

GÉANT Data Protection Code of Conduct

(GDPR Version)

Draft of version 11.0 (25 November 2019)

The work leading to this Code of Conduct has received funding from the European Union's Horizon2020 programme under Grant Agreement No. 731122 (GN4-2). This work is © 2012-2018 GÉANT Association, used under a Creative Commons Attribution ShareAlike license (CC BY-SA 3.0)

TABLE OF CONTENTS

Table of contents	2
Purpose of this Code of Conduct	5
Who can adhere this Code of Conduct?	5
Territorial scope	5
Functional Scope	6
Roles of the parties involved	6
Principles of the Processing of Attributes	7
a. Legal compliance	7
b. Purpose limitation	8
c. Deviating purposes	10
d. Data minimisation	10
e. Information duty towards End User	11
f. Information duty towards Home Organisation	12
g. Data retention	13
h. Security measures	14
i. Security breaches	14
j. Transfer of personal data to third parties	15
k. Transfer of personal data to third countries	16
l. End User’s consent	17
m. Liability	17
n. Governing law and jurisdiction	18
o. Eligibility	19
p. Termination of the Code of Conduct	19
q. Survival of the code of conduct	19
r. Precedence	19
Attribute Providers	20
Appendix 1: Information duty towards End Users	22
I. How a Service Provider Organisation can develop a Privacy Notice	22

Privacy Notice Template	22
Appendix 2: Information Security, technical and organisational guidelines for Service Provider Organisations	26
Normative Assertions	26
1 Operational Security [OS]	26
2 Incident Response [IR]	27
3 Traceability [TR]	27
4 Participant Responsibilities [PR]	27
References	27
Appendix 3: Handling non-compliance of Service Provider Organisations	29
Introduction	29
Examples of SP non-compliance	29
monitoring body of the code of conduct	30
Appendix 4: Glossary of Terms	32

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19

DISCLAIMER

The principles laid down in this Code of conduct shall be considered as legally binding provided that this Code of Conduct is approved by the competent supervisory authority in accordance with the procedure described in Article 40 of General Data Protection Regulation.

Before being approved, this Code of Conduct shall be interpreted as non-legally binding guidance and shall not be considered as providing appropriate safeguards within the meaning of the General Data Protection Regulation.

20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66

PURPOSE OF THIS CODE OF CONDUCT

This Code of Conduct relates to the processing of personal data for online access management purposes in the research and education sector and is ruled by the General Data Protection Regulation^{1, 2}.

This Code takes into account the specific characteristics of the processing carried out in the research and education sector and describes the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons. When drafting the Code, relevant stakeholders, including data subjects, were consulted. The text of the Code takes into account the valuable submissions received and views expressed in response to the consultations.

Notwithstanding the provisions as set forth in an agreement between the **Home Organisation** and the **Service Provider Organisation**, which in all cases takes precedence, this Code of Conduct sets the rules that Service Provider Organisations can commit to when they want to receive End Users' Attributes from **Home Organisations** or their Agent for enabling the End Users to access their Services. Home Organisations will feel more comfortable to release affiliated End Users' Attributes to the Service Provider Organisation if they can see that the Service Provider Organisation has taken measures to properly protect the Attributes.

This Code of Conduct observes the data protection principles stemming from the General Data Protection Regulation (GDPR), and respects the national provisions adopted by Member States, or rules, regulations and policies adopted by International Organisations.

This Code of Conduct constitutes a binding community code for the Service Provider Organisations that have committed to it.

This Code includes three appendices, detailing best practices on how to adhere to the rules of the Code.

These appendices relate to:

- (1) information duties towards **End Users**,
- (2) information security guidelines for **Service Provider Organisations** and,
- (3) enforcement procedures for **non-compliance** with the Code of Conduct.

WHO CAN ADHERE THIS CODE OF CONDUCT?

TERRITORIAL SCOPE

This Code of Conduct is addressed to any **Service Provider Organisation** established in any of the

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

² For further information regarding the purposes of this Code of Conduct, see the Explanatory Memorandum GEANT Code of Conduct.

67 Member States of the European Union and in any other countries belonging to the European Economic
68 Area (Iceland, Liechtenstein and Norway).

69
70 Furthermore, **Service Provider Organisations** established in any third country offering an adequate level
71 of data protection in the terms of Article 45 of the GDPR and International Organisations can also
72 subscribe to this Code of Conduct.

73
74 In addition to this, Article 40.3 of the GDPR gives the opportunity to **Service Provider Organisations**
75 that do not fall under the territorial scope of the Regulation (Article 3, territorial scope) and that are
76 established outside of the EEA to join this Code of Conduct in order to provide appropriate safeguards
77 within the framework of transfers of personal data to third countries or International Organisations under
78 the terms referred to in point (e) of Article 46(2).

80 FUNCTIONAL 81 SCOPE

82
83
84 This Code of Conduct is limited to the processing of **Attributes which are released for enabling the**
85 **End User to access the Service** as described in clause b. Purpose limitation.

86
87 In case the Service Provider Organisation uses the Attributes for purposes other than enabling the End
88 User to access the Service, these activities fall out of the scope of this Code of Conduct.

89
90 The Service Provider Organisations and the communities representing the Service Provider Organisations
91 can agree to apply the Code of Conduct also to other Attributes, such as those the Service Provider
92 Organisations manage and share themselves, as further described in the Attribute Providers section.

94 ROLES OF THE PARTIES 95 INVOLVED

96
97
98 This Code of Conduct is addressed to Service Provider Organisations acting as data controllers
99 notwithstanding potential processing agreement between the Service Provider Organisation and the Home
100 Organisation as described in clause r. Precedence.

101
102 In the context of this Code of Conduct:

103
104 1. A **Home Organisation** acts as a data controller as to the wider relationship with the **End User**,
105 for example operating the Identity Provider (IdP) server in respect of the Attributes. An Agent
106 who operates the IdP server on behalf of the **Home Organisation** acts as a data processor. This
107 includes also the Federation Operators who operate a (potentially centralised) IdP server on behalf
108 of the **Home Organisation**.

109
110 2. A **Service Provider Organisation** acts as a data controller in respect of the **Attributes**,
111 processing them for the purposes as described in the clause b. Purpose limitation. In certain
112 circumstances a **Service Provider Organisation** may be acting as a data processor, acting on
113 behalf and as instructed by the **Home Organisation**. A **Service Provider Organisation** can also
114 manage (and be a Data Controller for) extra attributes of an End User and further become an
115 Attribute Provider, as described in the Attribute Providers section. A **Service Provider**
116 **Organisation** may manage several independent Services and commits to the Code of Conduct for
117 each of them separately.

118

119 3. An **End User** acts as a data subject whose personal data are being processed for the purposes as
120 described in clause b. Purpose limitation.
121

122 The processing of the **Attributes** by the **Service Provider Organisation** for enabling the End User to
123 access the Service is further explained in the Service-related Privacy Notice. As explained in Appendix
124 1, the Service-related Privacy Notice describes the reason for the processing, the way the data is collected,
125 handled and the protection provided. It further explains how the data is used and the rights of the End
126 User in relation to his personal data.
127

128 In the case that a Federation and a Federation Operator do not process the **Attributes** of the **End User**,
129 no specific privacy notice needs to be put in place between the End User and the Federation Operator.
130

131 PRINCIPLES OF THE PROCESSING OF 132 ATTRIBUTES

133
134
135 To the extent the **Service Provider Organisation** acts as a data controller, it agrees and warrants:
136

137 A. LEGAL 138 COMPLIANCE

The Service Provider Organisation warrants to only process the Attributes in accordance with: the contractual arrangements with the Home Organisation, this Code of Conduct, or the relevant provisions of the GDPR.

143
144 Where the Service Provider Organisation processes the Attributes, the Service Provider Organisation shall
145 comply with:
146

- 147 1. the agreement between the Home Organisation and the Service Provider Organisation;
 - 148 2. if not applicable, the provisions of this Code of Conduct;
 - 149 3. if not applicable, the relevant provisions of the GDPR.
- 150
151
152

153 In particular, the Service Provider Organisation shall ensure that all personal data processing activities
154 carried out in this context comply with the GDPR.
155

156 The **Service Provider Organisation** based in the EEA territory commits to process the End User's
157 **Attributes** in accordance with the applicable European data protection legislation. In principle, a Service
158 Provider Organisation established in the EEA territory, subject to the European Data Protection
159 legislation, shall not find itself in a situation where their national data protection laws would contradict
160 this Code of Conduct.
161

162 **Service Provider Organisations** established outside the EEA territory but in a country offering an
163 adequate data protection pursuant to Article 45 of the GDPR, should assess the compliance of this Code
164 of Conduct with the laws of its jurisdiction. If observance of any provision of the Code of Conduct would
165 place the Service Provider Organisation in breach of such laws, the national law of its jurisdiction shall
166 prevail over such provision of the Code of Conduct, and compliance with national law to this extent will

167 not be deemed to create any non-compliance by the Service Provider Organisation with this Code of
168 Conduct.
169

170 The **Service Provider Organisation** based outside the EEA and countries offering adequate data
171 protection commits to process the End User's Attributes in accordance with the GDPR, this Code of
172 Conduct and any other contractual or other arrangements, such as the use of EU model clauses. Such
173 Service Provider Organisations shall make binding and enforceable commitments to apply the appropriate
174 safeguards, including as regards data subjects' rights³, in addition to committing to abide by this Code of
175 Conduct.

176
177 **Service Provider Organisations** that are International Organisations may be subject to their own internal
178 rules, regulations and policies. Such International Organisations, which may not be subject to GDPR, shall
179 make binding and enforceable commitments to apply the appropriate safeguards provided by this Code of
180 Conduct, including with regard to the rights of data subjects, in accordance with Article 40 (3) of the
181 GDPR

182
183 Regarding the applicable law, see clause n. Governing law and jurisdiction.

184
185 In the event of conflict between the provisions of this Code of Conduct and the provisions of a contractual
186 arrangement with the Home Organisation, see clause r. Precedence.
187

188 B. PURPOSE 189 LIMITATION

190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212

The **Service Provider Organisation** warrants that it will process Attributes of the **End User** only for the purposes of enabling access to the Service.

The Attributes shall not be further processed in a manner which is not compatible with the initial purposes (Article 5.b of the GDPR).

The Service Provider Organisation must ensure that Attributes are used only for enabling the End User to access the Service. As far as the use of Attributes for deviating purposes is concerned, see clause c. Deviating purposes.

In practice, enabling access to the Service covers:

- **Authorisation:** managing **End User's** access rights to Services provided by the **Service Provider Organisation** based on the **Attributes**. Examples of such **Attributes** are those describing the End User's **Home Organisation** and organisation unit, their role and position in the **Home Organisation** (whether they are university members, students, administrative staff, etc.) and, for instance, the courses they are taking or teaching. The provenance of those **Attributes** is important for information security purposes; therefore, authorisation cannot be based on an Attribute that an End User has self-asserted.

³ In the event where a EU End User would lodge a complaint against a Service Provider Organisation based outside the EU (i.e. in the US), the competent European Data Protection Authority would be able to investigate on the alleged violation of data protection.

- 213 ● **Identification: End Users** need to have a personal identifier with the Service Provider
214 Organisation to be able to access their own files, datasets, pages, documents, postings, settings,
215 etc. The origin of an **Attribute** used for identification is important; to avoid an identity theft, an
216 End User cannot self-assert their own identifier. Instead, the Identity Provider authenticates
217 them and the Home Organisation (or Attribute Provider) provides the **Service Provider**
218 **Organisation** with an **Attribute** that contains their authenticated identifier.
219
- 220 ● **Transferring real-world trust** to the online world: if the **Service Provider Organisation** supports
221 a user community that exists also in the real world, **Attributes** can be used to transfer that
222 community to the online world. For instance, if the members of the user community know each
223 other by name in the real world, it is important that their names (or other identifiers) are displayed
224 also in any discussion or collaboration forum offered by the **Service Provider Organisation**. The
225 source of those **Attributes** is important; to avoid identity theft, the **Service Provider Organisation**
226 must retrieve users' names from trustworthy sources and not rely on self- assertions.
227
- 228 ● **Researcher unambiguity**: ensuring that a researcher's scientific contribution is associated
229 properly to them and not to a wrong person (with potentially the same name or initials). In the
230 research sector, publishing scientific results is part of researchers' academic career and the
231 researchers expect to receive the merit for their scientific contribution. There are global researcher
232 identification systems (such as ORCID and ISNI) which assign identifiers for researchers to help
233 scientific **Service Provider Organisations** to properly distinguish between researchers, even if
234 they change their names or organisation they are affiliated with.
235
- 236 ● **Accounting and billing**: personal data can be processed for accounting (for instance, that the
237 consumption of resources does not exceed the resource quota) and billing purposes. In the research
238 and education sector, the bill is not always paid by the End User but by their Home Organisation,
239 project, grant or funding agency.
240
- 241 ● **Information Security**: personal data can be processed to ensure the integrity, confidentiality and
242 availability of the Service (e.g.: incident forensic and response).
243
- 244 ● **Other functionalities** offered by the **Service Provider Organisation** for enabling the End User to
245 access the Service: using **Attributes** of End Users for the purposes of other functionalities offered
246 by the Service Provider Organisation. It is common that services on the Internet send e- mail or
247 other notifications to their users regarding their services. Examples of scenarios where processing
248 End User's email address or other contact detail falls within the scope of enabling access to the
249 Service include for instance:
250
 - 251 ▪ the End User's application to access the resources has been approved by
252 the resource owner;
 - 253
 - 254 ▪ the End User's permission to use a resource is expiring or they are
255 running out of the resource allocation quota;
 - 256
 - 257 ▪ someone has commented on the End User's blog posting or edited their
258 wiki page.
259

260 See also the next clause on deviating purposes.
261
262

263 C. DEVIATING 264 PURPOSES 265

266
267
268

The Service Provider Organisation commits not to process the Attributes for purposes other than enabling the End User to access the Service, unless the End User has given prior consent to the Service Provider Organisation.

269

If the Service Provider Organisation wants to use the Attributes for purposes other than “enabling the End User to access the Service” (see b. Purpose limitation), it can only do so if the End User gives their consent to the Service Provider Organisation. See also clause 1. End User's consent for the requirements on consent.

270
271
272
273
274

Examples of deviating purposes⁴ are: sending the End User commercial or unsolicited messages, including End User's e-mail address to a newsletter offering new services, selling the Attributes to third parties, transferring information to third parties such as the search history, profiling activities etc.

275
276
277
278

D. DATA MINIMISATION

279
280
281
282
283
284

The Service Provider Organisation commits to minimise the Attributes requested to those that are adequate, relevant and not excessive for enabling access to the Service and, where a number of Attributes could be used to provide access to the Service, to use the least intrusive Attributes possible.

285

The following list presents examples of Attributes that are **adequate, relevant** and **not excessive** for enabling the End User to access the Service. The Attribute names refer to the schema (e.g. eduPerson, Schac) and protocol (SAML2) definitions currently used widely in the GÉANT community:

286
287
288
289

- an Attribute (such as, eduPerson(Scoped)Affiliation, eduPersonEntitlement or schacHomeOrganisation) indicating that the End User is authorised to use the Service:

290
291
292
293
294
295

- a trusted value provided by the IdP is needed instead of a value self-asserted by the End User.

- an Attribute (such as, SAML2 PairwiseID or PersistentID) uniquely identifying the End User required, for instance, to store the End User's Service profile:

296
297
298
299
300
301

- a trusted value provided by the IdP is needed. To avoid an identity theft, an End User cannot self-assert their own identifier.

- if there are several alternative unique identifiers available for the Service, the least intrusive must be used:

302
303
304
305
306

- a pseudonymous bilateral identifier (such as, SAML2 PairwiseID or PersistentID) is preferred;

⁴ Consult the Article 29 Working Party's Opinion 03/2013 on purpose limitation. This document can guide the Service Provider to ascertain whether the purpose for the processing of the personal data is compatible or not.

- 307
- 308
- 309
- 310
- 311
- 312
- 313
- 314
- 315
- 316
- 317
- 318
- 319
- 320
- 321
- 322
- 323
- 324
- 325
- 326
- 327
- 328
- 329
- 330
- 331
- 332
- 333
- if enabling access to the Service requires matching the same End User's accounts between two Service Provider Organisations, a Service Provider Organisation can request a more intrusive identifier (such as SAML2 Subject ID, eduPersonPrincipalName or eduPersonUniqueID), whose value for a given user is shared by several Service Provider Organisations;
 - if there is a legitimate reason for an End User (such as a researcher) to keep their identity and profile in the Service Provider Organisation even when the organisation they are affiliated with changes, a permanent identifier (such as, ORCID identifier) can be used.
- a name Attribute (such as commonName or DisplayName Attribute) is necessary for a wiki or other collaboration platform, if the End Users know each other in real life and need to be able to transfer their existing real-world trust to an online environment.
 - if knowing the contributor's name is important for the collaboration, the name can be requested;
 - otherwise, the name cannot be requested. Instead, the Service may indicate the user as "unknown" or use a pseudonym the user has selected or the system has assigned to him/her.
 - e-mail address or other contact details, if it is necessary to contact the **End User** for the proper functioning of the Services offered by the **Service Provider Organisation**.

334 In the context of this Code of Conduct, under no circumstances is a **Service Provider Organisation** is
335 authorised to request End User's Attribute revealing racial or ethnic origin, political opinions, religious
336 or philosophical beliefs, trade-union membership, genetic data, biometric data for the purposes of
337 uniquely identifying a natural person or data concerning health or sex life or sexual orientation.
338

E. INFORMATION DUTY TOWARDS END USER

339
340

The **Service Provider Organisation** shall provide the **End User** with a Privacy Notice before they initiate the federated login for the first time.

This Privacy Notice must be concise, transparent, intelligible and provided in an easily accessible form.

The Privacy Notice shall contain at least the following information:

- the name, address and jurisdiction of the **Service Provider Organisation**; where applicable;
- the contact details of the data protection officer, where applicable;
- the purpose or purposes of the processing of the **Attributes**;
- a description of the **Attributes** being processed as well as the legal basis for the processing;
- the third party recipients or categories of third party recipient to whom the **Attributes** might be disclosed, and proposed transfers of **Attributes** to countries outside of the European Economic Area;
- the existence of the rights to access, rectify and delete the **Attributes** held about the **End User**;
- the retention period of the **Attributes**;
- a reference to this Code of Conduct;
- the right to lodge a complaint with a Supervisory Authority.

341

342 The Privacy Notice can be, for instance, linked to the front page of the Service. It is important that the
343 **End User** can review the policy before they log in for the first time. The Privacy Notice shall use clear
344 and plain language.

345

346 The Privacy Notice is Service specific and not the same for different Services of a Service Provider
347 Organisation.

348

349 The **Service Provider Organisation** needs to describe in its Privacy Notice how End Users can exercise
350 their right to access, request correction and request deletion of their personal data.

351

352 The **Service Provider Organisation** may include additional information, but must include as a minimum
353 the information described above. The additional information could for example refer to the additional data
354 processing activities of the **Service Provider Organisation**. Additional processing activities must
355 comply with the provisions of clause c. Deviating purposes and be included in the Privacy Notice.

356

357 The **Service Provider Organisations** are advised to make use of the Privacy Notice template that belongs
358 to the supporting material of the Code of Conduct in Appendix 1: Information duty towards End Users.

359

360 F. INFORMATION DUTY TOWARDS HOME
361 ORGANISATION

362

363

364

365

The **Service Provider Organisation** commits to provide to the **Home Organisation** or its Agent at least the following information:

- a) a machine-readable link to the Privacy Notice;
- b) indication of commitment to this Code of Conduct;
- c) any relevant updates or changes in the local data protection legislation or rules, regulations and policies adopted by International Organisations. that may affect this

366

367

Code of Conduct.

368

369

370

371

372

373

374

GÉANT has put in place a scalable technical solution allowing **Service Provider Organisations** to publicly announce their adherence to this Code of Conduct and to communicate its Service Privacy Notice's URL. When a Service Provider Organisation has several Service Privacy Notice, the URL of each Service Privacy Notice will be provided to the Home Organisation. This information is shared with the Home Organisation's Identity Provider before it releases the End User's Attributes to the **Service Provider Organisation**, enabling the Home Organisation to present it to the End User.

375

376

377

378

The current technical infrastructure is based on the standard SAML 2.0 metadata management and distribution system operated by Federation Operators. However this Code of Conduct will apply despite the future changes in the technical infrastructure.

379

G. DATA

380

RETENTION

381

382

383

384

The **Service Provider Organisation** shall delete or anonymize all **Attributes** without undue delay as soon as they are no longer necessary for the purposes of providing the Service.

385

386

387

388

Under the GDPR, anonymized data does not constitute personal data; therefore, anonymized data can be kept indefinitely.

389

390

391

392

The retention period of the **Attributes** depends on the particularities of the Service and it needs to be decided by the **Organisation**. However, a **Service Provider Organisation** shall not store the **Attributes** for an unlimited or indefinite period of time.

393

394

395

396

397

The **Service Provider Organisation** has to implement an adequate data retention policy compliant with the GDPR and other applicable data protection legislation. The existence of this policy must be communicated in the Service's Privacy Notice (see clause e. Information duty towards End User).

398

399

400

In principle the personal data must be deleted or anonymised if the **End User** (or their **Home Organisation**) no longer wishes to use the Service.

401

402

403

404

405

However, in many cases, the **End User** does not explicitly inform the **Service Provider Organisation** that they no longer wish to use the Service, they just do not log in to the Service anymore. In this case it is considered as a good practice to delete or anonymise the **End User's** personal data if they have not logged in for 18 months.

406 On the other hand, there are also circumstances where an **End User** not signing in does not necessarily
407 mean that they no longer wish to use the Service. The **Service Provider Organisation** shall implement
408 appropriate processes to manage this type of situation. For instance:

- 409
- 410 ● if the Service is an archive for scientific data, the researchers who deposit their datasets to the
411 archive may still remain the owners or custodians of the dataset although they do not log in for a
412 while;
- 413
- 414 ● if the Service is a source code control system (for example, git), an **End User** uses to publish
415 their computer program code, the **End User** may still want to be able to log in and maintain their
416 code, although they have not logged in for a while;
- 417
- 418 ● if the Service is a repository where researchers publish their scientific findings and contribution,
419 the researchers still want to have their name and other **Attributes** attached to the finding,
420 although they do not regularly log in;
- 421
- 422 ● if the Service is a collaborative application (such as, a wiki or a discussion board) where the **End**
423 **User** has their name or other **Attribute** attached to their contribution to let the other users learn
424 and assess the provenance of the contribution and Attribute it to a specific person.
- 425

426 The Personal Data, including log files, do not need to be removed or anonymised as long as they are
427 needed:

- 428
- 429 ● for archiving purposes in the public interest, scientific or historical research purposes or statistical
430 purposes;
- 431
- 432 ● for compliance with a legal obligation which requires processing by International, European or
433 Member State law to which the **Service Provider Organisation** is subject;
- 434
- 435 ● for the performance of a task carried out in the public interest;
- 436
- 437 ● for the establishment, exercise or defence of legal claims, such as resource allocation or invoices;
- 438
- 439 ● for exercising the right of freedom of expression and information.
- 440

441 H. SECURITY 442 MEASURES

443

444

445

446

The **Service Provider Organisation** warrants taking appropriate technical and organisational measures to safeguard Attributes against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access. These measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the state of the art and the cost of their implementation.

447

448 The **Service Provider Organisation** shall implement the security measures described in Appendix 2:
449 Information Security, technical and organisational guidelines for Service Provider Organisations.

451 I. SECURITY

452
453
454
455
456

BREACHES

The **Service Provider Organisation** commits to, without undue delay, report all suspected privacy or security breaches, meaning any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise

457
458

processed concerning the **Attributes** to the **Home Organisation** or its Agent and, where this is legally required, to the competent data protection authority and/or to the **End Users** whose data are concerned by the security or privacy breach.

459

Article 33 of the GDPR describes the conditions when a personal data breach must be notified to the supervisory authority. This clause imposes an obligation to notify also the Home Organisation, to allow them to take the necessary technical and organisational measures for mitigating any risk the **Home Organisation** may be exposed to.

460
461
462
463
464

For example, if the **Service Provider Organisation** suspects that one or more user accounts in the **Home Organisation** has been compromised, the **Service Provider Organisation** contacting the **Home Organisation** enables the **Home Organisation** to take measures to limit any further damage (such as, suspend the compromised accounts) and to start the necessary actions to recover from the breach, if any.

465
466
467
468
469

The **Service Provider Organisation** shall use the security contact point of the Home Organisation or its Agent as provided in the technical infrastructure (currently, SAML 2.0 metadata), or an appropriate alternative, for the reporting.

470
471
472
473

J. TRANSFER OF PERSONAL DATA TO THIRD PARTIES

474
475
476
477
478
479

The **Service Provider Organisation** shall not transfer Attributes to any third party (such as a collaboration partner) except:

- a) if mandated by the **Service Provider Organisation** for enabling the End User to access its Service on its behalf, or;
- b) if the third party is committed to the Code of Conduct or has undertaken similar duties considered sufficient under the data protection law applicable to the **Service Provider Organisation** or;
- c) if prior consent has been given by the End User.

480

The **Service Provider Organisation** shall not transfer Attributes to any third party (third party means a data controller other than the Home organisation or the Service Provider Organisation such as a collaboration partner) except:

481
482
483
484
485

- a) if the third party is a data processor for the **Service Provider Organisation** in which case an

486 ordinary controller-processor relationship applies between the **Service Provider**
487 **Organisation** and the third party working on behalf of the **Service Provider Organisation**.
488 The **Service Provider Organisation** must conclude a written agreement with such data
489 processor in accordance with applicable laws.
490

491 b) if the third party is committed to the Code of Conduct. This is expected to be the case for
492 various collaborative research scenarios, where the Service is provided to the **End User** by
493 several data controllers working in collaboration.
494

495 A typical scenario is where a research collaboration has a **Service Provider Organisation**
496 that receives **Attributes** from **Home Organisations** and passes on (parts of) those **Attributes**
497 to third parties providing the actual Services. In this case, where the **Service Provider**
498 **Organisation** acts as a proxy for the third parties, the **Service Provider Organisation** must
499 ensure that all third parties receiving Attributes are committed to the Code of Conduct or
500 similar (such as a Data Processing Agreement or a Data Transfer Agreement).
501

502 In contrast, if none of the **Attributes** received from the **Home Organisation** are being passed
503 on, e.g. when only an internal identifier assigned by the proxy is sent to the third parties, the
504 proxy does not need to make sure those third parties are committed to the Code of Conduct.
505

506 The organisation operating a proxy service, as described above, must act as intermediary
507 between the **Home Organisation** and the third party. For instance, the proxy needs to relay
508 the suspected privacy or security breaches to the **Home Organisation** or its Agent, as
509 described in clause h. Security measures.
510

511 c) if prior consent has been given by the **End User**. For the requirements of such consent, see
512 clause l. End User's consent.
513

514 If transfer to a third party includes also a transfer to a third country, the next clause imposes further
515 requirements.
516

517 K. TRANSFER OF PERSONAL DATA TO THIRD
518 COUNTRIES

519
520
521

522

1. Transfers among **Service Provider Organisations** that have adhered to the Code of Conduct.

This Code of Conduct constitutes an adequate legal basis for cross-border transfers of Attributes among the **Service Provider Organisations** that have adhered to it, whether the **Service Provider Organisation** receiving the Attributes is established in the European Economic Area or not. In other terms, the Code of Conduct legitimates cross-border transfers among the parties that have committed to the Code of Conduct.

2. Transfers to parties that have **not** adhered to this Code of Conduct established outside the EEA

The **Service Provider Organisation** guarantees that, when transferring **Attributes** to a party that has not adhered to this Code of Conduct and that is based outside the European Economic Area or in a country without an adequate level of data protection pursuant to Article 45.1 of the GDPR or the recipient is an International Organisation, to take appropriate safeguards.

523

Under European data protection legislation, transfers of personal data from the European Economic Area to third countries that do not offer an adequate level of data protection are restricted, unless the recipient territory ensures so-called "*appropriate safeguards*". However, Article 49 of the GDPR provides with an exhaustive list of derogations to this general prohibition. The following derogations are relevant for this context:

524
525
526
527
528
529

- **Consent of the End User:** The unambiguous consent of the data subject legitimates data transfers to third countries, even if the recipient does not offer an adequate level of protection. The **Service Provider Organisation** may rely on the End User's freely given informed revocable consent as described in clause l. End User's consent.
- **Contractual guarantees:** The existence of an appropriate contractual framework, supported by Standard contract clauses, either adopted by the European Commission or by a supervisory authority, the use of appropriate safeguards such as Binding Corporate Rules or other legally binding and enforceable instruments are recognised methods of transferring personal data. The use of Standard contract clauses does not exclude the possibility for the contracting parties to include them in a wider contract nor to add other clauses as long as they do not enter in contradiction. When using EU model clauses, the **Service Provider Organisation** needs to verify and ascertain that the other party is able to comply with all contractual obligations set out in the model clauses, especially taking into account local law applicable to such party.
- **Approved code of conduct:** an approved code of conduct pursuant to Article 40 of the GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548

If transferring Attributes to a third country involves also a transferring them to a third party, also clause j. Transfer of personal data to third parties needs to be satisfied.

549
550
551

L. END USER'S
CONSENT

552
553
554
555
556

557

Consent must be freely given, specific, informed and must unambiguously indicate the **End User's** wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of their personal data.

558

559 When a **Service Provider Organisation** relies on End User's consent (e.g. c. Deviating purposes, j.
560 Transfer of personal data to third parties, k. Transfer of personal data to third countries), it can be provided
561 by a written statement, including by electronic means. This could include ticking a box when visiting an
562 internet website, choosing privacy settings options of a software or another statement or conduct (i.e. a
563 clear affirmative action) which clearly indicates the data subject's acceptance of the proposed processing
564 of their personal data. Consent shall always be documented. Furthermore, the **End Users** shall be able to
565 withdraw their consent .

566

567 Following Recital 43 of the GDPR, the Service Provider Organisation shall not rely on consent when there
568 is a clear imbalance between the End User and the Service Provider Organisation.

569

570 Notice that this Code of Conduct for Service Provider Organisations does not make normative
571 requirements on the Home Organisation's legal grounds to release Attributes to the Service Provider
572 Organisation. However, the user interaction assumes the Attribute release is not based on the End User's
573 consent.

574

575

M.

576

LIABILITY

577

578

579

The Service Provider Organisation agrees to hold harmless the **End User and the Home Organisation** (as well as the Agent) who has suffered damage as a result solely of any violation of this Code of Conduct by the **Service Provider Organisation** as determined in a binding and enforceable judicial ruling.

580

581 In the event of damages related to the breach of this Code of Conduct (i.e.: using the **Attributes** for other
582 purposes, sharing the **Attributes** with third parties etc.), the **Service Provider Organisation** will hold
583 the other parties harmless following a binding and enforceable judicial ruling.

584

585 For example, in case an **End User** files a complaint against their **Home Organisation** for unlawful
586 release of **Attributes** after a **Service Provider Organisation** has released the **Attributes** to a third party,
587 the **Service Provider Organisation** agrees to assume the liabilities of the **Home Organisation** towards
588 the **End User** in respect of a breach of this Code of Conduct by the Service Provider Organisation.

589

590 A Service Provider Organisation shall be exempt from liability if it proves that it is not in any way
591 responsible for the event giving rise to the damage

592

593

N. GOVERNING LAW AND

594

JURISDICTION

595

596

597

598

This Code of Conduct shall be interpreted in the light of the GDPR and of the guidance issued by the European Data Protection Board or its predecessor⁵, always notwithstanding any privileges and immunities of Service Provider Organisations being International Organisations, as these are awarded by their constituent and/or statutory documents and international law.

If there are any disputes regarding the validity, interpretation or implementation of this Code of Conduct, the parties shall agree on how and where to settle them.

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

This Code of Conduct shall be interpreted in the light of the GDPR and of guidance issued by the regulatory authorities such as the European Data Protection Board

If there are disputes regarding the validity, interpretation or implementation of this Code of Conduct which cannot be settled amicably, the parties shall agree on how and where to settle them. For instance, if there is a dispute between a Home Organisation and Service Provider Organisation who are established in the same EU Member State, the parties can agree on using the local law and court. If the parties cannot come to an agreement, the Dutch laws and courts are assumed. If at least one party to the dispute is an International Organisation, the dispute must be submitted to final and binding arbitration. In the absence of agreement over applicable arbitration rules, any dispute, controversy or claim arising out of or in relation to this Code of Conduct, or the existence, interpretation, application, breach, termination, or invalidity thereof, shall be settled by arbitration in accordance with the PCA Arbitration Rules 2012.

O. ELIGIBILITY

The Code of Conduct must be implemented and executed by a duly authorised representative of the **Service Provider Organisation**.

623

624

625

626

627

628

629

630

631

Each **Service Provider Organisation** must make sure that the commitment to this Code of Conduct is done by a person or by several persons (sometimes called a “signature authority”) who has or have the right to commit the **Service Provider Organisation** to this Code of Conduct.

The person administering the Service that receives **Attributes** must identify the person or body in their organisation that can decide if the **Service Provider Organisation** commits to this Code of Conduct, as the Service administrator cannot necessarily take this decision on their own.

P. TERMINATION OF THE CODE OF CONDUCT

632

633

634

635

636

⁵ The Opinion 8/2010 on applicable law of the Article 29 Working Party, as updated in 2015, provides useful guidance on how to determine the applicable law in cross-national collaborations.

637

The **Service Provider Organisation** can only terminate adherence to this Code of Conduct in case of:

- this Code of Conduct being replaced by a similar arrangement, or;
- the termination of the Service provisioning to the Home Organisation or;
- the effective notification provided by the authorised representative of the Service Provider Organisation to terminate its adherence to this Code of Conduct.

638

639 Even after the **Service Provider Organisation** has terminated its adherence to the Code of Conduct, the
640 Attributes received continue to be protected by the principles enshrined in this Code of Conduct (see q.
641 Survival of the Code of Conduct).

642

643 Q. SURVIVAL OF THE CODE OF 644 CONDUCT

645

646

647

648

The **Service Provider Organisation** agrees to be bound by the provisions of this Code of Conduct that are intended to survive due to their sense and scope after the end, lapse or nullity of this Code of Conduct until the processing terminates.

649

650 R. 651 PRECEDENCE

652

653

The Service Provider Organisation warrants to comply with the stipulation that, in the event of conflict between a provision contained in this Code of Conduct and a provision of the agreement concluded between the **Service Provider Organisation** and the **Home Organisation**, the provision of the agreement concluded between **Service Provider Organisation** and **Home Organisation** takes precedence over the provision of this Code of Conduct.

In case of conflict between the provisions of the agreement between the Service Provider Organisation and the Home Organisation, this Code of Conduct and/or the data protection legislation, the following order shall prevail:

1. the agreement between the Home Organisation and the Service Provider Organisation;
2. the provisions of this Code of Conduct and;
3. Applicable Data Protection Laws (such as other country specific law on Data protection or Privacy).

654

655 If a **Service Provider Organisation** has an agreement (possibly a data processing agreement) with (some
656 of) the **Home Organisation(s)** and the agreement is in conflict with this Code of Conduct, that agreement
657 has precedence.

658
659 This section allows the **Service Provider Organisation** to have a bilateral agreement overriding the Code
660 of Conduct with some **Home Organisations**, meanwhile, this Code of Conduct will still apply to the
661 other **Home Organisations** that have not entered into a bilateral agreement.
662

663 **ATTRIBUTE** 664 **PROVIDERS**

665
666
667 An Attribute Provider is an organisation other than the Home Organisation that manages extra Attributes
668 for End Users of a Home Organisation and releases them to the Service Provider Organisation.

669
670 According to Section Functional Scope, the Service Provider Organisation and the communities
671 representing the Service Provider Organisation can agree to apply the Code of Conduct also to other
672 Attributes, such as those the Service Provider Organisation manage and share themselves. The
673 organisation managing the extra Attributes becomes an Attribute Provider.
674

675 When the Code of Conduct is applied to Attributes managed by Attribute Providers, the Service Provider
676 Organisation further agrees and warrants the following:
677

- 678 - (see clause i. Security Breaches) the Service Provider Organisation commits to report all
679 suspected privacy or security breaches also to the Attribute Provider;
- 680 - (see clause m. Liability) the Service Provider Organisation agrees to hold harmless also the
681 Attribute Provider who has suffered damage as a result solely of any violation of this Code of
682 Conduct by the Service Provider Organisation as determined in a binding and enforceable judicial
683 ruling;
- 684 - (see clause r. Precedence) the Service Provider Organisation warrants to comply also with the
685 stipulation that, in the event of conflict between a provision contained in this Code of Conduct
686 and a provision of the agreement concluded between the Service Provider Organisation and the
687

688 Attribute Provider, the provision of the agreement concluded between Service Provider
689 Organisation and Attribute Provider takes precedence over the provision of this Code of Conduct.
690
691

692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722

APPENDIX 1: INFORMATION DUTY TOWARDS END USERS

This appendix consists of two parts:

- I. How a Service Provider Organisation can develop a Privacy Notice.

Although this is a mandatory obligation, practice has shown that it is a challenge for many **Service Provider Organisations** to develop an appropriate Privacy Notice for the Services they provide. A practical template is provided to assist the **Service Provider Organisations**.

- II. How the **Home Organisation** should inform the **End User** about the **Attribute release**.

This guideline is primarily for software developers who develop an **End User** interface for the **Attribute** release on an **Identity Provider** server.

PRIVACY NOTICE TEMPLATE

This template intends to assist **Service Provider Organisations** in developing a Privacy Notice document that fulfils the requirements of the GDPR and the Code of Conduct. The template presents some examples (in italics) and proposes some issues that should be taken into account.

The Privacy Notice must be provided at least in English. You can add another column to the template for a local translation of the text. Alternatively, the local translation can be a parallel page, and you can use the xml:lang element to introduce parallel language versions of the Privacy Notice page as described in SAML2 Profile for the Code of Conduct.

Name of the Service	SHOULD be the same as mdui:DisplayName <i>WebLicht</i>
Description of the Service	SHOULD be the same as mdui:Description <i>WebLicht is a service for language research. It provides an execution environment for automatic annotation of text corpora.</i>
Data controller and a contact person	<i>Tübingen university, Institute for language research</i> <i>Laboratory manager Bob Smith, bob.smith@example.org</i>
Personal data processed and the legal basis for processing	<i>A. Personal data retrieved from your Home Organisation:</i> <i>- your unique user identifier (SAML persistent identifier) *</i> <i>- your role in your Home Organisation (eduPersonAffiliation Attribute) *</i> <i>- your name *</i>

B. Personal data you have provided or may be generated as a result of your use of our service:

*- logfiles on the service activity **

- your profile

...

** = the personal data is necessary for providing the Service that the End User has requested. Other personal data is processed because you have consented to it.*

Please make sure the list A. matches the list of requested Attributes in the Service Provider Organisation's SAML 2.0 metadata.

Purpose of the processing of personal data

Don't forget to describe also the purpose of the log files, if they contain personal data (usually they do).

Your personal data is used

- to authorise your access to and use of the compute resources we provide;*
- to properly account your use to relevant infrastructure funding bodies;*
- to ensure the integrity and availability of our service*

Third parties to whom personal data is disclosed

Notice clause j of the Code of Conduct for Service Provider Organisations.

We may share your personal data with third parties (or otherwise allow them access to it) in the following cases:

(a) to satisfy any applicable law, regulation, legal process, subpoena or governmental request

(b) to enforce this Privacy Policy, including investigation of potential violations thereof;

Inform the user that his/her personal data may be displayed to other users of the service or to the public.

Your personal data may be accessible by others users and by the public (e.g. for a wiki, a text in the bottom of the page may state "This page was last edited by [first name] [last name] ...".)

Are the 3rd parties outside EU/EEA or the countries or international organisations whose data protection EC has decided to be adequate? If yes, add references to the appropriate or suitable safeguards.

	<p><i>In the case where a third party is located in a country whose data protection laws are not as comprehensive as those of the countries within the European Union we will take appropriate steps to ensure that transfers of your personal data are still protected in line with European standards.</i></p> <p><i>You have a right to contact us for more information about the safeguards we have put in place to ensure the adequate protection of your personal data when this is transferred as mentioned above.</i></p>
How to access, rectify and delete the personal data and object its processing.	<p><i>Contact the contact person above.</i></p> <p><i>To rectify the data released by your Home Organisation, contact your Home Organisation's IT helpdesk.</i></p>
Withdrawal of consent	<p>If personal data is processed based on user consent, how can they withdraw it?</p>
Data portability Data retention	<p>Can the user request their data be ported to another Service? How? When the user record is going to be deleted or anonymised? Remember, you cannot store user records infinitely. It is not sufficient that you promise to delete user records on request. Instead, consider defining an explicit period.</p> <p><i>Personal data is deleted on request of the user or if the user hasn't used the Services for 18 months</i></p>
Data Protection Code of Conduct	<p><i>Your personal data will be protected according to the Code of Conduct for Service Provider Organisations, a common standard for the research and higher education sector to protect your privacy.</i></p>
Data controller's data protection officer, if applicable	<p>If the controller has a data protection officer (GDPR Section 4)</p> <p><i>Chief Security Officer bill.smith@example.org</i></p>
Jurisdiction and supervisory authority	<p>The country in which the Service Provider Organisation is established and whose laws are applied.</p> <p>SHOULD be an ISO 3166 code followed by the name of the country and its subdivision if necessary for qualifying the jurisdiction.</p> <p><i>DE-BW Germany Baden-Württemberg</i></p> <p>How to lodge a complaint to the competent Data protection authority:</p> <p><i>Instructions to lodge a complaint are available at ...</i></p>

725

APPENDIX 2: INFORMATION SECURITY, TECHNICAL AND ORGANISATIONAL GUIDELINES FOR SERVICE PROVIDER ORGANISATIONS

726

728 This annex describes the technical and organizational security measures for protecting the **Attributes** as
 729 well as the information systems of the Service Provider Organization where they are processed (such as a
 730 SAML SP software, the infrastructures on which the software is deployed and the application(s) it supplies
 731 with the Attributes). Note that the scope of this document is limited to what is required to protect the
 732 Attributes. The Service Provider Organization may need to define additional requirements for the
 733 protection of its assets.

734

735 To address the technical and organizational measures to protect the Attributes as well as the information
 736 systems of the Service Provider Organization where they are processed, it is recommended that the **Service
 737 Provider Organizations** adopt the security measures described in the Sirtfi trust framework (ver 1.0)
 738 [SIRTFI] which are copied below for convenience.

739

NORMATIVE

ASSERTIONS

740

741

742

743

744 In this section a set of assertions are defined that each organization shall self-attest to so that they may
 745 participate in the Sirtfi trust framework. These are divided into four areas: operational security, incident
 746 response, traceability and participant responsibilities.

747

748 An attestation to the assertions in this document refers specifically and only to the statements in this
 749 section that are identified by labels within square brackets “[“, “]”.

750

751 How comprehensively or thoroughly each asserted capability should be implemented across an
 752 organization’s information system assets is not specified. The investment in mitigating a risk should be
 753 commensurate with the degree of its potential impact and the likelihood of its occurrence, and this
 754 determination can only be made within each organization.

755

1 OPERATIONAL SECURITY [OS]

756 Managing access to information resources, maintaining their availability and integrity, and maintaining
 757 confidentiality of sensitive information is the goal of operational security.

758

759 ● [OS1] Security patches in operating system and application software are applied in a timely
 760 manner.

761

762 ● [OS2] A process is used to manage vulnerabilities in software operated by the organization.

763

764 ● [OS3] Mechanisms are deployed to detect possible intrusions and protect information systems
 765 from significant and immediate threats

766

767 ● [OS4] A user’s access rights can be suspended, modified or terminated in a timely manner.

768

769 ● [OS5] Users and Service Owners (as defined by ITIL [ITIL]) within the organization can be
 770 contacted.

771

772 ● [OS6] A security incident response capability exists within the organization with sufficient
 773 authority to mitigate, contain the spread of, and remediate the effects of a security incident.

774

2 INCIDENT RESPONSE [IR]

775 Assertion [OS6] above posits that a security incident response capability exists within the organization.
776 This section's assertions describe its interactions with other organizations participating in the Sirtfi trust
777 framework.

- 778 • [IR1] Provide security incident response contact information as may be requested by an R&E
779 federation to which your organization belongs.
- 780 • [IR2] Respond to requests for assistance with a security incident from other organizations
781 participating in the Sirtfi trust framework in a timely manner.
- 782 • [IR3] Be able and willing to collaborate in the management of a security incident with affected
783 organizations that participate in the Sirtfi trust framework.
- 784 • [IR4] Follow security incident response procedures established for the organization.
- 785 • [IR5] Respect user privacy as determined by the organizations policies or legal counsel.
- 786 • [IR6] Respect and use the Traffic Light Protocol [TLP] information disclosure policy.
- 787
- 788
- 789
- 790
- 791
- 792
- 793

3 TRACEABILITY [TR]

794 To be able to answer the basic questions "who, what, where, and when" concerning a security incident
795 requires retaining relevant system generated information, including accurate timestamps and identifiers of
796 system components and actors, for a period of time.

- 797 • [TR1] Relevant system generated information, including accurate timestamps and identifiers of
798 system components and actors, are retained and available for use in security incident response
799 procedures.
- 800 • [TR2] Information attested to in [TR1] is retained in conformance with the organization's security
801 incident response policy or practices.
- 802
- 803
- 804

4 PARTICIPANT RESPONSIBILITIES [PR]

805 All participants (IdPs and SPs) in the federations need to rely on appropriate behavior.

- 806 • [PR1] The participant has an Acceptable Use Policy (AUP).
- 807 • [PR2] There is a process to ensure that all users are aware of and accept the requirement to abide
808 by the AUP, for example during a registration or renewal process.
- 809
- 810
- 811
- 812
- 813

814 REFERENCES

817 [ITIL] Axelos ITIL Glossary of Terms, <https://www.axelos.com/glossaries-of-terms>

818 [SIRTFI] A Security Incident Response Trust Framework for Federated Identity, version 1.0:
819

GÉANT -Data Protection Code of Conduct (GDPR Version). (version 11 – 25 November 2019)

820 <https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf>

821

822 [TLP] US Cert Traffic Light Protocol, <https://www.us-cert.gov/tlp>

823

824

825



APPENDIX 3: OVERSIGHT OF THE CODE OF CONDUCT

INTRODUCTION

This appendix describes the oversight mechanism for the monitoring of compliance with GÉANT Data Protection Code of Conduct . As a result, actions can be raised and the monitoring body can intervene. It also provides with examples of situations of non-compliance to this Code of Conduct.

This Data protection Code of Conduct relies on the following principles:

- the **Home Federation** that has registered a **Service Provider Organisation** records a technical indication (currently, using a tag embedded in SAML 2.0 metadata) of the **Service Provider Organisation's** adherence to the Code of Conduct. The indication signals that the **Service Provider Organisation** believes that its Service is being operated in a manner that is consistent with the Code of Conduct.
- The technical infrastructure (currently, SAML 2.0 metadata exchange service) that the federation(s) provides delivers the indications from Service Provider Organisations to **Home Organisations'** Identity Provider servers.
- Notifying a **Service Provider Organisation** of a potential (suspected) non-compliance issue does not transfer responsibility from the **Service Provider Organisation to the notifying party**.

The oversight mechanism of this Data Protection Code of Conduct implies:

- The appointment of an accredited Monitoring Body;
- Three layers of monitoring:
 - Technical conformance checks;
 - Behavioral conformance checks;
 - Complaints handling mechanism.

Taking into account the nature of the personal data processed and the potential number of SPOs (thousands), the oversight mechanisms focus on measures that can be fully automated or that rely on self-assessments made by the SPOs.

MONITORING BODY OF THE CODE OF CONDUCT

The Monitoring Body of the Code of Conduct is accredited in accordance with Article 41 of the GDPR. This section shall be interpreted in the light of the guidance to be issued by the regulatory authorities such as the European Data Protection Board.

875 The Monitoring body has:

- 876 • demonstrated its independence and expertise in relation to the subject-matter of this Data
877 Protection Code of Conduct to the satisfaction of the competent Supervisory Authority;
- 878 • established procedures which allow it to assess the eligibility of **Service Provider Organisation**
879 concerned to apply this Data Protection Code of Conduct, to monitor their compliance with its
880 provisions and to periodically review its operation;
- 881 • established procedures and structures to handle complaints about infringements of this Data
882 Protection Code of Conduct or the manner in which this Data Protection Code of Conduct has
883 been, or is being, implemented by **Service Provider Organisation**, and to make those procedures
884 and structures transparent to data subjects and the public; and
- 885 • demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties
886 do not result in a conflict of interests.

887
888 The Monitoring Body is responsible for:

- 889 • monitoring the **Service Provider Organisations**' compliance with the Code of Conduct;
- 890 • issuing guidelines on the implementation of the Code of Conduct;
- 891 • providing guidance on the self-assessment procedure for Service Provider Organisations and
892 issue checklist;
- 893 • establishing procedures and structures to handle complaints about infringements of the Code
894 transparent and making its contact details available to the public;
- 895 • handling complaints received from End Users, Home Organisations, Federation Operators or
896 other parties.

897
898
899 The working language of the Monitoring Body shall be English.
900

901 MONITORING MECHANISM

902 1 TECHNICAL CONFORMANCE

905
906 The monitoring body does automated technical checks through a monitoring tool⁶ at least every day to all
907 SPs committed to the Code of Conduct. The monitoring tool performs technical checks to the Services to
908 make sure they have published a privacy notice document and the list of necessary Attributes that Home
909 Organisations need to release. The tool provides a page where Service administrators can check their
910 technical conformance (see Figure below) and sends e-mail message to its administrator if it encounters a
911 problem.
912 Should the problem persist, the process to remove the indication of the SP's conformance with the code of
913 conduct will be initiated.
914

⁶ <http://monitor.edugain.org/coco>

951 If anyone (such as an End User, a **Home Organisation** or a Federation Operator) suspects that a **Service**
952 **Provider Organisation** is not complying with the Code of Conduct to which it has committed, the
953 following alternative, mutually non-exclusive, actions are suggested:

- 954 1. Contact the Service Provider Organisation directly (with a copy to the **Service Provider**
955 **Organisation's** Home Federation), describing the suspected problem, and ask the **Service**
956 **Provider Organisation** to check if it has a compliance problem and correct it;
- 957 2. Contact the Service's Home Federation, and request to contact the **Service Provider**
958 **Organisation** and to check if there is a compliance problem and request to correct it. Depending
959 on the Home Federation's policy, there may be also additional measures available for handling
960 non-compliance;
- 961 3. Contact the Monitoring Body accredited to monitor compliance with the Code of Conduct, if
962 applicable, as defined in Article 41 of the GDPR and below;
- 963 4. Determine the location of the legal entity operating the **Service Provider Organisation** (see
964 clause e), and lodge a complaint with the competent Supervisory Authority (as defined in Articles
965 57 and 58 of the GDPR).

966
967
968
969 Having received a complaint the Monitoring Body will:

- 970
971 I. ask the **Service Provider Organisation** to present its counterpart,
- 972 II. if the monitoring body finds the **Service Provider Organisation** to be non-
973 compliant with the Code of Conduct, give the **Service Provider Organisation** at
974 most four weeks' time to remediate the issue,
- 975 III. communicate the **Service Provider Organisation** the decision to remove the
976 **Service Provider Organisation's** tag and allow the **Service Provider**
977 **Organisation** to introduce an appeal within two weeks after the notification of
978 the decision to the **Service Provider Organisation**,
- 979 IV. acknowledge receipt and consider the appeal submitted by the **Service Provider**
980 **Organisation**,
- 981 V. mandate the Home Federation to remove the **Service Provider Organisation's**
982 tag if the appeal has been dismissed and if the Service Provider Organisation has
983 not fixed the non-compliance issue within the given timeframe.

984 The Service's Home Federation must be informed on steps I-IV and Service Provider Organisation on
985 step V.
986

987 The **Service Provider Organisation** whose tag has been removed can reclaim the tag only after
988 demonstrating to the monitoring body that it has returned to compliance. The Service Provider Organisation
989 can appeal the decision of the Monitoring Body with the competent Supervisory Authority pursuant to
990 Article 41.4 of the GDPR.

991
992
993

994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046

APPENDIX 4: GLOSSARY OF TERMS

Agent: the organisation operating the Identity Provider on behalf of the Home Organisation, if applicable.

Attribute(s): the End User's Personal Data as managed by the Home Organisation (or its Agent) and requested by the Service Provider Organisation, such as (but not limited to) name, e-mail and role in the Home Organisation.

Attribute Provider: an organisation other than the Home Organisation that manages extra Attributes for End Users of a Home Organisation and releases them to the Service Provider Organisations.

Data Controller: the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for their nomination may be designated by national or Community law

Data Processor: a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

EEA: European Economic Area.

End User: any natural person affiliated with a Home Organisation, e.g. as a researcher or student, making use of the Service of a Service Provider Organisation.

End User's consent: any freely given, specific, informed and unambiguous indication of the End Users wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.

Federation: an association of Home Organisations and Service Provider Organisations typically organised at national level, which collaborate for allowing cross-organisational access to Services.

Federation Operator: an organisation that manages a trusted list of Identity Providers and Services registered to a Federation.

GDPR: Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Home Organisation : the organisation with which an End User is affiliated, operating the Identity Provider by itself or through an Agent. It is responsible for managing End Users' identity data and authenticating them.

Identity Provider (IdP): the system component that issues Attribute assertions on behalf of End Users who use them to access the Services of Service Provider Organisations.

International Organisation: an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

Personal Data: any information relating to an identified or identifiable natural person.

1047 **Processing of personal data:** any operation or set of operations which is performed upon personal data,
1048 whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or
1049 alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making
1050 available, alignment or combination, blocking, erasure or destruction.

1051
1052 **Service:** an information society service, in the sense of Article 1 point 2 of Directive 98/34/EC. This
1053 means any service provided, at a distance, by electronic means and at the individual request of a recipient
1054 of services.

1055
1056 **Service Provider Organisation (SP):** an organisation that is responsible for offering the End User the
1057 Service they desire to use.

1058
1059 **Supervisory Authority:** an independent public authority responsible for monitoring the application of the
1060 GDPR and the national data protection legislations in order to protect the rights and freedoms of the data
1061 subjects in relation to the processing of their personal data.