Instructions for Processor Agreement

SURF Framework of Legal Standards for (Cloud) Services – Annex B

Utrecht, October 2016
Version number: 1.0

Credits

Instructions for Processor Agreement
SURF Framework of Legal Standards for (Cloud) Services – Annex B

SURF
P.O. Box 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

October 2016

SURF is the collaborative ICT organisation for higher education and research in the Netherlands.
This publication is available in digital format on the SURF website: www.surf.nl/publicaties

Introduction

These instructions and explanations form part of the Processor Agreement, version 1.1 (October 2016) which in turn is part of the SURF Framework of Legal Standards for (Cloud) Services.

A Processor Agreement focuses specifically on processing Personal Data. All provisions in this Agreement are therefore about Personal Data.

Broader subjects are generally included in the master agreement. Examples of such subjects are intellectual property (this may also concern data that is not personal) and confidentiality (data such as sensitive business information can be confidential, but not personal). Standard provisions regulating these subjects in the master agreement can be found in the memorandum of the SURF Framework of Legal Standards for (Cloud) Services.

This document shall continue to undergo development and regular updates shall appear in response to questions from the target group. The document provides guidance during the use of the Processor Agreement, but in the event of any doubt or questions, always consult a (legal) adviser in your organisation.

READING GUIDE

This document uses boxes such as this one to explain why certain provisions are important and how they should be read. It also refers to the laws and regulations that are developed in provisions or on which provisions are based. This document also includes instructions that help you complete Annex A.

The document refers to the following legislation, regulations, documentation and websites:

The Dutch Personal Data Protection Act (Wet Bescherming Persoonsgegevens or Wbp)
The Personal Data Protection Act is a currently valid national law to be replaced by a European regulation in May 2018: the General Data Protection Regulation.

The General Data Protection Regulation (GDPR)
The General Data Protection Regulation came into force in May 2016, but is not yet applicable. This legislation must be met within a two-year term. The regulation shall replace the Personal Data Protection Act in May 2018, so it is advisable to bear in mind the rules of the General Data Protection Regulation now.

Personal Data Protection Authority guidelines, Personal Data Security, February 2013
The Personal Data Authority (formerly the Personal Data Protection Board) published guidelines in 2013 which explain how the Personal Data Authority applies the security standards of the Personal Data Protection Act to investigate and assess Personal Data security. This document can be found on its website: https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-publiceert-richtsnoeren-beveiliging-van-persoonsgegevens

Policy rules for the implementation of Article 34a of the Personal Data Protection Act, Personal Data Authority, December 2015
Policy rules with regard to the duty to report data breaches are available on the Personal Data Authority's website: https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

The Personal Data Authority's website
References to news reports and explanation of legislation.

Security Measures Guide, Framework of Legal Standards – Annex C
Guide about the implementation of a suitable security level as part of the SURF Framework of Legal Standards for (Cloud) Services. October 2016 version. The document is available on the SURF website:
https://www.surf.nl/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html

Audit Requirement Guide, Framework of Legal Standards – Annex D
Implementation guide for the audit requirement of the Processor Agreement under the SURF Framework of Legal Standards for (Cloud) Services. October 2016 version. The document is available on the SURF website: https://www.surf.nl/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html

The Parties

- **[INSTITUTION NAME]**, based at [ADDRESS] in [CITY], with Chamber of Commerce number [COC] and legally represented by **[REPRESENTATIVE]** (hereinafter referred to as "**the Controller**");

- **[SUPPLIER NAME]**, based at [ADDRESS] in [CITY], with Chamber of Commerce number [COC] and legally represented by **[REPRESENTATIVE]** (hereinafter referred to as "**the Processor**");

taking into account that:

- The Controller wants to have Personal Data processed by the Processor in execution of the Agreement concluded with the Processor on XX-XX-XX (hereinafter referred to as "the Agreement").
- The Processor working with Responsible Personal Data in the execution of the Agreement shall be regarded as the Processor in the sense of the Personal Data Protection Act and the institution shall be regarded as the Controller in the sense of the Personal Data Protection Act.

> As part of the Agreement, it is specifically stated that if the supplier processes Personal Data, the institution is the Controller and the supplier is the Processor in the sense of the Personal Data Protection Act. This specific statement makes it clear which rights and obligations of the Personal Data Protection Act apply to the institution and the supplier.
>
> Legislation and regulations:
> - Article 1 of the Personal Data Protection Act
> - Article 4 of the General Data Protection Regulation

- Taking into account the requirement of Article 14, paragraph 5 of the Personal Data Protection Act, the Processor and Controller, hereinafter referred to as "the Parties", wish to document their rights and obligations in this Processor Agreement, hereinafter referred to as "the Processor Agreement".
- The general provisions of the Processor Agreement apply to all processing in the execution of the Agreement.

have agreed as follows:

ARTICLE 1. DEFINITIONS

1.1 The Data Subject is the individual the Personal Data is about.

1.2 The Processor Agreement is this Agreement.

1.3 Sensitive Data is Personal Data as referred to in Article 16 of the Personal Data Protection Act.

1.4 A Data Breach is a security breach as referred to in Article 13 in conjunction with Article 34a of the Personal Data Protection Act.

1.5 The Service is the Supplier's service to be delivered under the Agreement.

1.6 The User is a (natural) person in any way associated with the Controller, such as staff, lecturers and/or students, authorised to use (a certain part of) the Service by the Controller.

1.7 The Subcontractor is a party used by the Processor to provide support in the execution of the Service. If the Subcontractor processes Personal Data at the Processor's request, the Subcontractor shall also be regarded as a Subprocessor.

1.8 Personal Data is any information regarding an identified or identifiable natural person (to be) processed in any way by the Processor under the Agreement.

1.9 The Subprocessor is a Subcontractor processing Personal Data at the request of the Processor.

1.10 Processing is any operation or set of operations with Personal Data, which always includes data collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, transmission, distribution or any other form of provision, combination, alignment, shielding, exchange or destruction.

ARTICLE 2. GENERAL

2.1 The Processor undertakes to process Personal Data at the Controller's request under the conditions of this Processor Agreement. The Processor shall process the Personal Data adequately and accurately in accordance with the Personal Data Protection Act and other applicable laws and regulations regarding the processing of Personal Data.

2.2 The Processor shall only process the Personal Data necessary to provide the Service to the Controller as described in the Agreement. Only the Personal Data categories specified in Annex A can be processed to provide the Service.

Only the Personal Data necessary to provide the Processor's service can be processed. The master agreement associated with this Processor Agreement includes a description of the Service. Annex A contains a specification of the Personal Data. This makes it clear to both the Controller and the Processor which Personal Data can be processed. Data minimisation plays a part in this regard: only the Personal Data necessary to provide the Service can be processed.

Legislation and regulations:

- Article 28 paragraph 3 (a) of the General Data Protection Regulation

2.3 Annex A describes which (groups of) employees have access to the Personal Data and which Data processing is permitted for which employees for each Service.

To increase Personal Data security, the Processor Agreement shall specify which employees (officials) or which employee groups can process the Personal Data in specific ways. Employees other than the mentioned (groups of) employees mentioned in this article are specifically banned from processing the data. These employees shall maintain confidentiality.

Legislation and regulations:
- Page 33 of the Personal Data Protection Authority guidelines, Personal Data Security, February 2013
- Article 28 paragraph 3 (b) of the General Data Protection Regulation

2.4 The Processor shall not keep the Personal Data it receives under the Agreement for longer than required (i) for the execution of this Agreement; or (ii) in order to meet an imposed legal obligation. Annex A specifies how long Personal Data can be kept for each (part of the) Service.

The institution shall ensure that the supplier does not keep the Personal Data for longer than is necessary to provide the Service. This means that when the Agreement is terminated, the Personal Data can no longer be processed and must be destroyed or transferred (see Article 13). The exception to this provision is a mandatory legal obligation that the Supplier must meet.

Legislation and regulations:
- Article 10 of the Personal Data Protection Act
- Page 34 of the Personal Data Protection Authority guidelines, Personal Data Security, February 2013
- Article 5 paragraph 1(e) of the General Data Protection Regulation

Examples of statutory retention periods are available on the Personal Data Authority's website:

https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/bewaren-van-persoonsgegevens

2.5 The Processor shall only process the Personal Data at the request and according to the instructions of the Controller. The Processor shall not process the Personal Data for its own benefit, for the benefit of third parties, for its own or a third party's advertising purposes or any other purpose, except when forced to do so by other legal mandatory obligations.

The supplier may only process the institution's Personal Data if it is necessary in order to provide the Service to the institution. The supplier shall not use the Personal Data for its own purposes. The Controller determines the purposes of the data processing.

Legislation and regulations:
- Articles 12 and 14 of the Personal Data Protection Act
- Article 28 paragraph 3(a) of the General Data Protection Regulation

2.6 The Processor shall inform the Controller of any future changes to the execution of the Agreement immediately to allow the Controller to ensure compliance with the arrangements made with the Processor. This includes the engagement of (new) Subcontractors, without prejudice to the provisions of Article 3 on the use of subcontractors and Article 12 on changes.

ARTICLE 3. USE OF SUBCONTRACTORS

3.1 The Processor shall not give any third parties – including Subcontractors and companies belonging to the same group as the Processor, such as subsidiaries and affiliates – access to the Personal Data without the Controller's prior written approval. The Controller shall not withhold this approval without a valid reason. The Controller is entitled to set certain conditions or time limits for its approval.

Under the General Data Protection Regulation, one processor shall not engage another processor without the Controller's prior specific or general written approval. This paragraph regulates the specific written approval. A general written approval can also be used. This is arranged in paragraph 3 of this article.

In the event of a general written approval, the Processor shall inform the Controller of the change in processors and shall offer the Controller the opportunity to object to this change.

Legislation and regulations:
- Article 28 paragraph 2 of the General Data Protection Regulation

3.2 The Controller's approval of the use of Subcontractors to provide the Service shall always be subject to the following conditions:

- The Processor has a written agreement with the Subcontractor in question, which shall always include the following:
  - an obligation that ensures the Subcontractor's actions are in accordance with all provisions of the Processor Agreement, including the Annexes with regard to Personal Data processing;
  - an obligation that ensures the Subcontractor follows all instructions by the Controller and Processor on how the Personal Data is to be processed;
  - an obligation that ensures the Subcontractor only processes Personal Data at the Processor's request and according to its instructions;
  - an obligation that ensures the Subcontractor does not engage any Subprocessors independently without the Controller's prior written approval;
  - an obligation that ensures the Subcontractor allows the Processor (and also the Controller) to meet their obligations in the event of a suspected or actual Data Breach.
- The Processor shall only give the Subcontractor access after the Controller has given its approval; and
- the Controller can request to see the arrangements made between the Processor and the Subcontractor.

The Controller's approval is without prejudice to the Processor's responsibility and liability for complying with the Processor Agreement.

Third parties may only help process the Personal Data if they are *directly* involved in the provision of the Service.

The supplier shall have a written agreement with the third party stating that the third party shall meet all the provisions of this Agreement. It is the only way the institution can ensure an adequate level of Personal Data protection in its position as Controller.

Legislation and regulations:
- Articles 12, 13 and 14 of the Personal Data Protection Act
- Pages 33 and 34 of the Personal Data Protection Authority guidelines, Personal Data Security, February 2013
- Article 28 paragraph 4 of the General Data Protection Regulation

3.3. If the Controller provides a general written approval of the engagement of Subcontractors to deliver the Service, this general approval shall be included in Annex A. If new Subcontractors are engaged or if any changes occur, the Processor shall inform the Controller in advance and offer a time limit for any objections. The Processor guarantees that each Subcontractor shall respect the conditions of Article 3, paragraph 2. The Processor must be able to provide an overview of the engaged Subcontractors at all times at the Controller's request.

A general approval is one option. In that case, the Controller does not need to approve each new Subcontractor in writing in advance. Instead, the Controller is informed in advance with an opportunity to object (also see explanation with paragraph 1). Annex A mentions a sample text to arrange the general approval.

Legislation and regulations:
- Article 28 paragraph 2 of the General Data Protection Regulation

ARTICLE 4. SECURITY

4.1 The Processor shall implement the appropriate technical and organisational measures to secure the Personal Data against loss or any form of unauthorised processing. These measures shall guarantee the appropriate security level for the risks involved in the data processing and the type of Personal Data to be protected, taking into account current technological developments and the costs of their implementation. The measures also aim to prevent unnecessary data collection and further processing. The Processor records the measures taken and ensures that the security referred to in this paragraph meets the security requirements pursuant to the Personal Data Protection Act. Annex A describes the security measures that shall always be implemented by the Processor.

As the Controller, the institution shall ensure the supplier maintains adequate Personal Data security. The Processors shall offer sufficient guarantees with regard to the implementation of the appropriate technical and organisational measures, to ensure that the data processing meets the legal requirements and the Data Subject's rights are protected. The institution shall perform a risk analysis to determine whether the supplier offers sufficient guarantees in terms of Personal Data protection.

Legislation and regulations:
- Articles 13 and 14 of the Personal Data Protection Act
- Page 33 of the Personal Data Protection Authority guidelines, Personal Data Security, February 2013
- Article 28 paragraph 1, paragraph 3(c) and Article 32 of the General Data Protection Regulation

More information on suitable security: see Security Measures Guide, Framework of Legal Standards – Annex C:

https://www.surf.nl/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html

4.2 The Processor shall immediately provide written information on (the organisation of) the Personal Data's security at the Controller's request.

As the Controller, the institution must be able to check whether the Personal Data is adequately secured. The supplier shall therefore provide written information on the data security immediately at the institution's request.

Legislation and regulations:
- Article 14 of the Personal Data Protection Act
- Page 33 of the Personal Data Protection Authority guidelines, Personal Data Security, February 2013
- Article 28 paragraph 3(h) of the General Data Protection Regulation

ARTICLE 5. DUTY TO REPORT DATA BREACHES AND SECURITY BREACHES

5.1 In the event of a suspected or actual (i) Data Breach; (ii) violation of security measures; (iii) breach of confidentiality or (iv) loss of confidential data, the Processor shall inform the Controller immediately and certainly no later than 24 hours after discovering the incident. The Processor shall take all the measures that are reasonably required to prevent or limit any (further) unauthorised access, alteration, access and otherwise unauthorised processing, and to stop and further prevent any violation of security measures, breach of confidentiality or further loss of confidential data, without any prejudice to the Controller's right to damages or other compensation. This provision applies to incidents involving the Processor and its possible Subcontractors.

The Personal Data Protection Act states that the Controller shall report any Data Breaches that fall under the reporting requirement to the Personal Data Authority within 72 hours. This also includes Data Breaches taking place at the location of the Processors or the Processor's Subcontractors.

The Controller shall therefore be notified on time, so that it can assess whether a report is required. This Article therefore states that the Processor shall notify Data Breaches to the Controller within 24 hours of their detection. This also includes Data Breaches of any engaged Subcontractors. The Processor shall therefore also make arrangements with the Subcontractors with regard to the duty to report Data Breaches. Because the chain of parties involved is longer here, an 18-hour term applies for Subcontractors. This allows the Controller to submit a report within 72 hours.

Annex B lists the information the Processor needs to provide to the Controller. This is based on the information the Personal Data Authority requests in a report.

In Annex A, you can indicate the Controller contact or department the Processor must contact to report a possible Data Breach.

Legislation and regulations:
- Article 34a of the Personal Data Protection Act
- Policy rules for the implementation of Article 34a of the Personal Data Protection Act, Personal Data Authority, December 2015.

NB: Certain points of the duty to report Data Breaches described in the Personal Data Protection Act differ from the General Data Protection Regulation's duty to report Data Breaches. This Article is based on the Personal Data Protection Act, because the duty to report Data Breaches shall continue to be valid until May 2018. The duty to report Data Breaches described in the Personal Data Protection Act shall be valid from May 2018. It is recommended to see whether new arrangements need to be made on the duty to report Data Breaches by then.

- Article 33 of the General Data Protection Regulation

5.2 The Processor's duty to provide information always includes the data described in Annex B if applicable. The Processor guarantees that the provided information is complete, correct and accurate.

5.3 The Processor shall help to inform the competent authorities and Data Subject(s) at the Controller's request.

Besides the duty to provide information, the supplier shall also respond to the incidents by securing the Personal Data, by taking measures to stop and/or prevent the incident and by cooperating in the further handling of the incidents.

Legislation and regulations:
- Article 14 of the Personal Data Protection Act
- Page 33 of the Personal Data Protection Authority guidelines, Personal Data Security, February 2013

5.4 The Processor makes written arrangements with the Subcontractors for incident reporting to the Processor. These arrangements enable the Processor and Controller to meet their obligations in the event of an incident as described in Article 5, paragraph 1. These arrangements shall always include the Subcontractor's obligation to inform the Processor of any incident described in Article 5 paragraph 1 immediately and certainly no later than 18 hours after discovering the incidents, and to help inform the competent authorities and Data Subject(s) at the Controller's request.

ARTICLE 6. AUDIT

6.1 The Processor is obliged to assign an independent IT auditor or expert to assess the Processor's organisation periodically or at the Controller's request to ensure the Processor meets the provisions on protection of confidentiality, integrity, availability and security of Personal Data and confidential data as described in the Agreement and the Processor Agreement. The frequency of the assessment is once every two years if the class is 'medium' risk. 'High' risk Data Processing requires an annual assessment of the Processor. The risk is always 'high' when processing sensitive Personal Data as referred to in the Personal Data Protection Act. If only public Personal Data is processed, the risk is considered 'low' and there is no obligation to perform a periodic investigation. Annex A describes the risks.

The institution shall inspect the supplier's Service and security depending on the risk class. This may involve periodic inspection by an independent expert. How often the Processor has to have an audit performed depends on the type of Personal Data.

There are three risk classes:
- The Low risk class: Personal Data that is already public. No periodic audit requirement
- Basic/Medium risk class: Personal Data that is not included in the 'Sensitive Personal Data' category. In that case, the audit shall be performed once every two years.
- The High risk class: always Personal Data that is included in the 'Sensitive Personal Data' category. In that case, the audit shall be performed every year.

Such an investigation also needs to take place before the agreement is concluded to ensure that the institution examines the supplier's Service.

More information on the audit requirement: see Audit Requirement Guide, Framework of Legal Standards – Annex D:
https://www.surf.nl/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html

Legislation and regulations:
- Article 14 of the Personal Data Protection Act
- Pages 33 and 35 of the Personal Data Protection Authority guidelines, Personal Data Security, February 2013
- Article 28 paragraph 3(h) of the General Data Protection Regulation

6.2 The Processor shall make available the findings of the IT auditor or expert to the Controller in a Third Party Memorandum upon request.

A TPM is a statement by an independent external expert assessing the measures taken by a Processor. The TPM is prepared at the Processor's request and is provided to the Controllers using the Processor's Services. The aim of providing a TPM is to give the Controllers a good understanding in the measures taken, so that the Controllers do not need to investigate this individually.

Source: Page 35 of the Personal Data Protection Authority guidelines, Personal Data Security, February 2013

6.3 The Processor shall prepare a monthly security management report within five working days of the start of next calendar month. This report shall include at least the following elements:

- number, status, progress and analysis of security incidents;
- security management measures taken in response to security incidents;
- general data security measures taken.

As the Controller, the institution is responsible for checking the supplier's information security. Periodic reporting on information security and security incidents allows the supplier's Service to be checked at a higher level.

Legislation and regulations:
- Article 14 of the Personal Data Protection Act
- Pages 33 and 35 of the Personal Data Protection Authority guidelines, Personal Data Security, February 2013
- Article 28 paragraph 3(h) of the General Data Protection Regulation

6.4 The Processor shall bear the costs of the periodic audit. The Controller shall bear the costs of a requested audit, unless the audit findings show that the Processor has not met the Processor Agreement provisions. In that case, the Processor shall bear the costs. This provision shall be without prejudice to any of the Controller's other rights, including its rights to compensation.

In areas where the risks are high, a periodic investigation is insufficient. If the institution reasonably suspects that the supplier is violating the arrangements in place, the institution shall investigate this suspicion with a (limited) quality check directly associated with the suspected violation. The scope of this examination is therefore limited to the arrangements that the institution reasonably suspects have been violated.

The costs of the investigation's execution are primarily covered by the institution. If the investigation shows that certain arrangements were indeed violated, the institution may charge the supplier for the costs of the examination.

Legislation and regulations:
- Article 14 of the Personal Data Protection Act
- Pages 33 and 35 of the Personal Data Protection Authority guidelines, Personal Data Security, February 2013

6.5 When it is established during an audit that the Processor does not meet the provisions of the Agreement and the Processor Agreement, the Processor shall take all steps that are reasonably required to ensure these are still met.

ARTICLE 7. INTERNATIONAL TRAFFIC

7.1 The Processor guarantees that all Personal Data processing by the Processor or on the Processor's behalf – including by third parties engaged by the Processor – in the execution of the Agreement shall take place in the European Economic Area (EEA) or in countries that guarantee an appropriate level of protection in accordance with the applicable privacy legislation. No Personal Data shall be forwarded to, stored in or made available from a country outside the EEA by the Processor without the Controller's prior written approval, unless the country has an appropriate protection level. The Controller may attach certain conditions to this approval. For example, it can oblige the Processor to show that the legal requirements on data traffic with countries outside the EEA are met.

In principle, Personal Data shall only be processed in other countries that ensure an appropriate level of protection. Countries in the European Economic Area (EEA) all ensure a high level of privacy protection. The European Commission also published a list of countries that ensure an appropriate level of protection (the so-called white list) via:

http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Data processing in other countries that do not ensure an appropriate level of protection is only permitted based on a statutory exception or with a permit from the Minister of Security and Justice. More information about statutory exceptions is available on the Personal Data Authority's website:

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu#wanneer-mag-ik-toch-persoonsgegevens-doorgeven-naar-een-derde-land-zonder-passend-beschermingsniveau-1753

Personal Data Processing in the US: the US does not have general legislation on Personal Data protection and therefore does not offer an appropriate level of protection.

Personal Data may only be processed in the US if:

- a statutory exception applies;
- the Minister of Security and Justice has provided a permit;
- the EU-US Privacy Shield is in use;
- the appropriate binding corporate rules are in place (internal codes of conduct).

More information about data processing in the US and the current status of the Privacy Shield is available on the Personal Data Authority's website:

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu

Legislation and regulations:
- Articles 76 and 77 of the Personal Data Protection Act
- Page 34 of the Personal Data Protection Authority guidelines, Personal Data Security, February 2013
- Article 44 et seq. of the General Data Protection Regulation

7.2 If the technical characteristics of a transmission medium make such a guarantee impossible, the data must always be encrypted for transmission. In that case, advanced techniques shall be used (at least as advanced as is customary in the industry). The Processor shall disclose the Data Processing location(s) before the Processor Agreement is concluded.

ARTICLE 8. SEARCH REQUESTS

8.1 If a Processor receives a request or an order to provide (access to) Personal Data from a Dutch or foreign regulator, government body, investigation authority, criminal or national security service, the Processor shall inform the Controller immediately. The Processor shall respond to the request or order by observing all the Controller's instructions (including the instruction to have the request or order partly or completely handled by the Controller) and shall cooperate with the Controller as reasonably required.

In case of cloud services, data is not kept at the institution's location. When the authorities request to access the data, the institution must respond adequately in its capacity of Controller. When the supplier receives such a mandatory request or order, it shall inform the institution. The institution's instructions must be observed in this regard. The instructions may be to let the request or order be handled by the institution. As the Controller of the (personal) data, the institution must be the point of contact for such requests or orders.

Legislation and regulations:
- Pages 34 and 35 of the Personal Data Protection Authority guidelines, Personal Data Security, February 2013

8.2 If the request or order prohibits the Processor from meeting its obligations pursuant to the above provisions, the Processor shall serve the reasonable interests of the Controller. In this case, the Processor shall always:

a. have a legal assessment performed of (i) the extent to which the Processor is obliged to comply with the request or order; and (ii) the extent to which the Processor is actually prohibited from meeting its obligations to the Controller pursuant to the above provisions;
b. cooperate to comply with the request or order only if it is legally obliged to do so and (legally) oppose the request, order or ban from notifying the Controller or from following its instructions where possible;
c. refrain from providing any Personal Data beyond or other than what is strictly necessary to comply with the request or order;
d. investigate the possibilities to comply with Articles 76 and 77 of the Personal Data Protection Act in the event data is transferred to a country outside the EEA;
e. inform the Controller immediately as soon as this is permitted.

In some cases, the supplier must not comply with the first paragraph due to mandatory laws and regulations. In these cases, the institution shall still guarantee the security of the data. The supplier shall therefore perform certain actions that are normally performed by the Controller.

The mentioned actions guarantee the Personal Data protection as much as possible.

8.3 In this article, "legal" not only refers to Dutch laws and regulations, but also to foreign laws and regulations.

ARTICLE 9. INFORMING THE DATA SUBJECTS

9.1 The Processor shall cooperate fully to ensure the Controller can meet its legal obligations in the event a Data Subject is exercising their rights under the Personal Data Protection Act or other applicable regulations regarding Personal Data processing.

Pursuant to the Personal Data Protection Act, the Data Subjects have access and correction rights in terms of their own Personal Data. The Data Subject can submit a request to the Controller (institution) in this regard. This provision obliges the supplier to cooperate in order to comply with the Data Subject's rights.

Legislation and regulations:
- Articles 35 and 36 of the Personal Data Protection Act
- Article 28 paragraph 3(e) of the General Data Protection Regulation

9.2 If Data Subjects contact the Processor directly with regard to the execution of their rights under the Personal Data Protection Act, the Processor shall not provide a response (in terms of content), but shall immediately report this to the Controller with a request for further instructions, unless specifically instructed otherwise by the Controller.

To protect the Data Subjects' rights and Personal Data security, the supplier is not permitted to respond to requests from Data Subjects. The Controller (the institution) shall first check the legitimacy of such requests. In exceptional cases, the institution may give a different instruction to the supplier.

Legislation and regulations:
- Articles 35 and 36 of the Personal Data Protection Act
- Article 28 paragraph 3(e) of the General Data Protection Regulation

9.3 If the Processor offers the Service directly to the User whose Personal Data is processed, the Processor shall notify the User by means of an easily accessible, permanently available privacy policy only if requested by the Controller to do so. This privacy policy shall include the following:

a. the name and address of the Controller and Processor;
b. the purposes of the Personal Data processing;
c. the categories of Personal Data the Processor is processing;
d. the third parties who are given access to Personal Data;
e. the countries to which Personal Data is transferred;
f. the right to access, correct and delete Personal Data.

The Processor shall inform the Controller where this information has been published.

Article 9.3 does not stem directly from the Personal Data Protection Act nor the General Data Protection Regulation, but has been added to the Processor Agreement to be in line with the GÉANT Data Protection Code of Conduct. This is a European code of conduct developed by GÉANT that Service Providers can sign unilaterally to show that they meet the strict European security and privacy laws. This Code of Conduct also includes a provision similar to 9.3. However, Article 9.3 specifically states that such an obligation to inform the User is only possible at the Controller's request. This obligation does not replace the Controller's own duties pursuant to the Personal Data Protection Act.

The Code of Conduct is available on the GÉANT website:

http://geant3plus.archive.geant.net/uri/dataprotection-code-of-conduct/Pages/default.aspx

ARTICLE 10. DISCLAIMER

The Processor shall indemnify the Controller against all claims by third parties – including the Data Subjects – filed against the Controller for an alleged breach of the Personal Data Protection Act or other applicable Personal Data processing regulations by the Processor or the Subcontractor it engaged.

When a third party (for example a Data Subject) addresses the institution with regard to a violation of the Personal Data Protection Act (or another Personal Data law or regulation) and the violation is due to the supplier or a third party engaged by the supplier, the supplier shall indemnify the institution against this claim.

When the supplier engages a third party for Personal Data processing, this does not mean that the supplier no longer needs to meet its Personal Data obligation.

Legislation and regulations:
- Page 34 of the Personal Data Protection Authority guidelines, Personal Data Security, February 2013

ARTICLE 11. REGULATOR MEASURES

If the regulator imposes a measure or penalty on the Controller as part of its enforcer role because the Processor failed to comply with the arrangements made in the Processor Agreement, the Controller can recover all the costs of this measure or penalty from the Processor. The Controller is entitled to dissolve the Agreement with immediate effect in the above situation. In that case, the Processor shall not be able to claim any type of compensation.

When the Personal Data Authority imposes a measure on the institution because it (or a Subcontractor engaged by the supplier) violated the Personal Data Protection Act by not complying with the Agreement's provisions, the institution can recover the costs of the measure from the supplier.

ARTICLE 12. CHANGES

12.1 The Parties shall discuss changes to the arrangements of the Processor Agreement at the Controller's request, if they are justified by a change in the Personal Data to be processed or a risk analysis of the processed Personal Data.

In order to execute its Controller task, the institution shall make sure the Personal Data is processed according to the risk level that is determined in advance. If the data processing (the supplier's Service) changes, the institution must be able to check before the change whether the data will be processed according to the appropriate level. The duty to provide information as stated in this article was included to this effect.

Legislation and regulations:
- Page 35 of the Personal Data Protection Authority guidelines, Personal Data Security, February 2013

12.2 The arrangements to be made must be recorded in writing as part of the Processor Agreement before they are implemented.

12.3 The changes shall never prevent the Controller from complying with the Personal Data Protection Act and other relevant Personal Data laws and regulations.

ARTICLE 13. DURATION AND TERMINATION

13.1 The duration of the Processor Agreement is the same as the duration of the Agreement. The Processor Agreement cannot be terminated separately from the Agreement.

13.2 If the Agreement is terminated at the Controller's request during the Agreement's term or for any other reason, the Processor shall receive a limited fee that shall not exceed the reasonable, demonstrable costs the Processor incurred to ensure that, at the Controller's discretion and in a way that is convenient for the Controller, (i) all the Personal Data provided as part of the Service or a specific portion of this Personal Data determined by the Controller is destroyed in all locations, (ii) all the Personal Data provided as part of the Service or a specific portion of this Personal Data determined by the Controller is made available to a subsequent Service Provider, or (iii) the Controller and/or Users are given the opportunity to withdraw from the Service their Personal Data provided as part of the Service or a specific portion of this Personal Data determined by the Controller. If necessary, the Controller may make further requirements with regard to the way the Personal Data is made available – file format, for example – or destroyed.

When the Agreement is terminated, the (Personal) Data processed by the supplier shall be either destroyed or transferred to a new supplier or the institution itself. Any other option does not offer the appropriate protection to the (Personal) Data.

The institution can also have data destroyed or moved outside the supplier's Service on request during the term of the Agreement. This allows the institution to further manage and stay in control of the data (also see Article 2, paragraph 4 of this Processor Agreement).

Data portability is the ability to move the data in the cloud. When there is no data portability, the institution can no longer recover the data.

Legislation and regulations:
- Article 10 of the Personal Data Protection Act
- Page 35 of the Personal Data Protection Authority guidelines, Personal Data Security, February 2013
- Article 28 paragraph 3 of the General Data Protection Regulation

13.3 The Processor shall always guarantee the data portability described in the previous paragraph to avoid any loss of functionality or (parts of) data.

13.4 Any obligations that by their nature persist after the Processor Agreement has been terminated shall remain valid after the dissolution of the Processor Agreement. These include obligations resulting from provisions on confidentiality, disclaimer and liability and applicable law.

ARTICLE 14. CONFIDENTIALITY

Although confidentiality extends beyond Personal Data (sensitive corporate data can also be confidential, for example), this Processor Agreement also contains a confidentiality clause for the sake of completeness in case the master agreement does not address this issue. The Personal Data Authority also stated in a news item in May 2016 that a processor agreement must include duty of confidentiality.

See: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-eist-betere-afspraken-over-digitalis-eren-pati%C3%ABntdossiers

14.1 If data confidentiality is not arranged in the Agreement or elsewhere, the Parties shall keep secret all (Personal) Data and other information received or accessed in the execution of the Agreement or the Processor Agreement if they know or can reasonably suspect that the data is confidential. They shall not disclose such data internally or externally or provide it to any third parties in any way, except:

a. when disclosure and/or provision of this (Personal) Data and other information is necessary in connection with the execution of the Agreement;
b. when any mandatory legal statutory or court ruling forces the Parties to disclose and/or provide the (Personal) Data or other information, in which case the Parties shall inform the other party first;
c. when the (Personal) Data is announced and/or provided with the other party's prior approval in writing; or
d. when the information was already lawfully considered public not caused by one of the Parties' actions or failure to act.

14.2 The Parties shall contractually oblige the internal and external people involved in the processing of confidential (Personal) Data to keep the confidential (Personal) Data and other information secret.

14.3 The Parties shall cooperate when the storage and use of confidential (Personal) Data and other information are supervised by or on behalf of the other Party.

14.4 The Parties shall make available all (Personal) Data and other information they have available for the execution of the Agreement – including any copies – at the other Party's request.

ARTICLE 15. APPLICABLE LAW AND DISPUTE RESOLUTION

15.1 The Processor Agreement and its execution are governed by Dutch law.

15.2 Any disputes arising between the Parties in connection with the Processor Agreement shall be presented to the competent court in the location where the Controller is based.

INSTITUTION NAME

_____/_____/_____

Date

_____

Name

_____

Signature

SUPPLIER NAME

_____/_____/_____

Date

_____

Name

_____

Signature

Annex A: Personal Data Processing Specifications

This Annex explains the following about the Processor's Service:

- Data Subject categories
- Personal Data (categories) to be processed;
- job roles and/or job groups and their Processing;
- affected security measures;
- Subcontractors;
- contact details.

If the Processor offers several separate services to the Controller, the information can be included in separate Annexes numbered as follows: "Annex A1", "Annex A2", etc.

These Annexes are attached to the Processor Agreement.

Annex A1: <SERVICE NAME>

Version number XX, date of last update: XX-XX-XX

Data Subject categories

<Specify who can be regarded as Data Subjects for the Service>

The Data Subject is the individual the Personal Data is about. There can be different Data Subject categories, such as students, staff or contacts.

Personal Data (categories) to be processed

The Processor processes the following Personal Data (categories) on the Controller's behalf. This is not just Personal Data the Controller provides to the Processor directly, but also Personal Data the User provides when using the Service.

<Enter Personal Data (categories)>

The level of detail of the Personal Data description in writing is at the discretion of the party providing it. In any case, it must be clear to everyone exactly which Personal Data the description refers to. Examples are names, addresses, telephone numbers, login details or exam results. See all Personal Data included in the Service. For more information about Personal Data, visit the Personal Data Authority's website: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens

The following risk class applies to the Agreement: <Enter which risk class applies, possibly with an explanation>.

The Framework of Legal Standards for (Cloud) Services mentions three types of risk classes:

- The Low risk class: Personal Data that is already public.
- The Basic risk class: Personal Data that is not included in the 'Sensitive Personal Data' category.
- The High risk class: always Personal Data that is included in the 'Sensitive Personal Data' category.

The risk class affects the audit requirement (see Article 6) and the appropriate security measures.

More information on the audit requirement: see Audit Requirement Guide, Framework of Legal Standards – Annex D:

https://www.surf.nl/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html

More information on suitable security: see Security Measures Guide, Framework of Legal Standards – Annex C:

https://www.surf.nl/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html

Retention periods

The Processor does not keep Personal Data for longer than is necessary for the execution of this Agreement or its compliance with a legal obligation. The following retention periods apply to Personal Data processed for the correct operation of the Service (logging, backup facilities, etc.):

<Enter which retention periods apply>

Some Personal Data is processed for as long as the Service is provided and arrangements are made about data transfer or deletion as soon as the Service is no longer used. However, some Personal Data does not have to be kept for the entire duration of the Service. Examples of this are back-up storage and logging. The Controller and Processor agree on how long this Personal Data is to be kept and when the Processor shall no longer keep this data.

Job roles/job groups and their Processing

Table 1 shows the job roles and/or job groups with access to certain Personal Data, followed by the Personal Data processing they are allowed to perform.

You can indicate which staff groups have access to the Personal Data in the table. Some examples are administrators, helpdesk staff, etc. You can also indicate what they can do with this Personal Data: read, edit or delete, for example.

Role (group)	Personal Data (category)	Type of processing

Table 1: Groups of employees and their processing

Security measures taken

<To be completed further>

The Personal Data Protection Act requires Processors to take suitable security measures to protect the Personal Data. See also the explanation with Article 4 of the Processor Agreement.

For more information on suitable security measures, see: Security Measures Guide, Framework of Legal Standards – Annex C:

https://www.surf.nl/kennisbank/2013/juridisch-normenkader-cloud-services-hoger-onderwijs.html

Subcontractors

The Processor needs the Controller's approval to use the following Subcontractors to perform the Service:

Article 3 states that the Controller shall give the Processor its written approval in advance if it wants to engage a Subcontractor. However, paragraph 3 allows the Controller to provide a general approval that includes the Processor's duty to inform the Controller in case of any changes. The general approval can be enclosed as an Annex here.

General approval sample text:

"The Processor engages the Subcontractors below to provide the Service. The general approval of the use of Subcontractors, as referred to in Article 3, paragraph 3 of this Processor Agreement, also applies. The Controller shall be informed of any changes in advance."

Enter the Subcontractors to be engaged by the Processor to provide the Service and state what type of Service the Subcontractor provides here. Management or hosting, for example. Also enter to what extent the Subcontractor has access to the Personal Data.

Finally, state in which country the data is processed. If this country is outside the EEA, it must be established whether that country ensures a suitable security level. For further information, see the additional section under Article 7 of this Processor Agreement.

Organisation name:	**<Name>**
Brief description of the Service:	<Complete>
Personal Data processing scale:	<Complete>
Data processing location/country:	<Complete>

Organisation name:	**<Name>**
Brief description of the Service:	<Complete>
Personal Data processing scale:	<Complete>
Data processing location/country:	<Complete>

Contact details

If you have any questions on this Annex and/or the provided Service, you can contact:

Name:	**<Name> (Supplier)**
Role:	<Complete>
E-mail address:	<Complete>
Telephone number:	<Complete>

Name:	**<Name> (institution)**
Role:	<Complete>
E-mail address:	<Complete>
Telephone number:	<Complete>

To report a Data Breach as referred to in Article 5, please contact:

Enter who the Processor should contact in the event of a possible Data Breach. You can enter a person, but also a general e-mail address, for example; as long as the Processor knows how to report the Data Breach.

Name:	**<Name> (institution)**
Role:	<Complete>
E-mail address:	<Complete>
Telephone number:	<Complete>

Annex B1: <SERVICE NAME>
Information that must be provided in the event of a Data Breach

Version number XX, date of last update: XX-XX-XX

This annex indicates which information the Processor must provide to the Controller in the event of a Data Breach. The questions are based on the data to be entered when the Controller is actually reporting a Data Breach to the Personal Data Authority.
The form for reporting a Data Breach (which this annex is based on) is available on the Personal Data Authority's website:

https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

Unlike Annex A, this annex does not need to be completed further. The annex version number and the name of the Service do need to be entered at the top of the annex.

If the Processor must inform the Controller pursuant to Article 5, it shall provide the following data:

Reporter contact details
Name, role, e-mail address, telephone number

Information on the Data Breach
- Provide a summary of the incident causing the Personal Data security breach.
- How many individuals have Personal Data that is involved in the breach? (Enter the number.)
  a) At least: (Complete)
  b) At most: (Complete)
- Describe the group of people whose Personal Data is involved in the breach.
- When did the breach take place? (Choose one of the following options and complete where necessary.)
  a) On (date)
  b) Between (period start date) and (period end date)
  c) Not known yet
- What type of breach is it? (You can tick several possibilities.)
  a) Reading (confidentiality)
  b) Copying
  c) Alteration (integrity)
  d) Removal or destruction (availability)
  e) Theft
  f) Not known yet
- What type of Personal Data is involved? (You can tick several possibilities.)
  a) Name, address and city
  b) Telephone numbers
  c) E-mail addresses or other addresses for electronic communication
  d) Access or identification data (such as login names, passwords or customer numbers)
  e) Financial information (for example account numbers, credit card numbers)
  f) Dutch social security numbers, referred to as citizen service numbers (BSN) or Sofi numbers
  g) Passport copies or copies of other proof of identity
  h) Gender, date of birth and/or age
  i) Sensitive Personal Data (such as race, ethnicity, criminal information, political beliefs, trade union membership, religion, sex life, medical information)

j) Other data: (Complete)

- Which consequences may the breach have on the Data Subjects' private lives? (You can tick several possibilities.)
  a) Stigma or exclusion
  b) Damage to health
  c) Exposure to (identity) fraud
  d) Exposure to spam or phishing
  e) Other: (Complete)

Further action following the Data Breach

- Which technical and organisational measures has your organisation taken to address the breach and to prevent further breaches?

Technical protection measures

- Is the Personal Data encrypted, hashed or made inaccessible or incomprehensible to unauthorised users in another way? (Choose one of the following options and complete where necessary.)
  a) Yes
  b) No
  c) Partly, i.e.: (Complete)
- If the Personal Data has been made partly or entirely incomprehensible or inaccessible, how did this happen? (Please answer this question if you chose options a or c in response to the previous question. If you used encryption, please also explain the encryption method.)

International aspects

- Is the breach related to persons in other EU countries? (Choose one of the following options.)
  a) Yes
  b) No
  c) Not known yet