Instructions regarding the RU Model Processing Agreement

Radboud Universiteit

Radboud University

Colophon

These are the instructions and explanations regarding version 3-0 of the instruction regarding the Model Processing Agreement from the Radboud University. This version is derived from the SURF Model PROCESSING AGREEMENT April 2019 (version 3.0) and the 'Instructie (conceptversie april 2019) van Surf'. SURF is a Legal Framework of standards for cloud at other services. The following changes has been made in the associated AGREEMENT by the Radboud University:

- The logo of SURF has been replaced by the logo of the Radboud University;
- Address information is filled in (where known).
- An index has been added;
- An end date of the concerning agreement on page 4 has been added;
- A reference has been made to the privacy statement of the Radboud University in article 3.2.3;
- Article 10 has been changed;
- The word "email'' has been used instead of "e-mail";
- The name of the controller has been prefilled on page 13;
- The contact details of the Controller in case of a data breach have been filled in in Annex A;
- The version number, month and year are prefilled in Annex A and B;
- The options for the frequency of performing an audit have been added in Annex A.

Moreelsepark 48
3511 EP Utrecht, the Netherlands
Postbus 19035
3501 DA Utrecht, the Netherlands
+31 88 - 787 30 00
info@surf.nl www.surf.nl

Introduction

This is an instruction and explanation that forms part of the Model Data Processing Agreement, version 3.0 (April 2019), which is part of the Legal Standards Framework for SURF (Cloud) Services.

This is a data processing agreement specifically focused on the processing of personal details. Therefore, this agreement only contains provisions in relation to personal details.

Broader topics are generally included in the main agreement. These include intellectual property (for instance data that are not personal details) and confidentiality (data that are not personal details can be confidential, for instance company sensitive information). Standard provisions for the regulation of these topics in the main agreement can be found in the memorandum of the Legal Standards Framework for SURF (Cloud) Services.

This document will be developed further and regular updates will be published to better match the target group requirements. The document offers support for the use of the data processing agreement. However, you should always consult with a (legal) advisor in your organisation if you have questions or uncertainty.

Index

Reading guide

In this document, by means of boxes such as these, some provisions are explained why these are important and how it should be read. There is also a reference made to laws and regulations on which the provision is based or on which the provision has an effect. Besides, this document also contains an instruction to help you complete Annex A.

In this document is referred to the following laws, regulations, documentation and websites:

The General Data Protection Regulation (GDPR)
The GDPR is an European regulation that is directly applicable in all EU member states as of May 25 2018.

The Dutch implementing law General Data Protection Regulation
This law is the implementation of the GDPR in the Netherlands.

Manual General Data Protection Regulation and the Implementing law General Data Protection Regulation
On the 22nd of January of 2018, the Ministry of Justice and Safety has published a manual to explain the most important provision of the GDPR and the Implementing law GDPR. This manual replaces the old 'Manual Wbp'.

GÉANT Data Protection Code of Conduct
A determined European Code of conduct by GÉANT, that solely Service Providers can sign, to show that they comply with the European safety- and privacylaws:
https://geant3plus.archive.geant.net/uri/dataprotectioncode-of-conduct/V1/Documents/GEANT_DP_CoC_ver1.0.pdf.

Guidelines Data breach reporting obligation
Guidelines for reporting a data breach, published by the Article 29 Working group. The guidelines can be found on the website of the Dutch Data Protection Authority:
https://autoriteitpersoonsgegevens.nl/en/news/data-breach-notification-obligation

Website of the Dutch Data Protection Authority
References to news items and explanation of regulations.

Security measures guide, Annex C Legal Standards
Guide for the implementation of an appropriate security level, associated with the SURF Legal Standards (Cloud)services. Version of October 2016. The document can be found on the website of SURF:
https://www.surf.nl/files/2019-03/surf_c-guidelines-for-security-measures-english-october-2016.pdf

Guide for the Audit obligation, Annex D Legal Standards
A guide for the implementation of the audit obligation in a processer agreement, associated with the SURF Legal Standards (Cloud)services. Version of October 2016. The document can be found on the website of SURF:
https://www.surf.nl/files/2019-03/surf_d-guidelines-for-audit-obligations-english-october-2016.pdfhtml

THE UNDERSIGNED:

Stichting Katholieke Universiteit, with its registered office at Geert Grooteplein-Noord 9, 6525 EZ Nijmegen, more particularly: **Radboud University** (hereinafter **RU**) with its registered office at Houtlaan 4, 6525 XZ Nijmegen (Postal address Mailbox 9102, 6500 HC Nijmegen), Chamber of Commerce number 41055629, more particularly [NAME FACULTY/INSTITUTE], with its registered office at [ADDRESS FACULTY/INSTITUTE],and legally represented by **<REPRESENTATIVE>** (hereinafter referred to as: "**RU**" and "**the Controller**");

And

<NAME OF SUPPLIER>, with its registered office at <ADDRESS> in <TOWN/CITY>, Chamber of Commerce
number <CoC No.> and legally represented by **<REPRESENTATIVE>** (hereinafter referred to as: "**the Processor**');

Hereinafter jointly referred to as: "**the Parties**" and individually as "**the Party**";

WHEREAS:

• On <DATE> the Parties concluded an Agreement and have set the following <END DATE> of this agreement and with reference <AGREEMENT REFERENCE> concerning <SUBJECT OF THE AGREEMENT>. For the purpose of the performance of the Agreement, the Processor processes Personal Data on behalf of the Controller;

• In the context of the performance of the Agreement, <NAME SUPPLIER> is to be regarded as the Processor within the meaning of the GDPR and <NAME SETTING> is to be regarded as the Controller within the meaning of the GDPR;

In the context of the data processing agreement, it is explicitly stipulated that, insofar as the supplier processes personal data for the institution, the institution is the data controller and the supplier is the processor within the meaning of the GDPR. By stating this explicitly, it is clear which rights and obligations of the GDPR are applicable to the institution and the supplier.

In the GDPR, the “data controller” is defined as the natural or legal entity that determines the purpose (“why”) and the means (“how”) of the processing. The “data processor” is defined as the natural or legal entity that processes the personal details on behalf of the controller.

Laws and regulations:
- Article 4 paragraph 8 of the GDPR

• The parties wish to handle the Personal Data that is or will be processed in the performance of the Agreement with due care and in accordance with the GDPR and other applicable laws and regulations concerning the Processing of Personal Data;

• In accordance with the GDPR and other applicable laws and regulations concerning the Processing of
Personal Data, the Parties wish to set out their rights and obligations with regard to the Processing of Personal Data of Data Subjects In Writing in this Processing Agreement.

Parties are obliged to lay down the processing of personal data by processor in an agreement or other legal act.

Laws and regulations:

- Article 28 paragraph 3 of the GDPR

AND HAVE AGREED AS FOLLOWS:

ARTICLE 1. DEFINITIONS

In this Processing Agreement, capitalised terms have the meaning given in this Article. Where the definition in this Article is given in the singular, it shall also include the plural and vice versa, unless expressly stated otherwise or the context dictates otherwise. If a term written with a capital letter is not included in this Article, this term will be given the meaning of the definition set out in Article 4 of the GDPR.

1.1 GDPR: regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

1.2 Annex: an annex to this the Processing Agreement, which forms an integral part of this Processing Agreement.

1.3 Service: the service or services to be provided by the Processor to the Controller on the basis of the Agreement.

1.4 DPIA: the data protection impact assessment carried out prior to the Processing with regard to the impact of the envisaged processing activities on the protection of Personal Data, as referred to in Article 35 of the GDPR.

1.5 Employee: the employees engaged by the Processor and other persons, not being Sub-Processors, whose activities fall under the responsibility of and who are engaged by the Processor in the performance of the Agreement.

1.6 Agreement: the agreement concluded between the Controller and the Processor on the basis of which the Processor processes Personal Data on behalf of the Controller for the purposes of the performance of this agreement.

1.7 In Writing/Written: in writing or electronically, as referred to in Book 6, Article 227a of the Dutch Civil Code.

1.8 Sub-processor: another processor, including but not limited to group companies, sister companies, subsidiaries and auxiliary suppliers, engaged by the Processor to perform specific processing activities at the expense of the Controller.

1.9 Processing agreement: this agreement including Annexes, as referred to in Article 28, paragraph 3 of the GDPR.

ARTICLE 2. OBJECT OF THE PROCESSING AGREEMENT

2.1 The Processing Agreement forms an addition to the Agreement and supersedes any arrangements previously made between the Parties with regard to the Processing of Personal Data. In the event of any conflict between the provisions of the Processing Agreement and the Agreement, the provisions of the Processing Agreement shall prevail.

Provisions in relation to privacy may have also been included in the main agreement or general conditions. It is wise to align the content of the main agreement with the data processing agreement to avoid contradictions. In case there are contradictions between both agreements, Article 2.1 states that the data processing agreement takes precedence over the main agreement. It is important that other agreements do not contain contradictory precedence ranking.

2.2 The provisions of the Processing Agreement apply to all Processing that takes place in the context of the performance of the Agreement. The Processor shall immediately inform the Controller if the Processor has a reason to believe that the Processor can no longer comply with the Processing Agreement.

2.3 The Controller assigns and instructs the Processor to process the Personal Data on behalf of the Controller.

2.3.1 The instructions of the Controller have been described in more detail in the Processing Agreement and the Agreement. The Controller may give reasonable additional or different instructions In Writing.

All provisions from the data processing agreement are only applicable to the processing of personal details in the context of the service.

As the data controller, the institution has an obligation under the GDPR to ensure that the supplier is able to comply with their obligations stipulated in the GDPR. Therefore, it is important that the supplier immediately notifies the institution if there is any doubt in relation to the supplier's ability to comply with the data processing agreement.

Laws and regulations:
- Article 28 paragraph 1 of the GDPR

2.3.2 The Parties shall record in Annex A which Processing operations the Processor carries out on the instructions of the Controller. The Processor is exclusively authorised to carry out the Processing specified in Annex A.

The supplier can only process the data as specified in this data processing agreement. Appendix A specifies the nature of the processing, the purposes of the processing, the categories of personal details, the categories of data subjects, the frequency of the audits to be performed, and the retention period of the personal details.

Data minimisation plays a role in the categories of personal details: no other personal details will be processed than those that are necessary for the provision of the service.

Laws and regulations:
- Article 28 paragraph 3, under a of the GDPR

2.3.3 Notwithstanding Articles 8 and 9, the Processor shall process the Personal Data exclusively on the orders of the Controller and on the basis of the instructions of the Controller as referred to in Articles 2.3.1 and 2.3.2. The Processor shall only process the Personal Data to the extent that the Processing is necessary for the performance of the Agreement, never for its own benefit, for the benefit of Third Parties and/or for advertising and/or other purposes, as the case may be, unless a provision of EU law or Member State law applicable to the Processor obliges the Processor to

Process. In that case, the Processor shall notify the Controller In Writing of this provision prior to Processing, unless such legislation prohibits such notification for important reasons of public interest.

The supplier is only allowed to process data based on written authorisation from the institution. Practically this means that the supplier can only process the personal details of the institution insofar as it is necessary to supply the service to the institution. The supplier is not allowed to use the personal details for their own purposes (such as advertising). The purpose of the processing is determined by the institution and is stipulated in Appendix A of the data processing agreement.

Laws and regulations:
- Article 28 paragraph 3, under a and article 29 of the GDPR

2.4 The Processor and the Controller shall comply with the GDPR and other applicable laws and regulations regarding the Processing of Personal Data. The Processor shall immediately notify the Controller if, in the opinion of the Processor, an instruction from the Controller constitutes a breach of the GDPR and/or other applicable laws and regulations concerning the Processing of Personal Data.

The GDPR stipulates separate obligations for both the data controller and the processor. According to the GDPR, the supplier needs to notify the institution immediately if they are of the opinion that an instruction received from the institution contravenes the GDPR and/or other applicable laws and regulations.

Laws and regulations:
- Article 28 paragraph 3 (second part) of the GDPR

2.5 If the Processor determines the purpose and means of the Processing of Personal Data in violation of the Processing Agreement and/or the GDPR and/or other applicable laws and regulations concerning the Processing of Personal Data, the Processor shall be deemed to be the Controller for such Processing.

The purpose and the means of the processing need to be determined by the institution. The role of the supplier is to process the personal details on behalf of the institution and to stay within their remit as specified by the institution. In instances in which the supplier independently determines the purpose or means of the processing, they become the data controller for that processing. They then need to independently comply with all obligations as stated in the GDPR.

Laws and regulations:
- Article 28 paragraph 10 of the GDPR

ARTICLE 3. PROVISION OF ASSISTANCE AND COOPERATION

3.1 The Processor shall provide the Controller with all necessary assistance and cooperation in enforcing the obligations of the Parties under the GDPR and other applicable laws and regulations concerning the Processing of Personal Data. To the extent that such assistance relates to the

Processing of Personal Data for the purpose of the performance of the Agreement, the Processor shall in any event provide the Controller with such assistance relating to:

(i) The security of Personal Data;

(ii) Performing checks and audits;

(iii) Performing DPIAs;

(iv) Prior consultation with the Supervisory Authority;

(v) Responding to requests from the Supervisory Authority or another government body;

(vi) Responding to requests from Data Subjects;

(vii) Reporting Personal Data Breaches.

The purpose and the means of the processing need to be determined by the institution. The role of the supplier is to process the personal details on behalf of the institution and to stay within their remit as specified by the institution. In instances in which the supplier independently determines the purpose or means of the processing, they become the data controller for that processing. They then need to independently comply with all obligations as stated in the GDPR.

Laws and regulations:

- Article 28 paragraph 10 of the GDPR

3.2 The provision of assistance and cooperation with regard to meeting the requests from Data Subjects will in any event include, but is not limited to, the following obligations on the part of the Processor:

3.2.1 The Processor shall take all reasonable measures to ensure that the data subject can exercise his rights.

Under the GDPR, data-subjects have certain rights:

- The right to information (article 13 and 14 GDPR)
- The right to access (article 15 GDPR)
- The right to rectification (article 16 GDPR)
- The right to erasure; 'the right to be forgotten' (article 17 GDPR)
- The right to restriction of processing (article 18 GDPR)
- The right to data-portability (article 20 GDPR)
- The right to object (article 21 GDPR)
- The right to not be subjected to automated individual decision making, including profiling (article 22 GDPR).

In order to protect the rights and personal data of data subjects, the supplier is not permitted to respond to requests from data subjects. Such requests must first be checked for legitimacy by the institution. In exceptional circumstances, the institution can provide different instructions to the supplier.

The relevant rights of the data subjects can be found in Articles 13 through 22 of the GDPR.

Laws and regulations:
- Article 12 paragraph 2 of the GDPR

When a data subject submits such a request to the institution, the assistance of the supplier will often be required to comply with the request. According to the GDPR, the data processing agreement needs to include the obligation of the processor to assist in the execution of these rights.

However, in the context of scientific research, statistics, and archiving purposes for the public interest, the rights of data subjects have a limited application. If the institution has implemented the necessary safeguards to ensure that the personal details can only be used for statistical or scientific purposes, or that the processing of personal details forms part of an archive, then Articles 15, 16, and 18 of the GDPR need not apply.

Laws and regulations:
- Article 28 paragraph 3 under e of the GDPR
- Implementation Act Article 44 and 45 Article 89 of the GDPR

3.2.2 If a Data Subject contacts the Processor directly with regard to exercising his rights, the Processor – unless explicitly instructed otherwise by the Controller - will not (substantively) respond to this, but will immediately inform the Controller and request further instructions.

3.2.3 If the Processor offers the Service directly to the Data Subject, the Processor is obliged to inform the Data Subject on behalf of the Controller about the Processing of the Personal Data of the Data Subject in a manner that is in accordance with the rights of the Data Subject. When informing Data Subjects, the Processor refers to the Controller's privacy statement, which can be found on: https://www.ru.nl/english/vaste-onderdelen/privacy-statement-radboud-university/

Article 3.2.3 does not directly follow from the GDPR, but is added to the data processing agreement to connect with the "GÉANT Data Protection Code of Conduct". This is a European Code of Conduct, developed by GÉANT, that can be signed by Service Providers to indicate that they are in compliance with the strict European security and privacy laws. That Code of Conduct includes a similar provision as formulated in Article 3.2.3. However, Article 3.2.3 explicitly states that such an obligation to inform the data subject can only be requested by the institution. This obligation does not supersede the obligations which the institution itself has in relation to the GDPR.

In accordance with Articles 12 and 13 of the GDPR, the processor needs to inform the data subject of the processing by way of a privacy declaration. For more transparency it is necessary that the Processor refers to the privacystatement of the Controller.

3.3 The provision of assistance and cooperation with regard to meeting requests from the Supervisory Authority or another government body shall in any case constitute the following obligations for the Processor:

3.3.1 If the Processor receives a request or an order from a Dutch and/or foreign government agency with respect to Personal Data, including but not limited to a request from the Supervisory Authority, the Processor shall inform the Controller immediately, to the extent permitted by law. When handling the

request or order, the Processor shall observe all instructions of the Controller and the Processor shall provide the Controller with all reasonably necessary cooperation.

In case of a cloud service, the data is not retained at the location of the institution. When authorities submit a request for access to information, the institution, as the controller, needs to adequately respond. If the supplier receives a mandatory request or order, the supplier is obliged to inform the institution about this. In this situation, instructions from the institution must be observed, including leaving the handling of the request or order to the institution. As the entity responsible for the (personal) details, the institution must be the point of contact for such requests or orders.

3.3.2 If the Processor is prohibited by law from fulfilling its obligations under Article 3.3.1, the Processor shall represent the reasonable interests of the Controller. This is in all cases understood to mean:

3.3.2.1 The Processor shall have a legal assessment carried out of the extent to which: (i) the Processor is legally obliged to comply with the request or order; and (ii) the Processor is effectively prohibited from complying with its obligations in respect of the Controller under Article 3.3.1.

3.3.2.2 The Processor shall only cooperate with the request or order if the Processor is legally obliged to do so and, where possible, the Processor shall (judicially) object to the request or order or the prohibition to inform the Controller about this or to follow the instructions of the Controller.

3.3.2.3 The Processor shall not provide more Personal Data than is strictly necessary for complying with the request or order.

3.3.2.4 In the event of a transfer within the meaning of Article 8, the Processor shall examine the possibilities of complying with Articles 44 up to and including 46 of the GDPR.

Under certain circumstances, and due to mandatory laws and regulations, it is prohibited for the supplier to comply with clause 3. In those cases, the institution still needs to safeguard the security of the data. This is why the supplier is obliged to perform a number of actions which are normally performed by the institution.

By performing these actions, the security of the personal details is safeguarded as much as possible.

Articles 44 to 46 of the GDPR are in relation to transferring data to third countries. This is only allowed in exceptional cases as described in those articles. See Article 9 of these instructions for a further elaboration of these articles.

ARTICLE 4. ACCESS TO PERSONAL DATA

4.1 The Processor limits access to Personal Data for Employees, Sub-processors, Third Parties and other Recipients of Personal Data to a necessary minimum.

4.2 The Processor shall only provide access to those Employees for whom such access to Personal Data is necessary for the performance of the Agreement. The categories of Employees have been specified in Annex A.

To protect the personal details, the data processing agreement must specify which staff members (officers) or which groups of staff members may perform what processing with regard to the personal details. Processing of data by other staff members than the (groups of) staff members designated in this article is explicitly prohibited. The data processing agreement needs to ensure that these staff members are bound by confidentiality. Staff members are already legally bound to confidentiality by Article 272 of the Criminal Law.

Laws and regulations:
- Article 28 paragraph 3 under b and Article 32 paragraph 4 of the GDPR
- Article 29 of the GDPR

4.3 The Processor shall not provide Sub-processors with access to Personal Data without the prior general or specific Written consent of the Controller. General permission In Writing for engaging Sub-processors has only been granted if this has explicitly been included in Annex A . Specific permission for the use of Sub-processors has only been granted to Sub-processors specified in Annex A.

On the basis of the GDPR, the supplier (processor) cannot engage other sub-processors without prior specific or general written approval of the institution (the data controller):

1. *Specific approval* is focused on a specific sub-processor. If a sub-processor changes, specific approval from the institution will be needed (again) to engage the new sub-processor.
2. In case of *general approval*, there is no need for the institution to request prior written permission for each new sub-processor. However, the institution needs to be informed prior to the engagement of the sub-processors and they have the right to object.

The type of approval can be specified in Appendix A.

Laws and regulations:
- Article 28 paragraph 2 of the GDPR

4.4 The Sub-processors engaged by the Processor in the performance of the Agreement have been listed in Annex A.

Based on the GDPR, it is important that the institution has an overview of the engaged Sub-processors by Processor at all times. In case of an amendment, the overview in Annex A has to adjusted in time, as well for specific as for general approval. This will ensure that Annex A always provides a complete overview of the engaged Sub-processors by Processor.

4.5 The Processor shall inform the Controller in the event of general consent In Writing for engaging Subprocessors no later than three (3) months prior to intended changes regarding the addition, replacement or change of Sub-processors and the amendment to Annex A required as a result of this, In Writing, whereby the Controller shall be given the opportunity to object to these changes In Writing within one (1) month after the Controller has been informed by the Processor of the intended change. The parties will enter into negotiations on this matter.

If the institution does not agree with the engagement of a certain Sub-processor, it has the right to object to this engagement. In the case of an objection, the Processor is not allowed to pursue the intended change. Parties will enter in negotiations to come to a solution. If Parties cannot come to a solution, one of the options is that the Processor agreement is terminated with mutual agreement.

The possibility of objection is needed, because the Controller must at all times be able to supervise the Processing of the Processor.

Laws- and regulations:

- Article 28 paragraph 2 of the GDPR

4.6 The general or specific consent of the Controller for engaging Sub-processors shall not affect the obligations of the Processor arising from the Processing Agreement, including but not limited to Article 8. The Controller may revoke its general or specific Written consent for engaging Sub-processors if the Processor fails to comply or no longer complies with the obligations under the Processing Agreement, the GDPR and/or other applicable laws and regulations regarding the Processing of Personal Data.

4.7 The Processor shall impose the obligations set out in the Processing Agreement on the Sub-processors engaged by the Processor by means of a Written Agreement.

The Processor guarantees that the persons authorised to process the Personal Data and other Recipients of Personal Data have undertaken to observe confidentiality or are bound by an appropriate legal obligation of confidentiality.

Based on the GDPR, the Processor is obliged to make engagements with the Sub-processor about the obligations of processing Personal Data by Agreement or other legal act. These obligations are at least the same as the engagements between Controller and Processor.

Laws and regulations:

- Article 28 paragraph 4 of the GDPR

The Processor Agreement must guarantee that the persons authorized to process Personal Data are bound by confidentiality.

Laws and regulations:

- Article 28 paragraph 3, under b of the GDPR

4.8 At the request of the Controller, the Processor shall provide evidence that the Processor, Sub-processors engaged by the Processor, the persons authorised to process the Personal Data and other Recipients of Personal Data comply with Article 4.7.

Because the institution, as the data controller, has to be able to verify that the processing is completed in accordance with the GDPR, the supplier is obliged to provide a copy of the agreement with the sub-processor and a copy of the engagements about confidentiality in processing the Personal data, without delay at the request of the institution.

Laws and regulations:

- Article 28 paragraph 3 under h and paragraph 4 of the GDPR

4.9 With regard to the Controller, the Processor shall remain fully responsible and fully liable for the fulfilment of the obligations by the (legal or natural) persons engaged by the Processor, including but not limited to Employees and/or Sub-processors and/or Recipients, arising from the GDPR and/or other applicable laws and regulations concerning the Processing of Personal Data and the obligations arising from the Agreement and the Processing Agreement.

The supplier shall remain fully liable to the institution for the fulfilment of the obligations of the engaged sub-processors.

Laws and regulations:
- Article 28 paragraph 4 of the GDPR

ARTICLE 5. SECURITY

5.1 The Processor will take appropriate technical and organisational measures to ensure a level of security appropriate to the risk, so that the Processing meets the requirements of the GDPR and other applicable laws and regulations concerning the Processing of Personal Data and the protection of the rights of Data Subjects is guaranteed. To this end, the Processor shall at least take the technical and organisational measures set out in Annex B.

The supplier, as the processor, has an independent obligation to ensure adequate protection of personal data under the GDPR. In addition, the institution, as the controller, must ensure that suppliers offer adequate guarantees with regard to the application of appropriate technical and organisational measures to ensure that the processing meets the legal requirements and that the protection of the data subject's rights is guaranteed.

With regard to security, the institution must determine, on the basis of a risk analysis, whether the supplier offers sufficient guarantees for the protection of personal details. The requested guarantees need to particularly relate to expertise, integrity, and resources.

More information about appropriate security: see Guidelines Security Measures, Appendix C, Legal Standards:

https://www.surf.nl/binaries/content/assets/surf/nl/2018/jnk-2018/surf_chandreikingbeveiligingsmaatregelen---bijlage-c---versie-mei-2018.pdf.

Laws and regulations:
- Article 28 paragraph 1 and paragraph 3 under c and Article 32 of the GDPR
- Recital no. 81 of the GDPR

5.2 In assessing the appropriate level of security, the Processor shall take into account the state of the art, the cost of implementation, as well as the nature, scope, context and purposes of processing, and the various risks to the rights and freedoms of individuals in terms of probability and seriousness, especially as a result of the destruction, loss, alteration or unauthorised disclosure of or access to data transmitted, stored or otherwise processed, whether accidentally or unlawfully.

The security measures must safeguard an “appropriate level” of security, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the varying likelihood and severity of risk to the rights and freedoms of natural persons.

Additionally, in determining what is considered an “appropriate” level, the emphasis needs to be on processing risks: what can go wrong? It includes both unforeseen processing (“accidental”) as well as processing that is deliberately contrary to the GDPR.

Laws and regulations:
- Article 32 article 1 and 2 of the GDPR.

5.3 The Processor records its security policy In Writing. At the request of the Controller, the Processor shall provide evidence of a Written Security Policy to the Processor.

Since the institution, as the controller, must be able to check whether the personal details are adequately protected, the supplier is obliged to provide written information about data security without delay at the request of the institution.

Laws and regulations:
- Article 28 paragraph 3 under h of the GDPR

ARTICLE 6. AUDIT

6.1 The Processor is obliged to have an independent external expert periodically carry out an audit of the organisation of the Processor in accordance with Article 6.2, in order to demonstrate that the Processor complies with the provisions of the Processing Agreement, the GDPR and other applicable laws and regulations concerning the Processing of Personal Data.

Under the GDPR, the processor has an independent responsibility to implement appropriate technical and organizational measures. A periodical audit (inspection) is an appropriate way for the processor to prove that he meets the legal obligations under the GDPR.

Moreover, the supplier is obliged to cooperate with audits by the institution or an auditor authorized by the institution to verify that it complies with the data processing agreement and more generally the GDPR.

Laws and regulations:

- Article 28 paragraph 3 under c, f, and h and article 32 paragraph 1 of the GDPR.

6.2 The Controller shall lay down the frequency of the periodic audit to be carried out by the Processor, as referred to in Article 6.1, in Annex A.

6.2.1 The Processor shall carry out a periodic audit as referred to in Article 6.1 at least once every two years, unless Article 6.2.2 or 6.2.3 applies.

6.2.2 If Special Categories of Personal Data are processed or a Processing is carried out that involves a high risk to the rights and freedoms of the Data Subjects, the Processor will carry out a periodic audit at least once a year, as referred to in Article 6.1.

6.2.3 If the Processor only carries out processing operations that present a low risk to the rights and freedoms of the Data Subjects, the Processor shall not be obliged to carry out a periodic audit as referred to in Article 6.1.

Depending on the risk class, the service and the security of the supplier must be checked by the institution. This can be accomplished through a periodical inspection by an independent expert. How often the supplier is obliged to perform an audit depends on the type of personal details.

There are three risk classes:

- Risk class Low: this category only includes personal details of which it is generally accepted that, with the intended use, they do not present a risk for the data subject. It could refer to publicly accessible information, but this may not always be the case. It includes, for instance, the name, business e-mail address, or occupation. *No periodical audit obligation.*
- Risk class Medium: this category includes personal details that do not fall into the Risk class "Low" or the category "Special Personal Details". It includes, for instance, the registration of a student, financial information, or location information. *The audit obligation is once every two years.*
- Risk class High: this relates to personal details that fall within the "Special Personal Details" category (GDPR Article 9) which includes information regarding political opinions, personal data revealing racial or ethnic origin, and genetic and biometric data, among other things. Additionally, it includes criminal records and national identity numbers (BSN/education number). It carries an annual audit obligation.

Combining data can influence the risk class of the information. In some cases, combining data can lead to a higher risk class.

Such an investigation must also have taken place prior to signing the agreement to ensure that the institution has investigated the service provided by the supplier.

More information about the audit obligation: see Guidelines Audit Obligation, Appendix D, Legal Standards:

Also see the "Recommendations for a methodology of the assessment of severity of personal data breaches" by Enisa for a further elaboration on the risk classes.

6.3 The Processor shall be obliged to make the findings of the independent, external expert from the periodic audit, on request, available to the Controller in the form of a statement, in which the expert:

(i) gives an opinion on the quality of the technical and organisational security measures taken by the Processor in relation to the Processing performed by the Processor on behalf of the Controller;

(ii) informs the Controller of the other findings relevant to the performance of the Processing Agreement and compliance with the GDPR and other applicable laws and regulations concerning the Processing of Personal Data.

As the data controller, the institution is obliged to ensure adequate security by the supplier. One of the instruments prescribed for this by the Dutch Data Protection Authority is a statement from an independent external expert: a Third Party Memorandum (TPM). A TPM is a statement in which an independent external expert provides an opinion about the measures implemented by the supplier. The TPM is drafted at the request of the supplier and is provided to the institution that uses the supplier's services. The purpose of the TPM is to offer the institution insight into the measures implemented by the supplier, without the need for every institution to instigate their own investigation.

6.4 At its request, the Controller is entitled to have an audit carried out by an expert authorised by the Controller with regard to the Processor's organisation, in order to demonstrate that the Processor complies with the provisions of the Processing Agreement, the GDPR and other applicable laws and regulations concerning the Processing of Personal Data. The Controller may, no more than once a year, exercise the right to have an audit carried out at the Processor, as referred to in this paragraph, or more often in the event of a concrete suspicion that the Processor is in breach of the Processing Agreement and/or the GDPR and/or other applicable laws and regulations regarding the Processing of Personal Data. The Controller shall notify the Processor In Writing at least 14 (fourteen) days before the start of the audit. The audit must not unreasonably interfere with the normal business activities of the Processor.

6.5 The costs of the periodic audit are borne by the Processor. The costs of the audit at the request of the Controller are borne by the Controller, unless the findings of the audit show that the Processor has failed to comply with the provisions of the Processing Agreement and/or the GDPR and/or other applicable laws and regulations concerning the Processing of Personal Data.

Under the GDPR, the supplier is obliged to cooperate with audits by the institution or an auditor authorised by the institution to verify that it complies with the data processing agreement and more generally the GDPR.

Laws and regulations:
- Article 28 paragraph 3 under h of the GDPR

When the institution has a reasonable suspect that the supplier does not comply with the provisions, the institution has to investigate this suspect. This involves a (limited) quality assessment. The execution of this investigation is initially funded by the institution itself. If the investigation shows that the supplier indeed breached the agreements made, then the institution can recover the costs of the investigation from the supplier.

The costs of the periodic audit from article 6.1 of the Processor Agreement are for the supplier's account.

6.6 If it is established during an audit that the Processor is not complying with the provisions of the Processing Agreement and/or the GDPR and/or other applicable laws and regulations concerning the Processing of Personal Data, the Processor shall immediately take all reasonably necessary measures to ensure the compliance of the Processor. The associated costs shall be borne by the Processor.

ARTICLE 7. PERSONAL DATA BREACH

7.1 The Processor shall inform the Controller of a Personal Data Breach without unreasonable delay and within 24 hours at the latest. The Processor shall inform the Controller via the contact person and the contact details of the Controller as included in Annex A and at least with regard to all information as it appears from the most recent Data Breaches form of the Dutch Data Protection Authority, which can be found on the website of the Data Protection Authority. The Processor warrants that the information provided, to the best of the Processor's knowledge at that time, is complete, correct, and accurate.

According to the GDPR, the institution has to report data breaches that fall under the reporting obligation to the Dutch Data Protection Authority within 72 hours. This includes data breaches that take place at suppliers or sub-processors of suppliers. Since it is the responsibility of the institution to determine whether a particular data breach needs to be reported or not, it is important that the supplier reports all breaches or reasonable suspicions thereof.

Therefore, the institution must be informed in good time of a potential data breach in order to be able to assess whether or not to report. This is why this article specifies that the supplier must report the data breach to the institution within 24 hours after discovery. This includes data breaches at any sub-processors involved. For this reason, the supplier also has an obligation to also make agreements with sub-processors regarding the data breach reporting obligation. Because the chain of involved parties is longer in this situation, the sub-processors must immediately report the data breach to the supplier in order to ensure that it is possible for the institution to report the breach to the Dutch Data Protection Authority within 72 hours.

In Appendix A, you can indicate the person or department of the institution to which the supplier must report the potential data breach.

Laws and regulations:

- Article 28 paragraph 3 under f and Article 33 of the GDPR
- Policy regulations for the application of Article 34a of the Wpb (Dutch Data Protection Act), Dutch Data Protection Authority, December 2015.

7.2 If and to the extent that it is not possible for the Processor to provide all information from the data breaches form of the Data Protection Authority simultaneously, the information may be provided to the Controller in stages, without unreasonable delay and in accordance with Article 7.1.

Laws and regulations:

- Article 33 clause 4 of the GDPR

7.3 The Processor has adequate policies and procedures in place to ensure that it can:

(i) Detect Personal Data Breaches at the earliest possible stage;

(ii) Inform the Controller of any Personal Data Breach in accordance with Article 7.1;

(iii) Respond adequately and promptly to any Personal Data Breach;

(iv) Prevent or limit any further unauthorised disclosure, alteration and provision or otherwise unlawful processing and prevent its recurrence.

At the request of the Controller, the Processor shall provide information on and access to this policy drawn up

by the Processor and these procedures drawn up by the Processor.

7.4 The Processor shall keep a Written register of all Personal Data Breaches that relate to or are connected with the Agreement or its performance, including the facts concerning the Personal Data Breach, its implications, and the corrective measures taken. At the request of the Controller, the Processor shall provide the Controller with a copy of this register.

Based on the GDPR, the institution has an obligation to keep a register of every data breach, whether or not the breach carries a reporting obligation. The supplier has a legal obligation to assist the institution in this. This means that the supplier also needs to keep such a register and provide it to the institution at the request of the institution.

Laws and regulations:
- Article 33 paragraph 5 and Article 28 paragraph 3 under f of the GDPR

7.5 The Processor will refrain from reporting Personal Data Breaches to the Supervisory Authority and/or the affected Data Subjects, unless expressly requested to do so In Writing by the Controller.

Based on the GDPR, the institution, as Controller, is in case of a Data Breach, the one that has to make the consideration if there is a high risk for rights and freedoms of data subjects and if there is a need to inform the Supervisory Authority and/or the data subjects. It is not the intention that the supplier makes this consideration.

Laws and regulations:
- Article 33 and 34 of the GDPR

ARTICLE 8. TRANSFER OF PERSONAL DATA

8.1 Personal data may only be transferred to countries outside the European Economic Area or international organisations if there is an adequate level of protection, Articles 44 to 49 of the GDPR are complied with, and the Controller has given specific Written consent to do so. This specific Written consent has only been granted if it has been included in Annex A.

In relation to the GDPR, the data processing agreement needs to include provisions regarding transferring personal details to third countries.

Under the GDPR, processing personal details in third countries is only allowed in three situations: A third country means every county outside the EEA (European Economic Area: all countries of the EU and Norway, Liechtenstein, and Iceland).

The three possibilities for transfer of personal details outside the EEA are:
1. If the country is designated by the European Commission as a country with an adequate level of protection (Article 45 of the GDPR). This list can be found at:

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

Processing of Personal Data in the US: the US is only considered an adequate country if personal data are only passed on to companies that have a so-called Privacy Shield. [1] More about processing in the US and the current state of affairs regarding the Privacy Shield can be found on the website of the Dutch Data Protection Authority:

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

2. In case of "appropriate safeguards" or Binding Corporate Rules (Article 46 and 47 of the GDPR). These measures are:
- Binding Corporate Rules;
- Model Contract of the European Commission;
- Model Contract of the Dutch Data Protection Authority;
- A self-drafted agreement that is approved by the Dutch Data Protection Authority;
- Code of Conduct;
- Certification.

3. In case of one of the specific situations from Article 49 clause 1 of the GDPR. They are:
- Explicit consent has been received from the data subject;
- The transfer is necessary for the performance or implementation of an agreement (restrictive interpretation);
- The transfer is necessary for important reasons of public interest;
- The transfer is necessary for the establishment, exercise or defence of legal claims;
- The transfer is necessary in order to protect the vital interests of a person;
- The transfer is necessary for a register designated by law;
- The so-called "incidental transfer" described in Article 49 clause 1 sub g) of the GDPR.

Laws and regulations:
Article 28 paragraph 3 under a and article 44 through 50 of the GDPR

8.2 At the request of the Controller, the Processor shall demonstrate that the requirements laid down in Article 8.1 have been met.

8.3 The transfers of Personal Data outside the European Economic Area or to international organisations for the purpose of implementing the Agreement are further described in Annex A. The Processor is authorised to make such transfers to third countries or international organisations specified in Annex A only, unless a provision of Union or Member State law applicable to the Processor obliges the Processor to Process. In that case, the Processor shall notify the Controller In Writing of this provision prior to Processing, unless such legislation prohibits such notification for important reasons of public interest.

ARTICLE 9. CONFIDENTIALITY OF PERSONAL DATA

9.1 All Personal Data is classified as confidential data and must be treated as such.

9.2 The Parties shall keep all Personal Data confidential and shall not further disclose it internally or externally in any way, except insofar as:

(i) Disclosure and/or providing of the Personal Data is necessary in the context of the performance of the Agreement or the Processing Agreement;

(ii) Any rule of mandatory Union or Member State law or a judicial decision of a competent court based on this requires the Parties to disclose, provide and/or transfer such Personal Data, with the Parties taking into account the provisions of Article 3;

(iii) Disclosure and/or providing of such Personal Data takes place with the prior Written consent of the other Party.

Although confidentiality extends beyond personal details (for example, business-sensitive data can also be confidential), this Model Data Processing Agreement also includes a confidentiality provision for completeness. In addition, the Dutch Data Protection Authority has indicated in a news release from May 2016 that a confidentiality obligation must be part of a data processing agreement.

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

- Directive on the protection of non-public know-how and company information against unlawful acquisition, use and disclosure (Pb EU 2016, L157) and (the proposal for) the Dutch Protection of Trade Secrets Act .

ARTICLE 10. LIABILITY

10.1 The Processor is liable for all damage ensuing from or in connection with the failure to comply with the Processor Agreement and/or the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data.

10.2 A Party may not invoke a limitation of liability provided for in the Agreement or any other agreement or arrangement existing between the Parties in respect of:

a. an action for recourse, brought by the other Party under Article 82 of the GDPR; or

b. an action for damages, brought by the other Party under the Processing Agreement, if and to the extent that the action consists of the recovery of a fine paid to the Supervisory Authority that is wholly or partly attributable to the other Party.

The provisions of this Article are without prejudice to the remedies available to the Party addressed under the applicable laws or regulations.

10.3 Each Party is obliged to inform the other Party without undue delay of any (possible) liability claim or the (possible) imposition of a fine by the Supervisory Authority, both in connection with the Processing Agreement. Each Party is obliged in all reasonableness to provide the other Party with information and/or support for the purpose of putting up a defence against a (possible) liability claim or fine as referred to in the previous sentence. The Party providing information and/or support is entitled to charge any reasonable costs in this respect to the other Party; the Parties shall inform each other as much as possible in advance of these costs.

Based on the Dutch Civil Code, a party that fails to comply with an agreement, is liable for the damage that ensues. In two specific cases it is not possible for a party to invoke any limitation of liability contained in the Main agreement with respect to:

1. A recourse action based on article 82 of the GDPR
2. A damage action under the Processor Agreement, if and insofar as the action consists of recovery of a fine paid to the Supervisory Authority that is wholly or partially attributable to the other party.

Article 82, paragraph 1, 2 and 4 of the GDPR determine that the data subject has the right to address as well the Controller as the Processor for possible damages, regardless of the fact who carries the blame. Paragraph 5 of article 82 GDPR introduces the possibility of a mutual redress between supplier and the institution.

Besides, it is important that the supplier has an adequate insurance. Insurances can vary widely and not all insurances are appropriate for Cloud suppliers. When assessing the supplier's insurance, it is important to pay attention to the following points:

- The amount of coverage
- What is covered by the insurance and what is excluded from coverage.

Laws and regulations:
- Article 28 paragraph 4 of the GDPR
- Article 82 paragraph 1, 2 and 4 of the GDPR

ARTICLE 11. AMENDMENTS

11.1 the Processor is obliged to immediately inform the Controller of intended changes to the Service, the execution of the Agreement and the execution of the Processing Agreement that relate to the Processing of Personal Data and that (may) require a change to the Processing Agreement and/or the Annexes. This is in all cases understood to mean (but not limited to):

(i) Changes that (may) affect the (categories of) Personal Data to be processed;

(ii) Changes in the means by which Personal Data is processed;

(iii) Engaging other Sub-processors;

(iv) Change in the transfer of Personal Data.

11.2 The Processor is only authorised to make a change to the Service, a change in the performance of the Agreement, a change in the performance of the Processing Agreement and/or a change that results in an amendment to Annex A or Annex B if the Controller has given prior Written consent for these change(s). A change to the Service is understood to mean a substantial change that may have implications for the Processing of Personal Data. Contrary to the foregoing, the Processor may, without the prior Written consent of the Controller, immediately implement necessary improvements, for example with regard to adequate security of the service. The Processor shall inform the Controller of the change as soon as possible.

In order to be able to perform the tasks of the data controller, the institution must ensure that personal data are processed in accordance with the predetermined level of risk. If the processing (the supplier's services) changes, the institution must be able to check prior to the change whether the processing still takes place at the appropriate level. The information obligation of this article has been included for this purpose.

Laws and regulations:
- Article 28 paragraph 1 of the GDPR

11.3 Changes relating to the Processing of Personal Data may never result in the Controller being unable to comply with the GDPR and/or other applicable laws and regulations regarding the Processing of Personal Data.

11.4 In the event of nullity or voidability of one or more provisions of the Processing Agreement, the other provisions shall remain in full force and effect.

ARTICLE 12. DURATION AND TERMINATION

12.1 The duration of the Processing Agreement is equal to the duration of the Agreement. The Processing Agreement cannot be terminated separately from the Agreement. Upon termination of the Agreement, the Processing Agreement ends by operation of law and vice versa.

Note: this provision links the duration of the agreement and the duration of the data processing agreement. Upon termination of the agreement, the data processing agreement also automatically terminates and vice versa.

In some cases this will not be desirable, for example if the agreement has a wider scope than the data processing agreement. In that case, it is advisable to agree on a separate duration of the data processing agreement.

12.2 The Controller is entitled to dissolve the Processing Agreement if the Processor fails to comply or can no longer comply with the Processing Agreement and/or the GDPR and/or other applicable laws and regulations concerning the Processing of Personal Data and the Processor is in default, without the Processor being entitled to claim any compensation. In the event of dissolution, the Controller shall observe a reasonable notice period, unless the circumstances justify immediate dissolution.

12.3 Within one (1) month after the end of the Agreement, the Processor shall destroy and/or return all Personal Data and/or transfer it to the Controller and/or another party to be designated by the Controller, at the discretion of the Controller. All existing (other) copies of Personal Data, whether or not held by legal entities or natural persons engaged by the Processor, including but not limited to Employees and/or Subprocessors, will demonstrably permanently be deleted, unless storage of the Personal Data is required under Union or Member State law.

When terminating the agreement, the GDPR stipulates two options:

1. the (personal) data that has been processed will be destroyed by the supplier; or
2. the (personal) data that has been processed will be returned to the institution by the supplier and existing copies will be destroyed.

The institution makes the choice. Any other option offers insufficient protection for the (personal) details. An exception applies if the supplier is required by law to store certain personal details.

Laws and regulations:
- Article 28 paragraph 3 under g of the GDPR

12.4 The Processor shall, at the request of the Controller, confirm In Writing that the Processor has fulfilled all obligations under Article 12.3.

12.5 The Processor shall bear the costs of destruction, return and/or transfer of the Personal Data. The Controller may impose further requirements on the manner of destruction, return and/or transfer of

the Personal Data, including requirements on the file format. The transfer of Personal Data is based on an open file format. The Parties will agree in joint consultation on a reasonable distribution of any additional costs for the further requirements.

12.6 Obligations under the Processing Agreement which by their nature are intended to continue after termination of the Processing Agreement shall continue after termination of the Processing Agreement.

ARTICLE 13. APPLICABLE LAW AND DISPUTE RESOLUTION

13.1 The Processing Agreement and its performance are governed by Dutch law.

13.2 All disputes arising between the Parties in connection with the Processing Agreement shall be submitted to the competent court in the place where the Controller has its registered office.

THUS AGREED BY THE PARTIES:

Radboud University	**<NAME OF THE PROCESSOR>**
_____/_____/_____ *Date*	_____/_____/_____ *Date*
_____ *Name*	_____ *Name*
_____ *Signature*	_____ *Signature*

Annex A: Specification of the Processing of Personal Data

Version number 3.0-RU, Date of latest amendment: july 2019
Note: If the Processor offers several (optional) Services to the Controller, it is possible to include the information in separate Annexes, which are numbered as follows: "Annex A1', 'Annex A2', etc. These Annexes are to be attached to the Processing Agreement.

See the infographic "The GDPR in a nutshell" that has been published by the Dutch Data Protection Authority as a practical tool for completing this appendix. *Laws and regulations:* - Article 28 paragraph 3 and 9 of the GDPR

Description of the Processing

Include the name of the service here. For instance: “payroll”.
Purposes of the Objectives *(to be completed by the Controller)*

Here, write the purpose of the processing as concretely as possible. This includes the processing of applications, personnel administration, salary administration, pensions, or the registration of enrolment fees for an educational institution.
Categories of Data Subjects *(to be completed by the Controller)*

A data subject is the person to whom the personal details relate. Different categories can be applicable. This includes students, staff members, or contact persons, for instance.
Categories of Personal Data *(to be completed by the Controller)*

It is at your own discretion as to how the specified personal details are recorded. It has to be clear to everyone what personal data are included. For instance, name, address, phone number, but also log data or exam results. View all personal details that are available in that service. More about personal details can be found on the website of the Dutch Data Protection Authority: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens

Frequency of audits *(to be completed by the Controller)*
☐ Annually ☐ every two years ☐ other: ☐ N / A because:

The frequency of the audit is dependent on the type of personal data that are processed. See the elaboration in Article 7 of the data processing agreement.
Retention period of the Personal Data or the criteria for determining this *(only complete if applicable)* *(to be completed by the Controller)*

An important starting point of the GDPR is “limited storage”. This means that personal details are not stored any longer than necessary for the processing. Some personal data are processed as long as the service is purchased. In such cases, agreements are made about transferring or deleting the data as soon as the service is no longer used. But there are also personal details for which it is not necessary to keep storing them continually during the use of the service. This includes storage of back-ups and logging. The institution and the supplier will agree on how long these personal details will be stored. *Laws and regulations:* - Article 5 paragraph 1 under e of the GDPR

Categories of Employees

Categories of Employees (job roles/job categories) of the Processor who Process Personal Data	Categories of Personal Data processed by Employees	Type of Processing	Country of Processing

The table above answers the following points:

- The groups of staff members which can access personal details. These include administrators, helpdesk staff, etc.
- The type of personal data concerned.
- What staff members can do with the personal details (the type of processing): for instance read, change, or remove.
- And the country where the processing takes place.

Sub-processors

The Controller has given the Processor [*to be checked as applicable by the Controller*]:

□ General permission to engage Sub-processors.
□ Specific permission to engage the following Sub-Processors *(to be completed by the Controller)*:

The Sub-processors engaged by the Processor are:

Sub-processor engaged by the Processor for the Processing of Personal Data	Categories of Personal Data processed by Sub-processor	Type of Processing	Country of Processing	Country where Sub-processor's registered office is located

Article 4.3 of the data processing agreement indicates that the institution needs to provide prior written permission to the supplier if they want to engage a sub-processor. This can be either a general or a specific permission. Check which one is applicable above.

In case of specific permission, the above table needs to be completed. The following questions are answered there:

- Which sub-processors (assistant suppliers) the supplier will engage in the performance of a service.
- The personal details to which the sub-processor will gain access.
- The type of service the sub-processor will provide. For instance administration or hosting.
- The country where the data will be processed. If this is outside the EEA, an assessment will have to be made to determine if any of the exceptions from Article 9.3 of the data processing agreement apply. For more information, see the elaboration in Article 9.3 of this data processing agreement

- The country where the sub-processor is located. If the processing itself takes place within the EEA, but the company with which you, as an institution, conclude the agreement is located in a country outside the EEA, an assessment will still have to be made to determine whether any of the exceptions in Article 9.3 of the data processing agreement in relation to transferring personal data are applicable.

Transfers outside European Economic Area

The Controller has given the Processor specific permission for the following transfers to third countries or international organisations included below (*to be completed by the Controller)*.

Transfer description	**Entity transferring the Personal Data + country**	**Entity receiving the Personal Data + country**	**Transfer mechanism**	**Additional safeguards implemented for transfers outside the EEA**

See the elaboration in Article 8 of the data processing agreement about the transfer of data.

Contact information

General contact information	**Name**	**Job title**	**Email address**	**Telephone number**
The Controller *(to be completed by the controller)*				
The Processor				

Contact information in the event of a Personal Data Breaches	**Name**	**Job title**	**Email address**	**Telephone number**
The Controller *(to be completed by the Controller)*	CERTRU	CERT	cert@ru.nl	7*24 uur: +31-243622222 (helpdesk)
The Processor				

Above, enter the details of who the processor needs to contact in case of a potential data breach. Fill in as much information as possible to ensure that the processor always has a way to report the data breach as soon as possible. The contact person will be the FG in a few cases, but this does not always have to be the case. If the contact person is not the FG, a choice can be made to add another table in which the contact details for the FG are provided.

Annex B: Security measures

Version number 3.0-RU, Date of latest amendment: july 2019

The GDPR states that processors must take "appropriate technical and organisational security measures" to protect personal data. A certification can help prove that a processor has taken "appropriate technical and organisational measures" to comply with the GDPR. When elaborating on the security measures taken in this appendix, the institution may, for example, request an ISO certification or the supplier's security policy. https://www.surf.nl/en/surf-framework-of-legal-standards-for-cloud-services

Details of the security measures taken by the Processor:

Certificates held by the Processor:

Certificates	Organisational unit/service to which the certificate relates	Period of validity of certificate	Declaration of applicability

It is important for an institution not only to ask for an (ISO) certificate, but also for the Declaration of Applicability. The certificate specifies what has been checked during the audit. With (ISO) certifications, however, it is possible to specify that control measures from the specific part of the ISO certification are "not applicable". These measures will therefore not form part of the audit. In that case, that part of the standard is not implemented in the services of the supplier. That is why it is important to request the certificate yourself, in order to identify the scope and to request the Declaration of Applicability, which elaborates on the control measures that have been declared applicable or not applicable for certification.

Qualifications statisfied by the processor:
