 collapse. An end user can use his personal data as they want.

339 Some federations have a distributed architecture, each Home Organisation operating an Identity Provider of
340 their own. Typically, the role of the federation operator is to maintain a trusted list of all registered Identity and
341 Service Providers. In such a federation, the federation operator is not processing personal data (except
342 possibly a list of Identity and Service Provider administrators' and their contacts). On the other hand, if the
343 federation operator is also operating Identity Provider(s) on behalf of the Home Organisations, they are
344 processing personal data, Therefore, they probably have data processor status, which is discussed next..

345 The eduGAIN service operator does not process personal data (except possibly a list of participant federations'
346 administrators and their contacts).

347 **B.4. Definition: Data Controller and Processor (Article 2d,e)**

348 *'Controller' shall mean the natural or legal person, public authority, agency or any other body which*
349 *alone or jointly with others determines the purposes and means of the processing of personal data;*
350 *where the purposes and means of processing are determined by national or Community laws or*
351 *regulations, the controller or the specific criteria for his nomination may be designated by national or*
352 *Community law;*

353 *'Processor' shall mean a natural or legal person, public authority, agency or any other body which*
354 *processes personal data on behalf of the controller;*

355 A research and higher education institution, which has registered an Identity Provider to eduGAIN, is typically
356 processing affiliated end users' personal data in order to support research and education in the institution. In
357 other words, the Home Organisation is a data controller and has determined that the purpose of processing is
358 to support institutions primary functions which are, in general, research and education.

359 The Service Provider's position as a data controller or processor depends on the service. When the Service
360 Provider is a subcontractor of the Home Organisation, the Service Provider is a data processor processing
361 personal data on behalf of the Home Organisation. An example of this is if the Service Provider provides
362 licensed content, such as library content or Software as a Service (SaaS), to the Home Organisation. Article 17
363 of the directive makes it explicit that the data processor must have a written contract with the Identity Provider.

364 *3. The carrying out of processing by way of a processor must be governed by a contract or legal act*
365 *binding the processor to the controller...*

366 *4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection*
367 *and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in*
368 *another equivalent form.*

369 In a (con)federation, bilateral agreements between Home Organisations and Service Providers are not
370 expected, in general. The scalability benefits of a (con)federation are questionable, if the directive enforces
371 bilateral written agreements between each Home Organisation and Service Provider. Fortunately, the directive
372 leaves the door open for Service Providers who are not data processors, but are data controllers. In this case,
373 release of personal data from a Home Organisation starts a new and separate processing of personal data in
374 the Service Provider.

375 In a (con)federation, it is also possible that a Service Provider is processing personal data on behalf of some
376 Home Organisation(s) with whom it has a data processing contract, but is also willing to grant access to end
377 users from other Home Organisations. In this case, the Service Provider is a data processor for some Home
378 Organisations and an independent data controller with regards to the other Home Organisations. The
379 (con)federation does not have built-in mechanisms to keep track of the bilateral agreements the Home
380 Organisations and Service Providers may have. Thus, it is safe to assume that each Service Provider is a data
381 processor for some Home Organisations and a data controller with regards to the other Home Organisations.

382
383 The data protection directive is applied both to data controllers and processors, but the obligations imposed
384 differ slightly. For example, it is the obligation of the data controller, not the data processor, to inform the end
385 user on processing his personal data. In an interfederation spanning multiple jurisdictions, it is also necessary
386 to note that the jurisdiction follows the data controller. More obligations are introduced in the next section.

387 **B.5. Security of Processing (Article 17)**

388 *1. Member States shall provide that the controller must implement appropriate technical and*
389 *organizational measures to protect personal data against accidental or unlawful destruction or*

390 *accidental loss, alteration, unauthorized disclosure or access, in particular where the processing*
391 *involves the transmission of data over a network, and against all other unlawful forms of processing.*

392 *Having regard to the state of the art and the cost of their implementation, such measures shall ensure a*
393 *level of security appropriate to the risks represented by the processing and the nature of the data to be*
394 *protected.*

395 This section makes it an obligation of a controller to make necessary measures to protect personal data, in
396 particular when it is transmitted over a network, which is the case in federated identity management. Having
397 this eduGAIN Data protection good practice profile and Service Providers manifesting conformance to it in
398 place is supposed to be part of the *appropriate technical and organisational measures* that Home Organisations
399 can rely on.

400 On the other hand, the article lets the controllers balance the obligation with the implementation costs, risks and
401 the nature of the data. It can be argued that personal data released via eduGAIN does not represent significant
402 risks. Especially, there seems to be no need to release Attributes which Article 8 defines as sensitive:

403 *Article 8*

404 *1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin,*
405 *political opinions, religious or philosophical beliefs, trade-union membership, and the processing of*
406 *data concerning health or sex life.*

407 ...

408 **B.6. Purpose of Processing (Article 6.1b)**

409 *Personal data must be collected for specified, explicit and legitimate purposes and not further*
410 *processed in a way incompatible with those purposes.*

411 As noted in section B.5, the institution as the controller of affiliated end user's data has defined the purpose of
412 processing personal data. In a research and education institution, the purpose typically follows from the
413 institution's charter and is, in general, to support research and education.

414 Following the directive, the institution must obey this purpose including when, acting as a Home Organisation, it
415 releases Attributes to a Service Provider. The purpose of processing personal data in the Service Provider may
416 not conflict with the purpose of processing in the Home Organisation. For example, a Home Organisation is not
417 conflicting with the directive when releasing student's data to a Learning Management System in another
418 university, but releasing students' personal data to a gambling service is hardly "supporting research and
419 education".

420 **B.7. Relevance of the Personal Data Processed (Article 6.1 c)**

421 *Personal data must be adequate, relevant and not excessive in relation to the purposes for which they*
422 *are collected and/or further processed.*

423 A Service Provider may process only those Attributes that are necessary for the service, whether gathered from
424 the end user him/herself, from a Home Organisation or from some other source. In federated identity
425 management, relevance of personal data translates to the principle of "minimal disclosure"; an Identity Provider
426 may release only relevant Attributes to a Service Provider.

427 In an identity federation, the concept of an Attribute Release Policy (ARP, having its origins in the Shibboleth
428 software) is commonly used for expressing which Attributes an Identity Provider releases to which Service
429 Providers. For scalability reasons, in a large (con)federation, some centralised mechanism to mediate Service
430 Providers' Attribute Requirements to all Home Organisations and their Identity Providers is desirable. It can be
431 assumed that the Service Provider is in a key role here; the Service Provider is the expert of the service.

432 **B.8. Informing the Data Subject (Article 11)**

433 *Information where the data have not been obtained from the data subject*

434 *1. Where the data have not been obtained from the data subject, Member States shall provide that the*
435 *controller or his representative must at the time of undertaking the recording of personal data or if a*
436 *disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide*
437 *the data subject with at least the following information, except where he already has it:*

438 *a) the identity of the controller and of his representative, if any;*

439 *b) the purposes of the processing;*

440 *c) any further information such as*

441 *o the categories of data concerned*

442 *o the recipients or categories of recipients*

443 *o the existence of the right of access to and the right to rectify the data concerning him/her*

444 *in so far as such further information is necessary, having regard to the specific circumstances in which*
445 *the data are processed, to guarantee fair processing in respect of the data subject.*

446 The data controller needs to inform the end user on processing his personal data. For a Home Organisation,
447 informing the end user is obvious and can be done when a new end user gets his account at the institution. The
448 Service Provider's obligation depends on if it is a data processor or a controller. As a data controller, a Service
449 Provider is responsible for providing this information to the end user. As a data processor a Service Provider
450 can refer to the Home Organisation.

451 In the Internet, a standard practice to inform the end user on processing his personal data in services is to
452 provide him/her a Privacy Policy web page in the service.

453 A convenient place to inform the end user is when the Attribute release takes place for the first time, and
 454 several federations in European higher education and research have already developed tools for that (e.g. the
 455 uApprove module implemented for Shibboleth, the consent module implemented for SimpleSAMLphp).
 456 Informing the end user can be conveniently bundled to the step where the end user, if necessary, consents to
 457 Attribute release, which is going to be discussed next.

458 **B.9. Criteria for Making Data Processing Legitimate (Article 7).**

459 **Withdrawal of Consent**

460 *Personal data may be processed only if:*

- 461 *(a) the data subject has unambiguously given his consent; or*
 462 *(b) processing is necessary for the performance of a contract to which the data subject is party or in*
 463 *order to take steps at the request of the data subject prior to entering into a contract; or*
 464 *(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or*
 465 *(d) processing is necessary in order to protect the vital interests of the data subject; or*
 466 *(e) processing is necessary for the performance of a task carried out in the public interest or in the*
 467 *exercise of official authority vested in the controller or in a third party to whom the data are disclosed;*
 468 *or*
 469 *(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by*
 470 *the third party or parties to whom the data are disclosed, except where such interests are overridden by*
 471 *the interests for fundamental rights and freedoms of the data subject which require protection under*
 472 *Article 1 (1).*

473 In summary this article concludes that data processing can be based either on consent or necessity. If based
 474 on consent, it must be freely given (an end user must have an option to say no) and informed (an end user
 475 must understand to what he consents. See the previous section.). Consent can be withdrawn any time:

476 *(Article 2 h) 'The data subject's consent' shall mean any freely given specific and informed indication of*
 477 *his wishes by which the data subject signifies his agreement to personal data relating to him/her being*
 478 *processed.*

479 Alternatively, data processing may be based on necessity, for example:

- 480 • Providing education to a student (c, e)
 481 • A teacher, researcher or other employee to do the jobs his employer has assigned to him/her (b)

482 However, deciding if a service is necessary or not is cumbersome. If a student is taking a course which is
 483 mandatory in his curriculum, release of personal data to the course's learning management system is probably
 484 necessary. But what if the course is optional? If a researcher is using licensed contents related to his subject of
 485 research, release of personal data is probably necessary, but what if the researcher is browsing contents
 486 outside his subject of research? As a result, the decision of whether Attribute release is based on consent or
 487 necessity becomes a complex function of (Service Provider, end user, time).

488 There seem to be two interpretations of this article. In some countries, consent is the primary way of making
489 data processing legitimate. In other countries, consent should be used only as a last resort, and the desirable
490 way is to base processing of personal data on necessity whenever possible.

491 It is worth noting that consent does not override the other obligations imposed by the directive, including the
492 purpose of processing, relevance of personal data processed and informing the data subject. It is wrong to
493 assume that anything can be done with an end user's personal data if he consents to it.

494 **B.10. Release of Personal Data to 3rd Countries**

495 Personal data may be released to other EU and EEA (Norway, Iceland, Lichenstein) countries as it is released
496 within an EU/EEA country. The directive recognises that also some non-EU/EEA countries (dubbed as 3rd
497 countries in the directive) may have adequate level of data protection. Personal data can be released to those
498 countries just as it is released to any EU/EEA country. In federated identity management, this principle is
499 applied to non-EU/EEA Service Providers.

500 The European Commission publishes a list of countries with adequate level of protection. For instance, in
501 Switzerland and Argentina, data protection laws ensure adequate level of protection. Canada has sector-
502 specific data protection legislation, and the protection is adequate if the Canadian data controller is subject to
503 the Personal Information Protection and Electronic Documents Act. In the United States, the level of data
504 protection is adequate if the data controller is committed to the "Safe Harbor privacy principles" that the US
505 Department of Commerce and the Commission have agreed on.

506 The Service Provider's jurisdiction follows the data controller. If the Service Provider is a data controller, the
507 Service Provider's local laws on data protection are applied to the Service Provider. If the Service Provider is a
508 data processor (i.e. processes personal data on behalf of the Home Organisation), the Home Organisation's
509 laws are applied.

510 To release personal data to countries that do not guarantee adequate data protection, the level of protection
511 must be ensured in an agreement with the data recipient. In federated identity management, the attribute
512 release takes place between the Home Organisation and the Service Provider, who should sign a bilateral
513 agreement which commits the Service Provider to an adequate level of protection. In a (con)federation, bilateral
514 contracts are not expected in general, which suggests that this Data protection good practice profile cannot be
515 used by Service Providers who are not bound to an adequate level of protection by the local law or the US Safe
516 Harbour privacy principles. This does not exclude US Service Providers or even federations from eduGAIN, but
517 their data protection issues must be solved using some other mechanism.

518 **B.11. Receiving Personal Data from 3rd Countries**

519 The directive is applied to processing personal data in EU/EEA, regardless of the Service Provider processing
520 personal data on behalf of a data controller in a 3rd country or not. However, if the Service Provider is a data
521 processor and the data controller is in a 3rd country, the directive expects the data processor to have a
522 representative in EU/EEA to ensure the directive can be enforced:

523 (Article 4) 1. Each Member State shall apply the national provisions it adopts pursuant to this Directive
 524 to the processing of personal data where:

525 ...
 526 (c) the controller is not established on Community territory and, for purposes of processing personal
 527 data makes use of equipment, automated or otherwise, situated on the territory of the said Member
 528 State, unless such equipment is used only for purposes of transit through the territory of the
 529 Community.

530 2. In the circumstances referred to in paragraph 1(c), the controller must designate a representative
 531 established in the territory of that Member State, without prejudice to legal actions which could be
 532 initiated against the controller him/herself.

533 If the Home Organisation outside EU/EEA has a data controller/processor relationship with any of the Service
 534 Providers in EU/EEA, it needs a representative in EU/EEA. On the other hand, if the Service Provider in
 535 EU/EEA is a data processor for a non-EU Home Organisation, it needs to have a written agreement with the
 536 non-EU Home Organisation anyway (see section B.4.), and the EU/EEA representative is covered there. In the
 537 (inter)federation agreement, the requirement for a non-EU/EEA Home Organisation having a representative in
 538 EU/EEA can be omitted. The Home Organisation does not need to reside in a country which guarantees
 539 adequate level of data protection.

540 Appendix C

541 C.1. Open Issues

- 542 • Currently, Data protection good practice profile covers only Identity and Service Providers, but the
 543 eduGAIN Policy Framework also recognises other Entities such as Attribute Providers. In principle, from
 544 a Data Protection perspective, Attribute Providers are like Identity Providers, but there may be no front-
 545 channel binding for Attribute Requests, which makes the implementation of this Profile more difficult for
 546 them.

547 Glossary

548 General terms:

549 AAI Authentication and authorisation infrastructure.

Attribute Provider An organisation which is responsible for managing additional identity data (attributes) for end users authenticated by a Home Organisation. Also a server that is acting in an Attribute Provider

role as defined in SAML 2.0. In this document, an Attribute Provider refers to an attribute provider who is a Member of a Participant Federation and whom the Participant Federation has exposed to eduGAIN.

DANTE	Delivery of Advanced Network Technology to Europe. The GÉANT network is managed by DANTE.
Entity	Entity means an AAI endpoint described with a SAML 2 EntityDescription. An Entity can be, for instance, an Identity Provider, a Service Provider or an Attribute Provider. In this document, an Entity refers to an entity that a Participant Federation has exposed to eduGAIN.
Federation	(identity federation) An association of organisations that come together to exchange information as appropriate about their users and resources in order to enable collaborations and transactions.
GÉANT	Gigabit European Academic Network project, the pan-European data network dedicated to the research and education community. The GÉANT network is managed by DANTE.
Home Organisation	The organisation which the end users are affiliated to and which is responsible for managing end users' identity data (attributes) and authenticating them. Home Organisation is responsible for setting up and operating either one or more Identity Providers, either by itself or via an outsourced service. In this document, a Home Organisation refers to a home organisation who is a Member of a Participant Federation and whose Identity Provider the Participant Federation has exposed to eduGAIN.
Identity Provider	A server acting in an Identity Provider role as defined in SAML 2.0 specifications. In this document, an Identity Provider refers to the Identity Provider that a Participant Federation has exposed to eduGAIN.
Member	Any organisation that has signed an agreement with a federation operator to cover the verification and publication of metadata. In this document, Member refers to a member whose Entity is exposed to eduGAIN.
NREN PC	The Policy Committee of the GÉANT network and project, which consists of appointed representatives from each partner in the project. It is responsible for setting and overseeing overall policy of the GÉANT network and project.
OT	eduGAIN Operational Team, as defined in section 2.4 of the eduGAIN Constitution.
Participant Federation	A Federation which has passed the joining process defined in section 3.2 of the eduGAIN constitution.
Policy Framework	(eduGAIN Policy Framework) This document, the profiles supplementing it and the eduGAIN Policy Declarations signed by Participant Federations.
Service Provider	An organisation that is responsible for offering the end user the service he is going to log in to. Also a server that is acting in a Service Provider role as defined in SAML 2.0. In this document, a Service Provider refers to a service provider who is a Member of a Participant Federation and whom the Participant Federation has exposed to eduGAIN.
TSG	eduGAIN Technical Steering Group, as defined in section 2.3 of the eduGAIN constitution.

550
551
552

Additional terms introduced in this Profile

Attribute	An end user's identifier (e.g. name, mail address, eduPersonPrincipalName or persistent NameID), role or other property that an Identity Provider releases or may release to a Service Provider.
-----------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Attribute Release Policy An Identity Provider's decision and related configuration regarding which Attributes will be released to a given Service Provider.

Attribute Requirements A list of Attributes a Service Provider requests from an Identity Provider

Home Federation The eduGAIN Participant Federation to which an Identity or Service Provider has been registered and which exposes the Provider to the eduGAIN service

553

554

References

555 [DPdirective] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the
556 protection of individuals with regard to the processing of personal data and on the free movement of such data

557 [MetadataUI] SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0.
558 Committee Specification Draft 01, 14 December 2011. <http://wiki.oasis-open.org/security/SAML2MetadataUI>