1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

GÉANT Data Protection Code of Conduct
(GDPR Version)

Draft 23st February 2017

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

48

49

50

Géant -Data Protection Code of Conduct (GDPR Version).

100

| 101 | **GLOSSARY** |

102 103 **Agent**: The organisation operating the Identity Provider on behalf of the Home Organisation, if applicable.

104 105 106 **Attribute(s):** The End User's Personal Data as managed by the Home Organisation or its Agent and requested by the Service Provider, such as (but not limited to) name, e-mail and role in the Home Organisation.

107 108 109 110 111 **Data Controller:** shall mean 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 his nomination may be designated by national or Community law.

112 113 **Data Processor**: shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

114 115 116 **DPD**: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

117 **EEA**: European Economic Area

118 119 **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.

120 121 122 **End User Consent**: any freely given, specific, informed and unambiguous indication of the End Users wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

123 124 **Federation**: An association of Home Organisations and Service Providers typically organised at national level, which collaborate for allowing cross-organisational access to services.

125 126 **Federation Operator**: An organisation that manages a trusted list of Identity and Service Providers registered to a Federation.

127 128 129 **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).

130 131 132 **Home Organisation (HO)**: 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.

133 134 **Identity Provider (IdP)**: The system component that issues Attribute assertions on behalf of End Users who use them to access the services of Service Providers.

135 136 **Personal Data**: any information relating to an identified or identifiable natural or legal person, if applicable.

137	**Processing of personal data:** any operation or set of operations which is performed upon personal
138	data, whether or not by automatic means, such as collection, recording, organisation, storage,
139	adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or
140	otherwise making available, alignment or combination, blocking, erasure or destruction.
141	**Service Provider (SP)**: An organisation that is responsible for offering the End User the service
142	he or she desires to use.

PURPOSE OF THIS CODE OF CONDUCT

This Code of Conduct related to the sector of access management in the European Research Area is ruled by the 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, GDPR).

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

Without prejudice to the provisions as set forth in the agreement between the **Home Organisation** and the **Service Provider**, which in all cases takes precedence, this Code of Conduct sets the rules that Service Providers adhere to when they want to receive End Users' Attributes from **Home Organisations** or their Agent for providing access to their services.

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 Providers** and,

(3) enforcement procedures for non-compliance with the Code of Conduct.

The GDPR principles and rules will apply to the whole Code of Conduct, specifically:

(a) fair and transparent processing;

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(h) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

 (i) the transfer of personal data to third countries or international organisations; or

172   (j) out-of-court proceedings and other dispute resolution procedures for resolving disputes between
173 controllers and data subjects with regard to processing, without prejudice to the rights of data subjects
174 pursuant to Articles 77.

175

WHO CAN ADHERE THIS CODE OF CONDUCT?

177

178 This Code of Conduct is addressed to any **Service Provider** established in any of the 28 Member States of
179 the European Union and in any of the countries belonging to the European Economic Area (28 Member
180 States of the European Union, Iceland, Liechtenstein and Norway).

181 Furthermore, **Service Providers** established in any third country offering an adequate level of data
182 protection in the terms of the article 45 of the GDPR can also subscribe to this Code of Conduct.

183 The GDPR gives the opportunity to **Service Providers** that do not fall under the territorial scope of the
184 Regulation (Article 3, territorial scope) and that are established outside of the EEA to join this Code of
185 Conduct in order to provide appropriate safeguards within the framework of transfers of personal data to
186 third countries or international organisations under the terms referred to in point (e) of Article 46(2).

187

CONTEXT

189

190 GÉANT is the pan-European research and education backbone network that interconnects Europe's
191 National Research and Education Networks (NRENs). Together with its national partners (the NRENs), the
192 GÉANT network offers network connectivity and associated services (such as an e-infrastructure for
193 electronic identity) to over 10.000 research and education institutions in 42 countries, including all EU
194 Member States.

195 Without a proper e-infrastructure for electronic identities, the researchers in the European Research Area
196 need to manage credentials for thousands of services, inhibiting effective co-operation and research and
197 creating administrative burdens. To provide an e-infrastructure for secure authentication, authorisation and
198 single sign-on of researchers and other End Users, a novel approach, Federated Identity Management is
199 deployed.

200

201

202

203

204
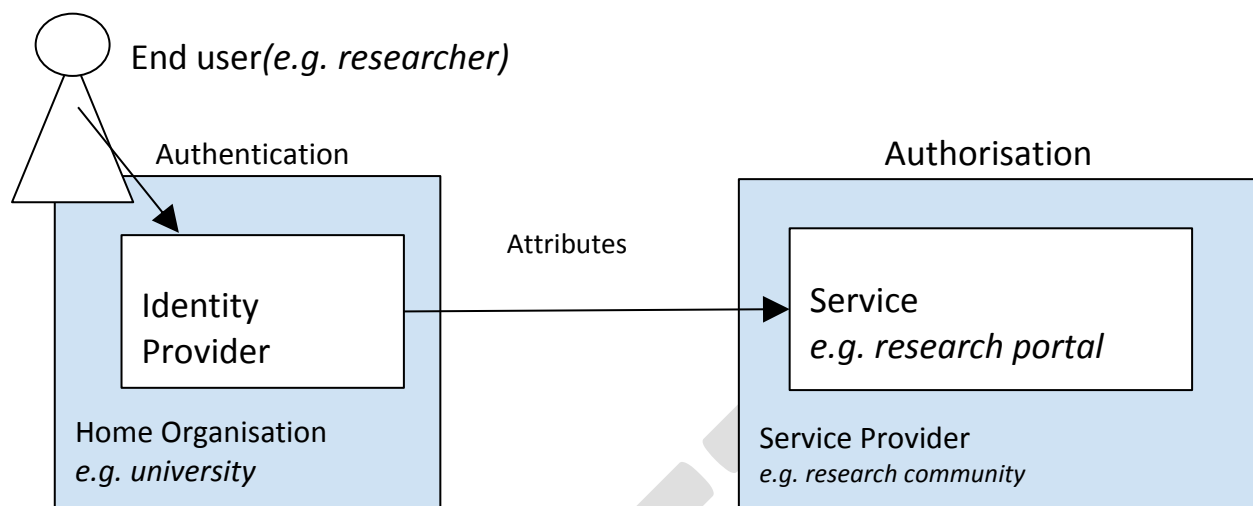
205   This Code of Conduct specifies the data protection rules applicable to **Service Providers** in the context of
206   the GÉANT federated identity management system, providing trust and confidence to all stakeholders
207   involved in the federated identity management. Not using the federated identity management system would
208   force the **End Users** either to register a local account and password and self-assert their attributes in the
209   **Service Provider** (which does not support information security) or to use a commercial Identity Provider
210   outside the EU/EEA territory and the countries with adequate protection, which does not necessarily
211   enhance their privacy.

212   In federated identity management, an End User's **Home Organisation** (e.g.: the university or research
213   institution employing a researcher, the student's university, etc.) manages his personal data and user account.
214   When the **End User** wants to log in to a service provided by another organisation - potentially in a different
215   country – the Home Organisation authenticates them and releases the **Service Provider** the Attributes
216   necessary for the service.

217   This approach allows the user's Attributes and authentication to be managed in the **Home Organisation**,
218   which has a close relationship with them, favouring the provenance and freshness of the Attributes and
219   reducing the risk of an identity theft.

220   As a result, the End User has a **single set of credentials** (such as, username and password) and potentially
221   a single sign-on that permits the End User to authenticate once and then access multiple services.

222   The **Service Provider** decides which users are authorised to access the service. Consequently, this approach
223   requires that the **Home Organisations** feel confident to release their End Users' Attributes to the **Service**
224   **Provider**.

225   This identification system also complies with the principle of **minimisation of personal data** (Article 5.c
226   of the GDPR), as the Service Provider will not necessarily need to process further categories of personal
227   data. For further information, see clause c. Data minimization.

228 In addition to this, taking into account the nature of the implementation and the purposes of processing, it
229 can be confirmed that both the **Service Provider** and the **Home Organisation** have designed a system that
230 complies, in an effective manner, with all the principles of the GDPR.

231 The GÉANT network integrates the necessary safeguards into the processing in order to meet the
232 requirements of the GDPR and ensures protection of the rights of data subjects and principles such data
233 protection by design and by default (Article 25 of the GDPR).

234

SCOPE

236

237 This Code of Conduct is limited to the processing of **Attributes which are necessary** for enabling access
238 to the Service.

239

ROLES OF THE PARTIES INVOLVED

241 As a reminder, the data controller is the **Home Organisation** (HO) which, alone or jointly with others,
242 determines the purposes and means of the processing of personal data (e.g.: the university).

243 The data processor is the organisation which processes personal data on behalf of the controller.

244 A data subject is the natural person whose **Attributes** are being processed, the **End User** (e.g: the researcher
245 or the student).

246 In the context of this Code of Conduct:

247   1. A **Home Organisation** acts as a data controller as to the wider relationship with the **End User**, for
248   example operating the IdP server in respect of the Attributes. An Agent who operates the IdP server
249   on behalf of the **Home Organisation** acts as a data processor. This includes also the Federation
250   Operators who operate a (potentially centralised) IdP server on behalf of the **HO**.

251   2. A **Service Provider** acts as a data controller in respect of the **Attributes**, processing them for the
252   purposes as described in the clause b. Purpose limitation. In certain circumstances a **Service
253   Provider** may be acting as a data processor, acting on behalf and as instructed by the **Home
254   Organisation**.

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

257

258 As presented in the picture below, the relevant data processing activities carried out by the **Home
259 Organisation** are typically being described in the **Home's Organisation** privacy policy.

260

End User
(data subject)

Privacy
policy

Service related
privacy policy

Code of
Conduct

Home
Organization
(data
controller)

Service Provider
(typically data
controller)

261

262

263
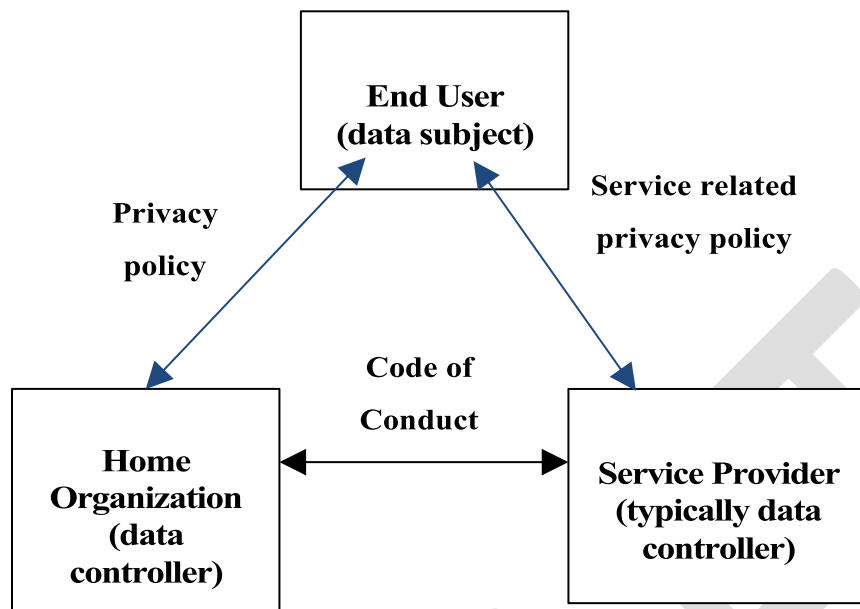
As far as the disclosure of the **Attributes** of the **End User** is concerned, the **Service Provider** is obliged to comply with the obligations of the Code of Conduct.

The processing of the **Attributes** by the **Service Provider** for enabling access to the service is further explained in the Service-related Privacy Policy.

In the case that a Federation and a Federated operator do not process the **Attributes** of the **End User**, no specific privacy policy needs to be put in place.

270

271

272

273

274

275

276

277

PRINCIPLES OF THE PROCESSING OF ATTRIBUTES

To the extent the **Service Provider** acts as a data controller, it agrees and warrants:

A. LEGAL COMPLIANCE

All data processing activities carried out in this context shall comply with the GDPR.

The **Service Provider** based in the EEA territory commits to process the End User's **Attributes** in accordance with the applicable European data protection legislation.

The **Service Provider** based outside the EEA commits to process the End User's Attributes in accordance with the GDPR, this Code of Conduct and the eventual contractual arrangements (e.g: EU model clauses).

In principle, a **Service Provider** established in the EEA territory, subject to the European Data Protection legislation, should not find himself in a situation where their national data protection laws would contradict this Code of Conduct.

The **Service Provider** is expected to examine if any point in this Code of Conduct enters into conflict with the national data protection laws of his jurisdiction. In case of conflict of laws, the national law of his jurisdiction should be applicable. However, the Service Provider shall not commit to the Code of Conduct.

Service Providers established outside the EEA territory but in a country offering an adequate data protection pursuant to Article 45 of the GDPR, should assess the compliance of this Code of Conduct with their local laws. The **Service Provider** shall communicate any incompatibility to the community.

As far as Service Providers established in countries outside the EEA territory without offering an adequate level of protection pursuant to Article 45 of the GDPR are concerned, they shall, together with this Code of Conduct, engage on binding and enforceable commitments to apply the appropriate safeguards, including as regards data subjects' rights.

Service Providers may be subject to internal regulations and policies of Intergovernmental Organisations.

Regarding the applicable law, please, see clause o. Governing law and jurisdiction.

308

B. PURPOSE LIMITATION

310

311 The **Service Provider** warrants processing Attributes of the **End User** solely for the purposes of enabling
312 access to the services. The Service Providers agree that the End User's personal data is collected for specific,
313 explicit and legitimate purposes. The Attributes shall not be further processed in a manner which is not
314 compatible with the initial purposes (Article 5.b of the GDPR).

315 The Service Provider must ensure that Attributes are used only for enabling access to the service. As far as
316 the use of Attributes deviating purposes is concerned, please, see clause d. Deviating purposes.

317 In practice, enabling access to the service covers:

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

325 • **Identification** i.e. **End Users** need to have a personal account to be able to access their own files,
326 datasets, pages, documents, postings, settings, etc. The provenance of an **Attribute** used for
327 identification is important; to avoid an identity theft, one cannot self-assert their own identifier.
328 Instead, the Identity Provider server authenticates them and provides the **Service Provider** an
329 **Attribute** that contains their authenticated identifier.

330 • **Transferring real-world's trust** to the online world i.e. if the **Service Provider** supports a user
331 community that exists also in the real world, **Attributes** can be used to transfer that community to
332 the online world. For instance, if the members of the user community know each other's by name
333 in the real world, it is important that their names (or other identifiers) are displayed also in any
334 discussion or collaboration forum offered by the **Service Provider**. The provenance of those
335 **Attributes** is important; to avoid identity theft, one cannot assume user's name to be self-asserted
336 but retrieved from a trustworthy source.

337 • **Researcher unambiguity** i.e. ensuring that a researcher's scientific contribution is associated
338 properly to them and not to a wrong person (with potentially the same name or initials). In the
339 research sector, publishing scientific results is part of researchers' academic career and the
340 researchers expect to receive the merit for their scientific contribution. There are global researcher
341 identification systems (such as, ORCID and ISNI) which assign identifiers for researchers to help
342 scientific Service Providers to properly distinguish between researchers, even if they change their
343 names or organisation they are affiliated with.

344 • **Other functionalities** offered by the **Service Provider** for enabling access to the services, i.e.
345 using **Attributes** of users for the purposes of other functionalities offered by the Service Provider.
346 It is common that services on the Internet send e-mail or other notifications to their users regarding

347 their services. Examples of scenarios where processing End User's email address or other contact
348 detail falls within the scope of enabling access to the service include for instance:

349 ▪ the End User's application to access scientific resources has been
350 approved by the resource owner;

351 ▪ the End User's permission to use a resource is expiring or they are running
352 out of the resource allocation quota;

353 ▪ someone has commented the End User's blog posting or edited their wiki
354 page.

355 Conversely, processing End User's e-mail address for sending them commercial or unsolicited messages
356 does not fall within the scope of enabling access to the service of the **Service Provider**.

357

358 ## C. DATA MINIMIZATION

359

360 To minimize the Attributes requested from a **Home Organisation** to those that are adequate, relevant and
361 not excessive for enabling access to the service and, where a number of Attributes could be used to provide
362 access to the service, to use the least intrusive Attributes possible.

363 The following list presents examples of attributes that are **adequate**, **relevant** and **not excessive** for
364 enabling access in the context of the service:

365 • an attribute (such as, eduPersonAffiliation, eduPersonEntitlement or schacHomeOrganisation)
366 indicating the End User's permission to use the service:

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

369 • an attribute (such as SAML2 PersistentId) uniquely identifying the End User required, for instance,
370 to store the End User's service profile:

371 ▪ a trusted value provided by the IdP is needed. The End User cannot self-
372 assert their unique identifier

373 • if there are several alternative unique identifiers available for the service, the least intrusive must
374 be used

375 ▪ pseudonymous bilateral identifier (SAML2 persistentId) is preferred

376 ▪ if there is a legitimate reason to match the same End User's accounts
377 between two Service Providers, a Service Provider can request a more
378 intrusive identifier (such as eduPersonPrincipalName or

379   eduPersonUniqueID), whose value for a given user is shared by several
380   Service Providers

381   ■   if there is a legitimate reason for an End User (such as, a researcher) to
382   keep their identity and profile in the Service Provider even when the
383   organisation they are affiliated with changes, a permanent identifier (such
384   as, ORCID identifier) can be used

385 • a name attribute (such as cn or DisplayName attribute) is necessary for a wiki or other collaboration
386   platform, if the End Users know each other in real life and need to be able to transfer their existing
387   real-world trust to an online environment.

388   ■   if it makes a difference in the collaboration platform to know the person's
389   name, it can be released.

390   ■   otherwise, the user may be indicated as "unknown" or a pseudonym the
391   user has selected or the system has assigned to him/her.

392 • e-mail address or other contact details, if it is necessary to contact the **End User** for the proper
393   functioning of the services offered by the **Service Provider**.

394

395 In the context of this Code of Conduct, under no circumstances a **Service Provider** is authorized to request
396 End User's Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical
397 beliefs, trade-union membership, genetic data, biometric data for the purposes of uniquely identifying a
398 natural person or data concerning health or sex life or sexual orientation.

399

400   **D. DEVIATING PURPOSES**

401

402 Service Providers commit not to process the Attributes for further purposes than enabling access, unless the
403 End User has given prior consent to the Service Provider. If the Service Provider wants to use the Attributes
404 for purposes other than "enabling access to the service" (see clause b. Purpose limitation), it can only do so
405 if the End User gives his or her consent to the Service Provider.

406 Examples of deviating purposes[1] are: including End User's e-mail address to a newsletter offering new
407 services, selling the Attributes to third parties, transferring information to third parties such as the search
408 history, profiling activities etc.

---

[1] Please, consult Article's 29 Working Party 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.

E. CONSENT

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

In the context of this Code of Conduct, when consent is required, it can be provided by a written statement, including by electronic means. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates the data subject's acceptance of the proposed processing of his or her personal data. Consent shall always be documented. Furthermore, the **End User** shall be able to withdraw his/her consent online.

In certain jurisdictions, employees cannot freely give their consent if the processing is required for performing their job. The same reasoning may apply with respect to students, as they cannot reasonably refuse the processing of their **Attributes**.

F. DATA RETENTION

The Service provider shall delete or anonymize all **Attributes** as soon as they are no longer necessary for the purposes of providing the service. Under the GDPR, anonymized data does not constitute personal data; therefore, anonymized data can be kept indefinitely.

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

The **Service Provider** has to decide a specific retention period for each category of personal data. This decision must be documented in its privacy policy (see clause j. Information duty towards End User).

For instance, the **Attributes** could be deleted after the expiration of the **End User's** session in the web service. On the other hand, for other services, it may be necessary to store the **Attributes** for a longer period of time.

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

It has to be taken into account that, in many cases, the **End User** does not explicitly inform the **Service Provider** that he has stopped using the services, he/she just does 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 he/she has not logged in for 18 months.

On the other hand, an **End User** not signing in does not necessarily mean that he/she no longer wishes to use the service. The **Service Provider** shall implement appropriate processes to manage this type of situations. For instance:

444
445
446

- if the service is an archive for scientific data, the researchers who deposit their datasets to the archive may still remain the owners or custodians of the dataset although they do not log in for a while.

447
448
449

- if the service is a Git (a widely used source code management system) an **End User** uses to publish their computer program code, the **End User** may still want to be able to log in and maintain their code, although they have not logged in for a while.

450
451
452

- if the service is a repository where researchers publish their scientific findings and contribution, the researchers still want to have their name and other **Attributes** attached to the finding, although they do not regularly log in.

453
454
455

- if the service is a collaborative application (such as, a wiki or a discussion board) where the **End User** has their name or other **Attribute** attached to their contribution to let the other users learn and assess the provenance of the contribution and attribute it to a specific person.

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

457
458

- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;

459
460

- for compliance with a legal obligation which requires processing by Union or Member State law to which the **Service Provider** is subject;

461

- for the performance of a task carried out in the public interest;

462

- for the establishment, exercise or defence of legal claims, such as resource allocation or invoices;

463

- for exercising the right of freedom of expression and information.

464

465 ## G. RESPECT THE END USER'S RIGHTS

466
467
468
The Service Provider shall respect End User's rights, including the right to access to personal data, the right to request correction of any inaccurate information relating to them and the right to request deletion of any irrelevant Personal Data the Service Provider holds about him or her.

469 ## H. TRANSFER OF PERSONAL DATA TO THIRD PARTIES

470
471
The Service Provider shall not transfer Attributes to any third party (such as a collaboration partner) except for:

472
473
474
475
476

a) a data processor, if mandated by the Service Provider for enabling access to its service on its behalf, or a data processor, in which case an ordinary controller-processor relationship applies between the Service Provider and the third party working on behalf of the Service Provider. The Service Provider must conclude a written agreement with such data processor in accordance with applicable laws.

477

478 b) a third party which is committed to the Code of Conduct. This is expected to be the case for
479   various collaborative research scenarios, where the service is provided to the **End User** by
480   several data controllers working in collaboration.

481   A typical scenario is a proxy setup where a research collaboration has a **Service Provider** that
482   receives **Attributes** from **Home Organisations** and passes on (parts of) those **Attributes** to
483   third parties providing the actual or additional services. In that case, the proxy **Service**
484   **Provider** must make sure all third parties receiving Attributes are committed to the Code of
485   Conduct or similar.

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

489   In a Service Provider proxy set-up, the organisation acting as the proxy (and operating the
490   proxy server) needs to assume a role as the intermediary between the **Home Organisation** and
491   the third party. For instance, the proxy needs to relay the suspected privacy or security breaches
492   to the **Home Organisation** or its Agent, as described in clause i. Security measures.

493 c) other third parties but only if prior consent has been given by the **End User** as described in
494   clause e. Consent

495

I. SECURITY MEASURES

497 The **Service Provider** warrants taking appropriate technical and organisational measures to safeguard
498 Attributes against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure
499 or access.

500 These measures shall ensure a level of security appropriate to the risks represented by the processing and
501 the nature of the data to be protected, having regard to the state of the art and the cost of their implementation.

502 The **Service Provider** shall implement the security measures described in Appendix 2: Information
503 Security, technical and organisational guidelines for Service Providers. The Service Provider can also
504 implement such additional security measures which, evaluated together, provide at least the same level of
505 security as the level of security provided by the measures described in Appendix 2.

J. INFORMATION DUTY TOWARDS END USER

507 The **Service Provider** shall provide -at first contact- the **End User** with a Privacy Policy.

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

509 The Privacy Policy shall contain at least the following information:

510   •   the name, address and jurisdiction of the **Service Provider**;

511   •   the contact details of the data protection officer, where applicable;

512   •   the purpose or purposes of the processing of the **Attributes**;

513   •   a description of the **Attributes** being processed as well as the legal basis for the
514   processing;

515   •   the third party recipients or categories of third party recipient to whom the Attributes
516   might be disclosed, and proposed transfers of **Attributes** to countries outside of the
517   European Economic Area;

518   •   the existence of the rights to access, rectify and delete the **Attributes** held about the
519   **End User**;

520   •   the retention period of the **Attributes**;

521   •   a reference to this Code of Conduct;

522   •   the right to lodge a complaint with a supervisory authority;

523 The Privacy Policy can be, for instance, linked to the front page of the service. It is important that the **End**
524 **User** can review the policy before they log in for the first time. The Privacy Policy shall use clear and plain
525 language.

526 The **Service Provider** may include additional information, but must include as a minimum the information
527 described above. The additional information could for example refer to the additional data processing
528 activities of the **Service Provider**.

529 The Service Providers are advised to make use of the Privacy Policy template that belongs to the supporting
530 material of the Code of Conduct in Appendix 1: Information duty towards End Users.

531

532   **K. INFORMATION DUTY TOWARDS HOME ORGANISATION**

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

535   a)   a machine-readable link to the Privacy Policy;
536   b)   indication of commitment to this Code of Conduct;
537   c)   any relevant updates or changes in the local data protection legislation that may affect this
538   Code of Conduct.

539 GÉANT has put in place a scalable technical solution allowing Service Providers to add their adherence to
540 this Code of Conduct and to communicate its privacy policy's URL. This information is shared with the
541 Home Organisation's Identity Provider server prior to sharing the End User's Attributes to the Service
542 Provider.

543 The current technical infrastructure is based on standard SAML 2.0 metadata management and distribution
544 system operated by Federation operators. However, the technical infrastructure may evolve over time.

545

546 L. SECURITY BREACHES

547 The **Service Provider** commits to, without undue delay, report all suspected privacy or security breaches
548 (including unauthorized disclosure or compromise, actual or possible loss of data, documents or any device,
549 etc.) concerning the **Attributes** to the **Home Organisation** or its Agent and, where this is legally required,
550 to the competent data protection authority and/or to the **End Users** whose data are concerned by the security
551 or privacy breach.

552 The **Home Organisations** or their **Agents** shall be informed without undue delay about any security
553 breaches relating to the **Attributes** they released to the **Service Providers**, to allow them taking the
554 necessary technical and organisational measures for mitigating any risk the **Home Organisation** may be
555 exposed to.

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

560 Regarding the contact point in the event of a security breach, the current technical infrastructure delivers
561 the contact point of the **Home Organisation** or its Agent to the **Service Provider**. The **Service Provider**
562 can use the contact point for reporting any suspected privacy or security breaches concerning the **Attributes**
563 to the **Home Organisation** or its Agent.

564

565 M. LIABILITY

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

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

572 For example, in case an **End User** files a complaint against his or her **Home Organisation** for unlawful
573 release of **Attributes**, and it turns out that a **Service Provider** has released the **Attributes** to a third party,
574 the **Home Organisation** will be held harmless against the **End User** by the **Service Provider** if it can
575 prove the **Service Provider** has not complied with all the obligations of this Code of Conduct.

576

577 N. TRANSFER TO THIRD COUNTRIES

578   1. Transfers among Service Providers that have adhered to the Code of Conduct.

579 This Code of Conduct constitutes an adequate legal basis for cross-border transfers of Attributes among the
580 Service Providers that have adhered to it, whether the Service Provider receiving the Attributes is
581 established in the European Economic Area or not.

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

583 The **Service Provider** guarantees that, when transferring **Attributes** to a party that has not adhered to this
584 Code of Conduct and that is based outside the European Economic Area or in a country without an adequate
585 level of data protection pursuant to Article 25.6 of the directive 95/46/EC or Article 45.1 of the GDPR, to
586 take appropriate measures

587 Under European data protection legislation, transfers of personal data from the European Economic Area
588 to third countries that do not offer an adequate level of data protection are restricted, unless the recipient
589 territory ensures a so-called *"adequate level of protection"*. However, there is an exhaustive list of
590 derogations to this general prohibition that are relevant for this context:

591   ▪   **Consent of the End User**: The unambiguous consent of the data subject legitimates data transfers to
592   third countries, even if the recipient does not offer an adequate level of protection. The Service
593   Provider may rely on the End User's freely given informed revocable Consent as described in clause
594   e. Consent.

595   ▪   **Contractual guarantees**: The existence of an appropriate contractual framework, supported by
596   Standard contract clauses, either adopted by the European Commission or by a supervisory authority,
597   the use of appropriate safeguards such as Binding Corporate Rules or other legally binding and
598   enforceable instruments are recognised methods of transferring personal data. The use of Standard
599   contract clauses does not exclude the possibility for the contracting parties to include them in a wider
600   contract nor to add other clauses as long as they do not enter in contradiction. When using EU model
601   clauses, the Service Provider needs to verify and ascertain that the other party is able to comply with
602   all contractual obligations set out in the model clauses, especially taking into account local law
603   applicable to such party.

604

605   O. GOVERNING LAW AND JURISDICTION

606

607 This Code of Conduct shall be interpreted in the light of the GDPR and of the guidance issued by the
608 European advisory body on data protection and privacy[2].

---

[2] 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.

609 This Code of Conduct shall be governed by the national laws of the country in which the **Service Provider**
610 is established.

611 Alternatively, the **Service Provider** and the **Home Organisation** can refer to this Code of Conduct in the
612 case where the **Service Provider** processed personal data on behalf of the **Home Organisation**. In that
613 scenario, the applicable law is the one of the **Home Organisation.**

614 Any disputes regarding the validity, the interpretation or the implementation of this Code of Conduct shall
615 be settled before the competent courts of the country in which the **Service Provider** is established.

616 International Private Law shall apply in order to confirm the applicable law and to determine whether a
617 **Service Provider** is established in a country or not.

618 The Privacy Policy requires specifying the jurisdiction and the applicable law (clause j. Information duty
619 towards End User).

620

P. ELIGIBILITY

622 The Service Provider must be implemented and executed by a duly authorized representative of the **Service
623 Provider**.

624 Each **Service Provider** must make sure that this Code of Conduct is executed by a person or by several
625 persons who has or have the right to commit the **Service Provider** to this Code of Conduct.

626 The person administering the service that receives **Attributes** must identify the person or body in his or her
627 organisation that can decide if the **Home Organisation** commits to this Code of Conduct, as typically, the
628 service administrator cannot take this decision on his own.

629

Q. TERMINATION OF THE CODE OF CONDUCT

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

632 • this Code of Conduct being replaced by a similar arrangement or

633 • the termination of the service provisioning to the Home Organisation.

634 Even after the **Service Provider** has terminated its adherence to the Code of Conduct, the Attributes
635 received continue to be protected by the GDPR.

636

R. SURVIVAL OF THE CLAUSES

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

640

S. PRECEDENCE

642

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** and the **Home Organisation**, the provision of the agreement concluded between **Service Provider** and **Home Organisation** takes precedence over the provision of this Code of Conduct.

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

This section allows the **Service Provider** to have a bilateral agreement overriding the Code of Conduct with some **Home Organisations**, meanwhile, this Code of Conduct will still applies to the other **Home Organisations** that have not entered in a bilateral agreement.

652

653

APPENDIX 1: INFORMATION DUTY TOWARDS END USERS

655   This annex consists of two parts:

656   I.   How to develop a privacy policy.

657   Although this is a mandatory obligation, practice has shown that many **Service Providers** have
658   problems in developing an appropriate privacy policy for the services they provide. A practical
659   template is provided to assist the **Service Providers**.

660   II.   How the **Home Organisation** should inform the **End User** on the **Attribute release**.

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

663

664

665

666

HOW TO DEVELOP A PRIVACY POLICY

668 To understand the interplay of the **Home Organisation** and the **Service Provider** within the frame of the
669 Code of Conduct, it is necessary to know that the Identity federations (and possible interfederation services
670 like eduGAIN) relay the following information (called SAML2 metadata) from the **Service Provider** server
671 to the Identity Provider server managed by the Home Organisation:

672 ● a link to **Service Provider's** privacy policy web page (an XML element with the name
673 mdui:PrivacyStatementURL) which must be available at least in English.
674 ● the Service Provider's name and description (mdui:DisplayName and mdui:Description) at least in
675 English. The name and description are expected to be meaningful also to the end users not affiliated
676 with the service.
677 ● optionally, the **Service Provider's** logo (mdui:logo) that can facilitate the user interface.
678 ● the list of **Attributes** that the **Service Provider** requests from the **Home Organisation** and, for
679 each Attribute, an indication that the Attribute is required. As the legal grounds for the attribute
680 release (Article 7 of the data protection directive and Article 6.1 of the GDPR), the **Home**
681 **Organisations** are suggested to use the legitimate interests legal grounds.

PRIVACY POLICY TEMPLATE

683 This template intends to assist **Service Providers** in developing a Privacy Policy document that fulfills the
684 requirements of the GDPR and the Code of Conduct. The second column presents some examples (in italic)
685 and proposes some issues that should be to taken into account.

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

690

Name of the service	SHOULD be the same as mdui:DisplayName *WebLicht*
Description of the service	SHOULD be the same as mdui:Description *WebLicht is a service for language research. It provides an execution environment for automatic annotation of text corpora.*

Data controller and a contact person	*Tübingen university, Institute for language research* *Laboratory manager Bob Smith, bob.smith@example.org*
Data controller's data protection officer, if applicable	If the controller has a data protection officer (GDPR Section 4) *Chief Security Officer bill.smith@example.org*
Jurisdiction and supervisory authority	The country in which the Service Provider is established and whose laws are applied. SHOULD be an ISO 3166 code followed by the name of the country and its subdivision if necessary for qualifying the jurisdiction. *DE-BW Germany Baden-Württemberg* How to lodge a complaint to the competent Data protection authority: *Instructions to lodge a complaint are available at ...*
Personal data processed and the legal basis	*A. Personal data retrieved from your Home Organisation:* *- your unique user identifier (SAML persistent identifier) ** *- your role in your Home Organisation (eduPersonAffiliation attribute) ** *- your name ** *B.Personal data gathered from yourself:* *- logfiles on the service activity ** *- your profile* *...* ** = the personal data is necessary for providing the service. 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'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).
Third parties to whom personal data is disclosed	Notice clause f of the Code of Conduct for Service Providers.
	Are the 3rd parties outside EU/EEA or the countries or international organisations whose data protection EC has decided to be adequate? If yes, references to the appropriate or suitable safeguards.
How to access, rectify and delete the personal data and object its processing.	*Contact the contact person above.* *To rectify the data released by your Home Organisation, contact your Home Organisation's IT helpdesk.*
Withdrawal of consent	If personal data is processed on user consent, how he/she can withdraw it?
Data portability	Can the user request his/her data be ported to another service? How?
Data retention	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. *Personal data is deleted on request of the user or if the user hasn't used the service for 18 months.*
Data Protection Code of Conduct	*Your personal data will be protected according to the Code of Conduct for Service Providers, a common standard for the research and higher education sector to protect your privacy.*

691

HOW THE HOME ORGANISATION SHOULD INFORM THE END USER ON THE ATTRIBUTE RELEASE

The Data protection laws create a set of requirements for the INFORM interactions with the user. This Data protection Code of Conduct proposes a division of responsibility where the INFORM interaction is carried out by the **Home Organisation** of the user, for instance, in an INFORM Graphical User Interface (GUI) installed to the Identity Provider server.

However, the Data protection regulators and the groups developing and enforcing these regulations recognize that there is a balance between full disclosure to meet the requirements and usability. A poor design of the user interaction screens can actually reduce the likelihood that users will understand what is happening.

LAW REQUIREMENTS

INFORMING THE END USER ("INFORM INTERACTION")

For a **Home Organisation**, informing the end user can be done when a new end user gets his/her account at the institution. At that time, the **Home Organisation** has the first opportunity to inform that the user's **Attributes** may also need to be released to a **Service Provider** when he/she wants to access it. However, the law requires that, additionally, the end user needs to be informed about the specific **Attribute** release every time his/her **Attributes** are to be released to a new **Service Provider**.

The **Service Provider's** obligation to inform the end user depends on if it is a data processor or a controller. As a data controller, the **Service Provider** is responsible for communicating with the End user the issues above; which **Attributes** it will be using, and what it will be doing with them. As a data processor, a **Service Provider** can refer to the **Home Organisation**.

The Article 29 Working Party, EU advisory body contributing to the uniform application of the Data protection directive, took the view that the information must be given directly to individuals - it is not enough for information to be "available[3]".In the Internet, a standard practice to inform the end user on processing his/her personal data in services is to provide him/her a Privacy Policy web page in the service.

In the Web Single Sign-On scenario of SAML 2.0, a convenient place to inform the end user is at the Home Organisation before the Attribute release takes place for the first time. Several federations supporting the European higher education and research communities have already developed tools implementing this approach (e.g. the uApprove module implemented for Shibboleth, the consent module implemented for SimpleSAMLphp). This allows the user's decision to directly affect the transfer of **Attributes** to the **Service**

---

[3] Opinion 15/2011 on the definition of consent, p.20.

723 **Providers**; if the **Service Providers** were communicating with the user it might have already received all
724 the **Attributes** and values.

725

726 GENERAL PRINCIPLES FOR INFORMING THE USER

727 Information dialogues should be short and concise.

728 The UK information commissioner proposes a "layered approach"[5], the basic information should appear on
729 the main page, and a hyperlink shall be provided for detail. Merely having a clickable link labelled "privacy
730 policy here" probably wouldn't be enough.

731 The goal is to provide a human readable form as the primary interface with the ability to click further to see
732 what the 'technical' data is. The Acceptable Usage Policies presented by most Internet services do not
733 suffice as they are rarely read nor understood by the users. The basic information should be provided as
734 short accurate "user-friendly" descriptions; detailed information about "exactly what's going on" can be
735 provided as a link.

736 Consequently, this profile recommends displaying the **Service Provider's** name, description, logo and
737 requested attributes on the main page. If a user wants to learn more, he/she can click a link resolving to the
738 **Service Provider's** Privacy policy. It is possible that users will actually not do the latter, but at least they
739 have the ability to inform themselves of what is going on.

740 Layered notices can be particularly useful when describing the attribute values which will be released. In
741 general, LDAP-style attributes are transferred to the SP. However, very few users have any familiarity with
742 the conventions and usage of LDAP attributes. Instead, the Identity Provider could ask the user to release
743 "name"; the link would take the user to a page listing all of the LDAP name attributes and values.

744 There are other attributes where the values are intentionally opaque (e.g.
745 ePE="urn:mace:rediris.es:entitlement:wiki:tfemc2"). It is NOT reasonable to expect the end user to
746 understand what this value means and to pick up a particular value to be released. Instead, natural language
747 descriptions of the values should be provided.

748 A good way to explain to a user why there is a transfer of information is "your email, name and affiliation
749 will be transferred". Explaining by analogy is human, albeit not necessarily academic in all disciplines.

750

---

[5] *"A layered notice usually consists of a short notice plus a longer notice. The short notice contains basic
information, such as the identity of the organisation and the way in which the personal information will be used...
The short notice contains a link to a second, longer notice which provides much more detailed information."* (the
UK information commissioner's Privacy Notices Code of Practice, page 18).

RECOMMENDATIONS

For all Attributes (INFORM interaction):

1. The user MUST be informed on the attribute release separately for each SP.

2. The user MUST be presented with the mdui:DisplayName value for the SP, if it is available.

3. The user MUST be presented with the mdui:Description value for the SP, if it is available.

4. The user SHOULD be presented with the mdui:Logo image for the SP, if it is available.

5. The user MUST be provided with access (e.g. a clickable link) to the document referenced by the mdui:PrivacyStatementURL.

6. The IDP MUST present a list of the RequestedAttributes defined as NECESSARY. No user consent is expected before release. (However, given how web browsers work, the user may have to click a CONTINUE button in order to continue in the sequence.)

   The IDP MAY list the NECESSARY attributes on the same screen as the username/password entry boxes, making clear that *if* you login then this is what will happen. It MUST be clear to the user that the consequence of their next action will be to release the   attributes.
   NOTE -- the attribute values for the specific user are not available when the login screen is presented, since the user's identity is not yet known.

7. The display software SHOULD provide the ability to configure and display localised descriptions of the attributes (e.g. what PersistentID means) and their values (e.g. what eduPersonEntitlement="urn:mace:rediris.es:entitlement:wiki:tfemc2" means)

8. The display software MAY inform the user of the release of an "attribute group" (eg attributes expressing the user's "name"), and then release all requested attributes in the group (e.g. various forms of the user's name such as cn, sn, givenName and displayName).

9. The display software MAY give the user the option to remember that they have been INFORMed of the release of the necessary attributes.

10. If any of the following has changed since the user accessed this SP for the last time, the user MUST be prompted again for the INFORM interaction

   a. the list of attributes the SP requests
   b. the DisplayName of the SP
   c. the Description of the SP

783   INTERNATIONALIZATION

784   The *lang* attribute of the *mdui* elements can be used to match the user's preferred language settings.

785   SAMPLE NOTIFICATION

786

787   Example of how a **Home Organisation** should inform **End Users** and provide an opt-out opportunity
788   before **Attributes** are released to a new **Service Provider**. Clicking the **Service's Provider** name leads to
789   its Privacy policy page.

790

791

792

793

794

795

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

798

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

804

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

NORMATIVE ASSERTIONS

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

813

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

816

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

1 OPERATIONAL SECURITY [OS]

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

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

- [OS2] A process is used to manage vulnerabilities in software operated by the organisation.

826 • [OS3] Mechanisms are deployed to detect possible intrusions and protect information systems from
827   significant and immediate threats

828 • [OS4] A user's access rights can be suspended, modified or terminated in a timely manner.

829 • [OS5] Users and Service Owners (as defined by ITIL [ITIL]) within the organisation can be
830   contacted.

831 • [OS6] A security incident response capability exists within the organisation with sufficient
832   authority to mitigate, contain the spread of, and remediate the effects of a security incident.

2 INCIDENT RESPONSE [IR]

834 Assertion [OS6] above posits that a security incident response capability exists within the organisation.
835 This section's assertions describe its interactions with other organisations participating in the Sirtfi trust
836 framework.

837 • [IR1] Provide security incident response contact information as may be requested by an R&E
838   federation to which your organization belongs.

839 • [IR2] Respond to requests for assistance with a security incident from other organisations
840   participating in the Sirtfi trust framework in a timely manner.

841 • [IR3] Be able and willing to collaborate in the management of a security incident with affected
842   organisations that participate in the Sirtfi trust framework.

843 • [IR4] Follow security incident response procedures established for the organisation.

844 • [IR5] Respect user privacy as determined by the organisations policies or legal counsel.

845 • [IR6] Respect and use the Traffic Light Protocol [TLP] information disclosure policy.

3 TRACEABILITY [TR]

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

850 • [TR1] Relevant system generated information, including accurate timestamps and identifiers of
851   system components and actors, are retained and available for use in security incident response
852   procedures.

853 • [TR2] Information attested to in [TR1] is retained in conformance with the organisation's security
854   incident response policy or practices.

4 PARTICIPANT RESPONSIBILITIES [PR]

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

857   •   [PR1] The participant has an Acceptable Use Policy (AUP).

858   •   [PR2] There is a process to ensure that all users are aware of and accept the requirement to abide
859   by the AUP, for example during a registration or renewal process.

860

REFERENCES

861

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

863   [SIRTFI] A Security Incident Response Trust Framework for Federated Identity, version 1.0:
864   https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf

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

866

867

868

869

APPENDIX 3: HANDLING NON-COMPLIANCE OF SERVICE PROVIDERS

870

INTRODUCTION

871

872

873 This appendix describes examples of situations of non-compliance to the GÉANT Data Protection Code of
874 Conduct. As a result, actions can be raised and monitoring bodies can intervene.

875 This Data protection Code of Conduct relies on the following principles:
876

877 • The **Home Federation** that has registered a **Service Provider** records a technical indication
878 (currently, using a tag embedded to SAML 2.0 metadata) on the **Service Provider's** adherence to
879 the Code of Conduct. The indication signals that the **Service Provider** believes that its service is
880 being operated in a manner that is consistent with the Code of Conduct.
881

882 • The technical infrastructure (currently, SAML 2.0 metadata exchange service) that the federation(s)
883 provides delivers the indications from Service Providers to **Home Organisations'** Identity
884 Provider servers.
885

886 • Reminding the **Service Provider** of a potential (suspected) non-compliance issue does not imply
887 to make the reminding party sharing any legal responsibility with the **Service Provider**.
888

EXAMPLES OF SP NON-COMPLIANCE

889

890

891 The **Service Provider** can violate the Code of Conduct in several ways, such as:
892

893 • requesting Attributes which are not relevant for the service (c.f. clause b. Purpose limitation);
894 • processing the Attributes for an undefined period of time (c.f. clause f. Data retention);
895 • processing the Attributes for a deviating purpose or transferring them to a third party in a way that
896 violates clause b. Purpose limitation and d. Deviating purposes of the Code of Conduct (for
897 instance, transferring the **Attributes** to a company for commercial purposes without user consent);
898 • Disclosing the **Attributes** (c.f. clause d. Deviating purposes);
899 • Omitting to install security patches (c.f. clause i. Security measures and Appendix 2: Information
900 Security, technical and organisational guidelines for Service Providers);
901 • Omitting to publish a privacy policy or publish an insufficient privacy policy (c.f. clause Appendix
902 1: Information duty towards End Users).
903

904 If anyone (such as an end user, a **Home Organisation** or a Federation Operator) suspects that a **Service**
905 **Provider** is not complying with the Code of Conduct to which it has committed, the following alternative,
906 mutually non-exclusive, actions are suggested:
907

908 1. Contact the Service Provider directly (with a copy to the **Service Provider's** Home Federation),
909 describing the suspected problem, and ask the **Service Provider** to check if it has a compliance
910 problem and correct it,

911   2. Contact the Service Provider's Home Federation, and request to contact the **Service Provider** and
912   to check if there is a compliance problem and request to correct it. Depending on the Home
913   Federation's policy, there may be also additional measures available for handling non-compliance.
914

915   3. Contact the body accredited to monitor compliance with the Code of Conduct, if applicable, as
916   defined in the Article 41 of the GDPR and below;
917

918   4. Determine the location of the legal entity operating the **Service Provider**, and lodge a complaint
919   with the competent Supervisory authority (as defined in Articles 57 and 58 of the GDPR).
920

921 CODE OF CONDUCT MONITORING BODY

922

923 A Federation operator can nominate a body to monitor the **Service Providers'** compliance with the Code
924 of Conduct. The monitoring body must be accredited by a competent supervisory authority.

925

926 Only the monitoring body nominated by the Home Federation of the **Service Provider** is competent to
927 assess the compliance of the **Service Provider** with the Code of Conduct.

928

929 The monitoring body publishes its contact details and procedures in a public and accessible way.

930

931 The monitoring body is responsible for processing complaints received from end users, Home
932 Organisations, Federation Operators or other parties.

933

934 Having received a complaint the monitoring body will:

935

936   I. ask the **Service Provider** to present its counterpart,
937   II. give the **Service Provider** at most four weeks' time to revise the issue if the
938   monitoring body finds the **Service Provider** to be non-compliant with the Code of
939   Conduct
940   III. mandate the Home Federation to remove the **Service Provider's** tag if the Service
941   Provider hasn't fixed the non-compliance issue within the given timeframe.

942 The **Service Provider** whose tag has been removed can reclaim the tag only after demonstrating to the
943 monitoring body that it has returned to compliance.