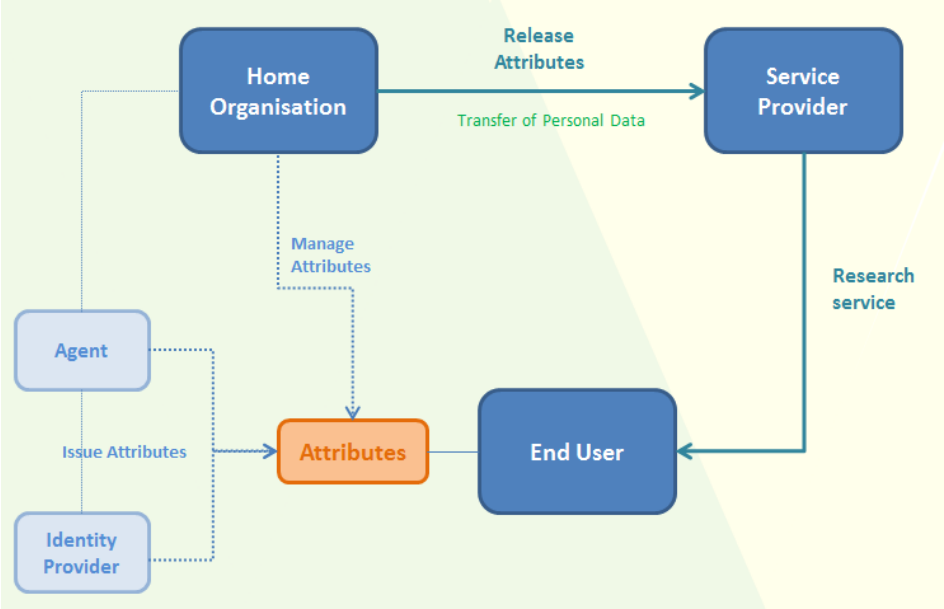
DLA PIPER
MEMORANDUM

TO	:	Valter Nordh, Mikael Linden, Josh Howlet (Géant)
FROM	:	Patrick Van Eecke (DLA Piper)
DATE	:	14 April 2014
SUBJECT	:	Code of Conduct for non-EEA Service Providers

1. OUR UNDERSTANDING OF THE CONTEXT

GÉANT, a pan-European research and education network, interconnects Europe's national research and education networks, connecting over 50 million users at over 10,000 institutions across Europe. So as to streamline the users' access to certain services, GÉANT has implemented federated identity management, as pictured in the figure below.



Since Attributes constitute Personal Data, and the processing thereof is as such subject to European data protection laws, GÉANT has established the GÉANT Data Protection Code of Conduct ("Code of Conduct"). The Code of Conduct designs an approach to meet the requirements set by the Data Protection Directive[1] in the context of federated identity management. It defines behavioral rules for Service Providers which want to receive End User Attributes from the Identity Provider servers, typically managed by the Home Organisations. The purpose of the Code of Conduct is to increase Home Organisations' willingness to release Attributes to the Service Providers who declare that they conform to the Code of Conduct.

GÉANT now wishes to extend its network to Service Providers established outside the European Economic Area (EEA). Releasing Attributes to such non-EEA Service Providers will constitute a transfer of Personal Data, which is subject to specific requirements under the EU Data Protection Directive.

[1] 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, O.J. L 281 , 23 November 1995, 31.

GÉANT wishes to understand how such release of Attributes to non-EEA Service Providers can occur in accordance with the EU Data Protection Directive, and which changes should be made to the Code of Conduct to reflect such release of Attributes to non-EEA Service Providers.

2. ANALYSIS OF SOLUTIONS FOR TRANSFER REQUIREMENTS

2.1 European data protection legislation

2.1.1 Revision of the current legal framework

The processing of personal data is regulated by the EU Data Protection Directive, as implemented into the national law of each EU Member State. The Data Protection Directive provides a regulatory framework for all aspects of personal data processing, including a.o. material requirements (e.g. the principle that any processing must be fair and lawful), formal requirements (e.g. information obligations and notification obligations) and specific requirements for transferring personal data to countries outside of the European Economic Area.

The Data Protection Directive dates from 1995. Technological progress and growth as well as globalisation have significantly changed the way personal data is collected, accessed and processed since then. Furthermore, the current European legal framework regarding data protection is regulated by a Directive, which results in diverging national interpretations as well as different local enforcement of the provisions.

The technical developments as well as the diverging national implementations have resulted in the European legislators reconsidering the current data protection framework in Europe. A first step towards a new legal framework was taken when the European Commission presented its draft proposal to a new Data Protection Regulation on January 25, 2012.

In the meantime, the draft Regulation has been voted on by the European Parliament (March 2014). Next steps in the legislative process include trialogue discussions between the European Parliament, Council and European Commission. The Council is expected to confirm and issue its position in 2015. This would mark the end of the first reading, and it is expected that a second reading will take place.

The current expectation is that the Regulation will formally enter into force in end of 2015 - beginning of 2016, after which a two-year transitional period will apply, which implies that companies and organisations are likely to be required to comply with the Regulations as from end of 2018.

2.1.2 Data transfers under the current and future legal framework

The draft Regulation further elaborates and fine-tunes the data transfer principles currently set out in the Data Protection Directive. The main underlying principles, however, remain the same.

Whereas it is expected that organisations will not have to comply with the new laws for another few years, it is important to note that in the meantime, organisations must of course comply with the current regulatory framework. Indeed, failure to comply can lead to application of a variety of sanctions, ranging from administrative sanctions to criminal sanctions including fines.

Furthermore, specifically with respect to data transfers outside the European Economic Area, it is important to note that EU data protection authorities have become increasingly following several (highly publicised) data breach and transfer scandals in the past few months.

Accordingly, it is recommended for organisations to promptly take all such steps as are required to comply with the current rules on data transfers as set out in the Data Protection Directive.

2.2 Transfer restrictions Data Protection Directive

2.2.1 Adequate protection

As a general principle, the Data Protection Directive only allows transfers of personal data to third countries (outside the European Economic Area) ensuring an adequate level of protection:

> *"The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer **may take place only if**, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, **the third country in question ensures an adequate level of protection**.*
>
> *The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country. (…)"*[2]

Pursuant to article 25.6 of the Data Protection Directive, the European Commission has the power to determine whether a third country ensures such adequate level of protection. The European Commission has so far recognised the following **countries as providing adequate protection:** Andorra, Argentina, Australia, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, New Zealand, Eastern Republic of Uruguay and (only in specific circumstances) the United States. It should be noted that some of the adequacy decisions only apply to specific types of data and/or are subject to specific requirements. For example, the Australian adequacy decision only relates to PNR data.

Another important example is the US **Safe Harbor** framework. The European Commission recognises that US established organisations adhering to the Safe Harbor framework offer adequate protection[3]. The decision to join the Safe Harbor scheme is voluntary. Organisations that decide to participate must comply with the Safe Harbor framework's requirements and publicly declare that they do so. To qualify for the Safe Harbor program, an organisation can join a self-regulatory privacy program that adheres to the framework's requirements or develop its own self-regulatory privacy policy that conforms to the framework.

It should be noted, however, that in order to be able to sign up to the Safe Harbor framework, an organisation must be subject to the statutory powers of the Federal Trade Commission or the US Department of Transportation.

Furthermore, it should be noted that the Safe Harbor scheme is currently heavily criticised by EU data protection authorities and other competent bodies. In a recent Resolution (dated March 2014), the European Parliament called for an immediate suspension of the Safe Harbor framework, alleging that it does not adequately protect European citizens. It remains to be seen if the European Commission (which entered into the agreements regarding Safe Harbor) will follow the opinion of the European Parliament or will maintain the possibility for organisations to transfer to the US on the basis of the Safe Harbor certification of the recipient.

2.2.2 Listed exceptions

As an exception to the foregoing, the Data Protection Directive allows for personal data transfers to third countries in certain exceptional cases, which are exhaustively listed in the Directive[5]:

1. the data subject has given her **consent** unambiguously to the proposed transfer;

2. the transfer is necessary for the performance of a **contract between the data subject and the controller** or the implementation of pre-contractual measures taken in response to the data subject's request;

3. the transfer is necessary for the conclusion or performance of **a contract concluded in the interest of the data subject** between the controller and a third party;

4. the transfer is necessary or legally required on important **public interest** grounds, or for the establishment, exercise or defence of **legal claims**;

---

[2] Article 25.1-2 Data Protection Directive.

[3] export.gov/safeharbor/eu/eg_main_018493.asp

[5] Article 26.1 Data Protection Directive.

5. the transfer is necessary in order to protect the **vital interests** of the data subject;

6. the transfer is made from a **register** which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2.2.3 Adducing additional safeguards

Additionally, the Data Protection Directive provides for a second exception to the general principle: Personal data may be transferred to third countries which do not ensure an adequate level of protection, where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights. such safeguards may in particular result from appropriate **contractual clauses**[6].

Article 26.4 of the Data Protection Directive, empowers the European Commission to adopt **standard contractual clauses** that offer such sufficient safeguards. By incorporating the standard contractual clauses into a contract, personal data can flow from an EEA data controller to a non-EEA recipient. The European Commission has issued standard contractual clauses for both transfers to controllers and transfers to processors[7].

Realising the need for organisations to have a global approach to data protection, the Article 29 Working Party8 has also authorised organisations to adopt binding internal rules, the so-called binding corporate rules ("BCR"), intended to regulate the transfers of personal data that are originally processed by the organisation as controller within the same organisation. The Working Party recently also adopted a framework for BCR for processors[9]. Personal data can be freely transferred within an organisation which has adopted BCR.

DRAFT

[6] Article 26 Data Protection Directive.

[7] The standard contractual clauses are available via ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm

[8] The Working Party was set up under article 29 of the Data Protection Directive. It is an independent European advisory body on data protection and privacy.

[9] BCR documentation is available via ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

3. ASSESSMENT OF LEGALLY COMPLIANT SCENARIO'S FOR RELEASE OF ATTRIBUTES TO NON-EEA SERVICE PROVIDERS

3.1 Assessment of legally compliant scenario's

The table below sets out a high level "pro/con" assessment of each of the legal bases, in relation to the release of Attributes by EEA Home Organisations to non-EEA Service Providers[10]:

LEGAL BASIS	PRO	CON
Adequate protection - general	• No formalities or other actions to be undertaken by the Home Organisations before Attributes can be released.	• Only a limited list of countries are considered to offer adequate protection. • Not all white-listed countries are deemed to offer adequate protection for all types of personal data. • This legal basis does not offer a comprehensive solution that allows worldwide release of Attributes.
Adequate protection - Safe Harbor	• No formalities or other actions to be undertaken by the Home Organisations before Attributes can be released to recipients adhering to the Safe Harbor framework.	• Each Service Provider must self-certify or join a program which adheres to the Safe Harbor framework (and re-affirm certification annually), which may be too high a barrier for Service Providers. • Limited cost for Service Providers. • Provides a comprehensive solution for US Service Providers only. • Only organisations which are subject to the statutory powers of the US Department of Transportation or the Federal Trade Commission can adhere to the Safe Harbor Framework. Each Service Provider would need to verify if and to which extent they are able to obtain Safe Harbor certification. It is our understanding that generally speaking, universities would not fall within these categories. • The Safe Harbor framework has been criticised lately by EU data protection authorities[11] and the European

[10] Please note that our assessment is based on controller-to-controller personal data transfers. Also, please note that our assessment focuses on data transfer issues only, and does not cover general requirements such as registrations with the DPA.

[11] See e.g. the Dutch data protection authority in its 2012 opinion regarding US cloud services: www.cbpweb.nl/downloads_med/med_20120910-zienswijze-toepassing-wbp-SURFmarket-cloud-computing.pdf

		Parliament[12]. The question arises whether the European Commission will reverse its recognition of Safe Harbor as providing adequate protection.
Exception - Consent	• Low cost. • No formalities or other actions to be undertaken by the Service Providers. • Consent can rather easily be obtained by the Identity Provider or Agent on the Home Organisations' behalf, with limited administrative burden for the Home Organisations.	• Any consent must be a freely given specific and informed indication of wishes of the data subject. It should be noted that EU data protection authorities sometimes consider that consent cannot be "freely" given in case the data subject is in a dependency relationship with the data controller (e.g. employee vs. employer). • Furthermore, consent is revocable, which entails (i) the need for a consent management system keeping track of all consents (and lack thereof, if applicable); and (ii) that consent as a legal basis is not entirely future-proof. • The list of Service Providers joining GÉANT will change over time, which may make it difficult for End Users to give "informed" consent.
Exception - Performance of contract with End User	• Low cost. • No formalities or other actions to be undertaken by the Service Providers.	• We assume that Home Organisations do not always have a contract with End Users, which implies this legal basis cannot offer a comprehensive, global solution. • This would require all contracts between Home Organisations and End Users to contain explicit clauses regarding GÉANT, that would allow the Home Organisation to argue that release of Attributes to non-EEA Service Providers is *necessary* for the performance of the contract.
Exception - Performance of contract concluded in the interest of the End User	• Not applicable. Given that the exceptions in the Data Protection Directive must be restrictively interpreted, we consider a judge or data protection authority may not always accept the argument that contracts between Home Organisations and Service Providers (if any) are concluded in the interest of the End User - at least not for data protection purposes.	
Exception - Public interest / legal claims	• Not applicable.	
Exception - End User vital interests	• Not applicable.	
Exception - Public register	• Not applicable.	
Additional safeguard - contractual clauses	• Allows for a tailor-made solution for GÉANT. • Can be structured so as to limit the administrative burden for both Home Organisations and Service	• (Non-standard) contractual clauses will in most jurisdictions require approval from the data protection authority, which may be too high a barrier for Home

[12] www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A7-2014-0139&language=EN

	Providers.	Organisations. • Local data protection authorities may require different clauses to be included, which may make it difficult to create a harmonised document which can be used by Home Organisations in all countries.
Additional safeguards - standard contractual clauses	• Low cost and low barrier. • Limited administrative burden. • Standard approach across all EEA countries, as the standard contractual clauses were issued on a European level by the European Commission. • Comprehensive solution for all transfers.	• Use of standard contractual clauses may still require notification to / approval by the data protection authorities in some countries.
Additional safeguards - BCR	• Not applicable.	

DRAFT

3.2 Standard contractual clauses - charter approach

So as to achieve a low cost, low barrier pragmatic mechanism that allows for release of Attributes by Home Organisations in all EEA countries, we consider that the **standard contractual clauses would provide GÉANT with the best solution**. Standard contractual clauses are a well-known and widely used catch-all approach, which can provide a legal basis for data transfers for longer periods of time.

For controller-to-controller transfers, the European Commission has issued two different sets of standard clauses, in 2001 and 2004. The 2004 version was originally drafted by a coalition of business associations (including the International Chamber of Commerce) and is generally perceived as more business friendly.

In principle, a data transfer agreement based on the standard contractual clauses needs to be concluded between each data exporter (Home Organisation) and data importer (Service Provider). However, as this would be practically burdensome and impractical, we propose to use a **"charter"-approach**, whereby the standard contractual clauses are embedded in a charter (code of conduct), to which all Home Organisations and Service Providers can adhere. In each case where Attributes are released by a Home Organisation, the Home Organisation will act as (and comply with the obligations of) data exporter, and the receiving Service Provider will act as (and comply with the obligations of) data importer.

The standard contractual clauses provide for a signature section at the end, indicating that both data exporter and data importer should sign the clauses. From a contractual perspective, the contractual clauses are governed by the national laws of the country of the data exporter. Accordingly, any validity and/or proof requirements relating to signature of the contract will need to be assessed from a local law perspective. It is therefore typically recommended to maintain the most stringent approach in a multi-country context, i.e. handwritten signature or use of an electronic signature which is equivalent to a handwritten signature (e.g. qualified advanced electronic signature).

Based on our experience with similar projects, we know that such charter approach is generally accepted in most EU jurisdictions. However, as also indicated above, in some jurisdictions, **notification to or approval** by data protection authorities may be required. This will need to be analysed on a case-by-case basis in each jurisdiction. In most jurisdictions which apply a notification or approval procedure, one such procedure will need to be followed by each EU data controller (i.e. each EU Home Organisation). In several of these countries, this procedure will be part of, or overlap, with the general notification obligation of data controllers towards data protection authorities.

Section 4 below sets out a draft charter (code of conduct) for non-EEA Service Providers, which is based on the 2004 standard contractual clauses for data transfers to controllers, and the existing Code of Conduct (v1.0 dd. 14 June 2013). As the Home Organisations, as data exporters, also need to comply with the standard contractual clauses, we note that not only the Service Providers but also the Home Organisations will need to adhere to the charter (code of conduct).

4. CODE OF CONDUCT FOR NON-EEA SERVICE PROVIDERS

See next pages.

REFEDS Data Protection Code of Conduct

For Service Providers in a country which is not deemed to offer adequate data protection pursuant to Article 25.6 of the directive 95/46/EC and Home Organisations. [REMARK ML12 TO BE DISCUSSED.]

Purpose and Context

This Code of Conduct sets the rules that (i) Service Providers adhere to when they want to receive End Users' Attributes from Home Organisations or their Agent for providing access to their services; and (ii) Home Organisations adhere to when releasing End Users' Attributes to Service Providers.

The work leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007-2013) under Grant Agreement No. 238875 (GÉANT). This work is © 2013 Dante, used under a Creative Commons Attribution ShareAlike license (CC BY-SA 3.0).

1. Definitions

For the purposes of this Code of Conduct, the following terms shall have the following meanings:

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

Attributes: the End User's personal data as managed by the Home Organisation or its Agent, such as (but not limited to) name, e-mail and role in the Home Organisation.

Code of Conduct: this REFEDS data protection code of conduct.

Code of Conduct Adherence Form: means the form to be completed by a Home Organisation or Service Provider to confirm acceptance of the Code of Conduct, the template of which is included in annex 1.

Controller-to-Controller Model Contract: a data transfer agreement in the exact same form as the European Commission's Model Clauses under Commission Decision of 27 December 2004 amending Decision 2001/497/EC, as included in, and with the attachments and schedules set out in, annex 2.

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.

EU Data Protection Law: 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, and national legislation implementing this directive in the countries which are members of the European Union and/or EEA.

GÉANT: DANTE, City House, 126-130 Hills Rd, Cambridge, CB2 1PQ, UK. [REFEDS?]

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 Providers.

Party: any Home Organisation or Service Provider which submitted a duly completed and executed Code of Conduct Adherence Form to GÉANT.

Personal Data: has the meaning given to it in EU Data Protection Law.

Relevant Transfer: a transfer of Attributes and/or other Personal Data from a Home Organisation to a Service Provider in circumstances that do not offer an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data as required by EU Data Protection Law, and which is not subject to any of the permitted derogations or conditions contained in EU Data Protection Law (including without limitation consent of the data subject) such that, in the absence of the obligations created by this Code of Conduct, the export of the Attributes and/or other Personal Data would be in breach of the EU Data Protection Law.

Service Provider (SP): an organisation that is responsible for offering the End User the service he or she desires to use.

2. Code of Conduct adherence

2.1 Each Home Organisation and Service Provider that executes and submits to GÉANT a duly completed Code of Conduct Adherence Form shall be bound by and subject to all the rights and obligations of this Code of Conduct. Notwithstanding the foregoing, this Code of Conduct applies without prejudice to the provisions as set forth in the agreement between the Home Organisation and Service Provider which in all cases takes precedence over this Code of Conduct (except to the extent it concerns mandatory provisions set out in the Controller-to-Controller Model Contract.

2.2 GÉANT shall maintain, and make available upon a Party's request, an updated list of all Parties to the Code of Conduct. The list of Parties may at all times be consulted via [*to be completed*]. [

3. Incorporation of the Controller-to-Controller Model Contract

3.1 In relation to any Relevant Transfer between a Home Organisation and a Service Provider, this Code of Conduct (including in particular the terms of the Controller-to-Controller Model Contract) shall apply as an agreement between such Home Organisation in its capacity as data exporter and such Service Provider in its capacity of data importer.

3.2 The details of each such Relevant Transfer, and in particular the categories of personal data and the purposes for which they are transferred, are set out in annex B to the Controller-to-Controller Model Contract, which forms an integral part of this Code of Conduct.

3.3 The relevant Home Organisation shall assume all the rights, obligations and liability of the "data exporter" under the Controller-to-Controller Model Contract and the relevant Service Provider shall assume all the rights, obligations and liabilities of the "data importer" under the relevant Controller-to-Controller Model Contract.

3.4 Upon the request of GÉANT or a Home Organisation, any Service Provider that is a Party to this Code of Conduct shall enter into a stand-alone Controller-to-Controller Model Contract with a Home Organisation in order to comply with the EU Data Protection Law or to assist and/or expedite any approval by the relevant supervisory authority.

3.5 In case of conflict or ambiguity between the provisions of the main body of this Code of Conduct and the Controller-to-Controller Model Contract, the provisions of the Controller-to-Controller Model Contract shall prevail.

4. Principles of Attributes Processing

The Service Provider agrees and warrants:

4.1 **[Legal compliance]** to only process the Attributes in accordance with the relevant provisions of EU Data Protection Law and any personal data protection laws applicable to the Service Provider;

4.2 **[Purpose limitation]** to only process Attributes of the End User that are necessary for enabling access to the service provided by the Service Provider;

4.3 **[Data minimisation]** to minimise the Attributes requested from a Home Organisation 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;

4.4 **[Deviating purposes]** not to process the Attributes for any other purpose (e.g. selling the Attributes or selling the personalisation such as search history, commercial communications, profiling) than enabling access, unless prior consent has been given to the Service Provider by the End User;

4.5 **[Data retention]** to delete or anonymise all Attributes as soon as they are no longer necessary for the purposes of providing the service;

4.6 **[Third parties]** not to transfer Attributes to any third party (such as a collaboration partner) except

- if mandated by the Service Provider for enabling access to its service on its behalf, or
- if the third party adheres to the Code of Conduct or has undertaken similar duties considered sufficient under the data protection laws applicable to the Service Provider, or
- if prior consent has been given by the End User;

and in any case always in accordance with the provisions of the Controller-to-Controller Model Contract;

4.7 **[Security measures]** to take appropriate technical and organisational measures to safeguard Attributes against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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.

4.8 **[Information duty towards End User]** to provide to the End User, at least at first contact, in an easily, directly and permanently accessible way a privacy policy, containing at least the following information:

- the name, address and jurisdiction of the Service Provider;
- the purpose or purposes of the processing of the Attributes;
- a description of the Attributes being processed;
- 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 EEA;
- 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;

4.9 **[Information duty towards GÉANT]** to provide Géant with a machine-readable link to the Privacy Policy;

4.10 **[Security Breaches]** to, without undue delay, report all suspected privacy or security breaches (including unauthorized disclosure or compromise, actual or possible loss of data, documents or any device, etc.) concerning the Attributes to the relevant Home Organisation or its Agent;

4.11 **[Liability]** to defend, indemnify and hold harmless the End User, the Home Organisation as well as the Agent who has suffered damage as a result of any violation of this Code of Conduct by the Service Provider as determined in a binding and enforceable judicial ruling;

4.12 **[Termination of Code of Conduct adherence]** to only terminate adherence to this Code of Conduct in case of

- it being replaced by a similar arrangement or
- termination of the service provisioning to all Home Organisations which are a Party to this Code of Conduct;

5. Miscellaneous

5.1 As between each Home Organisation and Service Provider, this Code of Conduct shall be interpreted according to and governed by the laws of the country in which the Home Organisation is established, except for those provisions or clauses (and in particular the clauses and provisions as set out in the Controller-to-Controller Model Contract) that dictate the application of another law.

5.2 If any part, term or provision under this Code of Conduct is held to be illegal or unenforceable the validity or enforceability of the remainder of this Code of Conduct will not be affected.

5.3 The Parties shall remain 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.

DRAFT

Annex 1 – Code of Conduct Adherence Form

_____[*name*],

with registered office at _____[*address*],

hereby duly represented by _____[*name*],

in his/her capacity as _____[*function*],

hereby

1. Acknowledges to have received and reviewed the Code of Conduct, including the Controller-to-Controller Model Contract; and

2. Explicitly agrees to the content of the Code of Conduct, and agrees to be bound by all the terms and conditions of the Code of Conduct as [*Home Organisation / Service Provider*] as from the date of this Code of Conduct Form.

Name: _____

Date: _____

Signature: _____

DRAFT

Annex 2 – Controller-to-Controller Model Contract

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Definitions

For the purposes of the clauses:

"personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

"the data exporter" shall mean the controller who transfers the personal data;

"the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

"clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. OBLIGATIONS OF THE DATA EXPORTER

The data exporter warrants and undertakes that:

(a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

(b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

(c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

(d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

(e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access

to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. OBLIGATIONS OF THE DATA IMPORTER

The data importer warrants and undertakes that:

(a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

(b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

(c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

(d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

(e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

(f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

(g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

(h) It will process the personal data, at its option, in accordance with:

(i) the data protection laws of the country in which the data exporter is established, or

(ii) the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data, or

(iii) the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: option (iii).

(i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

(i) the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

(ii) the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

(iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

(iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer.

III. LIABILITY AND THIRD PARTY RIGHTS

(a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

(b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. LAW APPLICABLE TO THE CLAUSES

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR THE AUTHORITY

(a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

(b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

(c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. TERMINATION

(a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

(b) In the event that:

(i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

(ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

(iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

(iv) a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

(v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed

where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

(c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

(d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. VARIATION OF THESE CLAUSES

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. DESCRIPTION OF THE TRANSFER

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

DRAFT

ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.

8. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

   (a) (i) such decisions are made by the data importer in entering into or performing a contract with the data subject, and

   (ii) the data subject is given an opportunity to discuss the results of a relevant automated decision

with a representative of the parties making such decision or otherwise to make representations to that parties.

or

(b) where otherwise provided by the law of the data exporter.

DRAFT

ANNEX B

DESCRIPTION OF THE TRANSFER

Data subjects

The personal data transferred concern the following categories of data subjects:

End Users, as defined in the Code of Conduct. [note: incorporation by reference of definitions to be discussed]

Purposes of the transfer(s)

The transfer is made for the following purposes:

So as to enable the End User (as defined in the Code of Conduct) to access the data importer's services. The transferred data may not be used for any other purposes.

Categories of data

The personal data transferred concern the following categories of data:

Attributes, as defined in the Code of Conduct. [TBD

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

Suppliers of data importer, only to the extent necessary to enable the End User to access the data importer's services.

Sensitive data

The personal data transferred concern the following categories of sensitive data:

Not applicable. [TBD]

Additional useful information (storage limits and other relevant information)

Not applicable.

Contact points for data protection enquiries

Contact points available on request from GÉANT.

DRAFT