Instructions to the Model Processing Agreement

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

Utrecht, the Netherlands, July 2019
Version number: 3.0

Colophon

Instructions to the Model Processing Agreement

SURF
Postbus 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

July 2019

SURF is the collaborative ICT organisation for higher education and research in the Netherlands.

Introduction

These instructions and explanations form part of the Model Processing Agreement, version 3.0 (July 2019), which in turn is part of the SURF Framework of Legal Standards for (Cloud) Services.

A processing agreement focuses specifically on the processing of personal data. All provisions of this agreement are therefore about personal data.

Broader subjects are generally included in the master agreement. An example of such subjects is intellectual property (this may also concern data that is not personal data). 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 processing agreement, but in the event of any doubt or questions, always consult a legal or other adviser in your organisation.

READER'S 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 General Data Protection Regulation (GDPR)
The GDPR is a European regulation that has been directly applicable in all EU Member States since 25 May 2018.

Dutch General Data Protection Regulation (Implementation) Act (the Implementation Act)
This Act regulates the implementation of the GDPR in the Netherlands.

Manual for the General Data Protection Regulation and the General Data Protection Regulation (Implementation) Act
On 22 January 2018, the Ministry of Justice and Security published a manual explaining the most important provisions of the GDPR and the Implementation Act. The Manual can be found via the following link:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf.

GÉANT Data Protection Code of Conduct
A European code of conduct developed by GÉANT, which Service Providers can sign unilaterally to demonstrate their compliance with strict European security and privacy legislation: https://geant3plus.archive.geant.net/uri/dataprotection-code-of-conduct/V1/Documents/GEANT_DP_CoC_ver1.0.pdf.

Guidelines on reporting data breaches
Guidelines on reporting data breaches, published by the Article 29 Working Party and can be found on the website of the Dutch Data Protection Authority:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken.

The website of the Dutch Data Protection Authority
References to news reports and explanation of legislation.

Security Measures Guide, Annex C Framework of Legal Standards
Guide to the implementation of a suitable security level as part of the SURF Framework of Legal Standards for (Cloud) Services. April 2018 version. The document can be found on the SURF website: https://www.surf.nl/files/2019-01/surf_c-handreiking-beveiligingsmaatregelen---bijlage-c---versie-mei-2018.pdf.

Audit Requirement Guide, Annex D Framework of Legal Standards
Implementation guide for the audit requirement of the processing agreement under the SURF Framework of Legal Standards for (Cloud) Services. March 2018 version. The document can be found on the SURF website: https://www.surf.nl/files/2019-01/surf_d-handreiking-auditverplichting---bijlage-d---versie-mei-2018.pdf.

THE UNDERSIGNED:

<NAME OF INSTITUTION>, 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 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 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;

  As part of the processing agreement, it is specifically stated that if the supplier processes personal data for the institution, the institution is the controller and the supplier is the processor in the sense of the GDPR. This specific statement makes it clear which rights and obligations of the GDPR apply to the institution and the supplier.

  The GDPR considers the 'controller' to be the natural or legal person who determines the purpose ('why') and the means ('how') of the processing. A 'processor' is considered to be the natural or legal person who processes personal data on the controller's instructions.

  Laws and regulations:
  - Article 4(7) and (8) of the GDPR

- In the context of the performance of the Agreement, <NAME OF SUPPLIER> is to be regarded as the Processor within the meaning of the GDPR and <NAME OF INSTITUTION> is to be regarded as the Controller within the meaning 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.

The Parties are required to lay down the processing of personal data by the processor in an agreement or other juridical act.

Laws and regulations:
- Article 28(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 natural persons with regard to the Processing of Personal Data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

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 support the performance of the Agreement.

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.

It could also be that agreements on privacy/personal data were made in the master agreement or general terms and conditions. It would be wise to bring the contents of this master agreement in line with the processing agreement to prevent any contradiction. As it may still be possible for both agreements to contain inconsistencies, Article 2(1) provides that the processing agreement takes precedence over the master agreement. It is important that the master agreement does not contain any order that is in conflict with this.

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 reason to believe that the Processor can no longer comply with the Processing Agreement.

All provisions of the processing agreement only apply to the processing of personal data as part of the service.

As a controller, the institution is only allowed to rely on suppliers who offer sufficient guarantees regarding compliance with the requirements from the GDPR and protection of the rights of data subjects. It is therefore important for the supplier to inform the institution immediately if the supplier has any reason to believe that it can no longer comply with the processing agreement.

Laws and regulations:

- Article 28(1) of the GDPR

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

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..

Under the GDPR, the processing agreement must include an overview of the processing operations carried out by the supplier. The supplier may only perform those processing activities that have been laid down in the processing agreement. The processing operations are specified in Annex A. This Annex specifies the purposes of the processing, the categories of personal data, the categories of data subjects, the frequency of the audits to be performed and the personal data retention period. The institution must always have an up-to-date version of this overview, based on its accountability under the GDPR.

Data minimisation is an important aspect when it comes to the categories of personal data: the personal data to be processed is limited to the data necessary in order for the service to be provided.

Laws and regulations:

- Article 28(3), opening words and under (a), of the GDPR
- Article 5(2) 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 may only carry out processing operations based on the institution's written instructions. In practice, this means that the supplier may only process the institution's personal data to the extent necessary in order to provide the services to the institution. The supplier is not allowed to use the personal data for its own purposes (such as advertising). The purposes of the processing are determined by the institution and included in Annex A to the processing agreement.

Laws and regulations:

- Article 28(3)(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.

Controllers as well as processors have their own obligations under the GDPR. Under the GDPR, the supplier must immediately inform the institution if it believes that any instruction given by the institution is contrary to the GDPR and/or other applicable laws or regulations.

Laws and regulations:

- Article 28(3) (second subparagraph) 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 purposes and means of the processing must be determined by the institution. It is the supplier's role to process personal data for the institution and, in doing so, to adhere to the limits set by the institution. As soon as the supplier starts determining the purpose and means of the processing independently, it will be considered a controller for the purpose of that processing. For this purpose, it must therefore comply with all obligations arising from the GDPR independently.

Laws and regulations:

- Article 28(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.

Under the GDPR, the supplier must provide the institution with assistance in performing its statutory obligations.

For instance, the supplier must provide the institution with assistance in answering requests from data subjects, in complying with the duty to protect personal data, reporting a data breach, performing DPIAs and prior consultation in case of a high-risk processing operation. Under the GDPR, these obligations must be included in the processing agreement.

Laws and regulations:

- Article 28(3)(e), (f) and (h) of the GDPR

3.2 The provision of assistance and cooperation with regard to complying with requests from Data Subjects will in any event include the following obligations on the part of the Processor:

3.2.1 The Processor shall take all reasonable measures to ensure that Data Subjects can exercise their rights.

Data Subjects have certain rights under the GDPR:

- A right to information (Articles 13 and 14 of the GDPR);
- A right of access (Article 15 of the GDPR);
- A right to rectification (Article 16 of the GDPR);
- A right to erasure (Article 17 of the GDPR);
- A right of restriction of the processing (Article 18 of the GDPR);
- A right to data portability (Article 20 of the GDPR);
- A right to object (Article 21 of the GDPR); and
- A right not to be subjected to automated individual decision-making (Article 22 of the GDPR).

If a data subject submits such a request to the institution, it will, in practice, often require the supplier's assistance in order to comply with this. Under the GDPR, the processing agreement must contain the obligation for the processor to provide assistance in the exercise 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 data can only be used for statistical or scientific purposes, or that the processing of personal data forms part of an archive, then the institution need not apply Articles 15, 16, and 18 of the GDPR.

Laws and regulations:

- Article 28(3)(e) of the GDPR
- Articles 44 and 45 of the Implementation Act and 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.

To protect the rights of data subjects and the security of the personal data, the supplier is not allowed to handle requests from data subjects; in principle, the institution is responsible for handling requests. The institution must first check the lawfulness of such requests. The institution may give the supplier other instructions in exceptional cases.

Laws and regulations:

- Article 12(2) of the GDPR

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.

Article 3.2.3 does not directly follow from the GDPR, but is added to the Processing Agreement to connect with the 'GÉANT Data Protection Code of Conduct'. This is a European code of conduct developed by GÉANT, which Service Providers can sign unilaterally to demonstrate their compliance with strict European security and privacy legislation. Article 2(h) of this code of conduct includes a similar provision as formulated in Article 3.2.3.

In accordance with Articles 12 and 13 of the GDPR, the supplier needs to inform the data subject of the processing by way of a privacy declaration.

3.3 The provision of assistance and cooperation with regard to complying with 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 body 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.

If processing operations are outsourced, especially in case of cloud services, the data is often not stored at the location of the institution. If authorities submit a request for access to information, the institution, as the controller, is required to adequately respond. If the supplier receives a mandatory request or order for this purpose, 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 controller of the personal data, 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 towards 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 object (at law and otherwise) 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 to 46 of the GDPR.

Under certain circumstances, and due to mandatory laws and regulations, it is prohibited for the supplier to comply with the obligation to provide information as referred to in Article 3.3.1. 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 data is safeguarded as much as possible.

Articles 44 to 46 of the GDPR are about transferring data to third countries (countries outside the European Economic Area). This is only allowed in exceptional cases as described in one of those articles. See Article 8 of this Instruction Model 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 data within the context of the principles of integrity and confidentiality, the processing agreement must specify which employees (officers) or which groups of employees may perform what processing with regard to the personal data. Processing of data by employees other than the (groups of) employees designated in this article is explicitly prohibited.

Laws and regulations:

- Article 29 of the GDPR
- Article 32(4) of the GDPR

4.3 The Processor shall not provide Sub-processors with access to Personal Data without the prior general or specific Written authorisation of the Controller. General Written authorisation for engaging Sub-processors has only been granted if this has explicitly been included in Annex A. Specific authorisation 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 authorisation of the institution (the controller):

1. *Specific authorisation* is aimed at a specific sub-processor. If a sub-processor changes, specific authorisation of the institution will be needed (again) to engage the new sub-processor.
2. In case of *general authorisation*, there is no need for the institution to grant prior written authorisation for each new sub-processor. However, the institution needs to be informed prior to the engagement of the sub-processors and it has a right to object.

The type of authorisation can be specified in Annex A.

Laws and regulations:

- Article 28(2) of the GDPR

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

Based on the GDPR, it is important that the institution has an overview of the sub-processors engaged by the supplier at all times. In case of a change, the overview in Annex A must be adjusted in time, for specific as well as for general authorisation. This will ensure that Annex A always provides a complete overview of the sub-processors engaged by the supplier.

4.5 The Processor shall inform the Controller in the event of general Written authorisation for engaging Sub-processors 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 general authorisation is required for the engagement of sub-processors, and the institution does not agree with the engagement of a certain sub-processor, it has the right to object to this engagement. In case of an objection, the supplier will not, in principle, be allowed to implement the change. The parties will enter into negotiations to come to a solution. If the parties cannot come to a solution, one of the options is that the processing agreement is terminated by mutual consent.

The possibility of objection is necessary because the institution, as the controller, must be able to supervise the processing at all times.

Laws and regulations:

- Article 28(2) of the GDPR

4.6 The general or specific authorisation 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 authorisation 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.

Based on the GDPR, the supplier is obliged to make arrangements with sub-processors about the obligations regarding the processing of personal data by means of an agreement or other juridical act. These obligations must be identical to the arrangements between the institution and the supplier.

Laws and regulations:

- Article 28(4) of the GDPR

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.

The processing agreement must guarantee that the persons authorised to process the personal data are bound by secrecy. Up to a certain extent, employees are already bound by secrecy by operation of law pursuant to Article 272 of the Dutch Penal Code and Article 611 of Book 7 of the Dutch Civil Code. The employment contract may include a further confidentiality clause, detailing or supplementing the obligation.

Laws and regulations:

- Article 28(3)(b) of the AVG 2012

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 controller, must be able to verify that the processing is carried out in accordance with the GDPR, the supplier is obliged to provide proof of the agreement with the sub-processors and of the confidentiality agreements made with the persons authorised to process the personal data and other recipients of personal data, without delay at the request of the institution.

Laws and regulations:

- Article 28(3)(h) and (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 any sub-processors engaged.

Laws and regulations:

- Article 28(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 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 under the GDPR to ensure an adequate level of security of personal data. 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 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 data. The guarantees requested must relate to expertise, integrity, and resources in particular.

More information about appropriate security: see the Security Measures Guide, Annex C Framework of Legal Standards:
https://www.surf.nl/files/2019-01/surf_c-handreiking-beveiligingsmaatregelen---bijlage-c---versie-mei-2018.pdf.

Laws and regulations:

- Article 28(1), (3)(c) and Article 32 of the GDPR
- Recital 81 to 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 risks to the rights and freedoms of natural persons.

Additionally, in determining what is considered an 'appropriate' level, the emphasis must be placed 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(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 data is adequately protected, the supplier is obliged to provide proof of a written security policy without delay at the request of the institution.

Laws and regulations:

- Article 28(3)(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 organisational measures. A periodic audit is an appropriate way for a processor to prove that it meets its statutory obligations under the GDPR.

Laws and regulations:

- Article 28(3)(c) and (f) and Article 32(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.

As shown by Article 6.2, the frequency of the periodic audits depends on the type of personal data that is processed. Combining data can influence the risk class of the data. In some cases, combining data can lead to a higher risk class.

There are three risk classes:

- Low: this category only includes personal data of which it is generally accepted that, if used as intended, it does not present a risk for the data subject. This could refer to publicly accessible information, but this need not always be the case. Examples are a name, business e-mail address or occupation.
  - *No periodic audit obligation.*
- Medium: this category includes personal data that does not fall into the 'Low' risk class or the 'Special Personal Data' category. This includes, for instance, the registration of a student or location information.
  - *An audit must be performed once every two years.*
- High: this relates to personal data that falls within the 'Special Personal Data' category (Article 9 of the GDPR), which includes information regarding political opinions, personal data revealing racial or ethnic origin, genetic and biometric data and criminal data, among other things. The Citizen Service Number (BSN) and education number also fall under the 'High' risk classification.
  - *An audit must be performed once a year.*

Such an audit must also be performed prior to signing the agreement to ensure that the institution has investigated the services provided by the supplier.

More information about the audit requirement: see the Audit Requirement Guide, Annex D Framework of Legal Standards:
https://www.surf.nl/files/2019-01/surf_d-handreiking-auditverplichting---bijlage-d---versie-mei-2018.pdf.

Also refer to 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 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 drawn up at the supplier's request and is provided to the institution that uses the supplier's services. The aim of providing a TPM is to give the institution a clear understanding of the measures taken by the supplier, so that each institution does not need to investigate this individually.

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.

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 processing agreement and, more generally, the GDPR.

Laws and regulations:

- Article 28(3)(h) of the GDPR

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.

If the institution has a reasonable suspicion that the supplier has violated the agreements made, the institution has to investigate this suspicion. This involves a (limited) quality assessment. The costs of this investigation are initially borne by the institution itself. If the investigation shows that the supplier has indeed violated the agreements made, the institution may recover the costs of the investigation from the supplier.

The costs of the periodic audit from Article 6.1 of the processing agreement are for the supplier’s account.

6.6 If it is established during an audit that the Processor fails 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, the Processor shall immediately take all reasonably necessary measures to ensure compliance by 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 no later than 24 hours after its discovery. 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 Dutch Data Protection Authority. The Processor warrants that the information provided is complete, correct, and accurate, to the best of the Processor's knowledge at that time.

The GDPR states that the institution shall report any data breaches that fall under the reporting requirement to the Dutch Data Protection Authority within 72 hours after discovery. This also includes data breaches taking place at the location of the suppliers or their auxiliary suppliers. As 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.

The institution must therefore 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 provides that the supplier must report the data breach to the institution within 24 hours of its discovery. This includes data breaches among any sub-processors engaged. For this reason, the supplier also has an obligation to make agreements on reporting data breaches with sub-processors as well. Because the chain of parties involved is longer in this situation, those 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.

The supplier must report to the institution all information as shown by the most recent data breaches form of the Dutch Data Protection Authority.

Laws and regulations:

- Article 28(3)(f) and Article 33 of the GDPR
- Guidelines on reporting data breaches

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 Dutch 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(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.

Laws and regulations:

- Article 33(5) and Article 28(3)(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 the controller, is the party that assesses whether a data breach entails a high risk for the rights and freedoms of natural persons and whether the data breach needs to be reported to the Dutch Data Protection Authority and possibly the data subjects. The supplier need not do this.

Laws and regulations:

- Article 33 and Article 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 authorisation to do so. This specific Written authorisation is only granted if included in Annex A.

Pursuant to the GDPR, the processing agreement must include provisions on the transfer of personal data to third countries. The Model Processing Agreement provides that the supplier needs the prior written authorisation of the institution before being allowed to engage a third party outside the EEA (European Economic Area: all EU countries plus Norway, Liechtenstein and Iceland). If, in derogation of this, the parties choose to replace this prior authorisation by the possibility for the institution to object, it is essential that sufficient agreements are made about this, for example the agreement that the institution is informed in good time and in writing of the intended change regarding a transfer outside the EEA and the possibility for the institution to object to this.

Under the GDPR, processing personal data in third countries is only allowed in three situations: A third country means every county outside the EEA. The three possibilities for transfer of personal data 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 is only transferred to companies that have a Privacy Shield (as, when this document was written, proceedings are pending before the Court of Justice of the European Union against the Privacy Shield, it is, however, uncertain if this agreement will remain effective).

2. In case of 'appropriate safeguards' or Binding Corporate Rules (Articles 46 and 47 of the GDPR). These measures are:
   a. Binding Corporate Rules;
   b. model contract of the European Commission;
   c. model contract of the Dutch Data Protection Authority;
   d. a self-drafted agreement that is approved by the Dutch Data Protection Authority;
   e. code of conduct;
   f. certification.

3. In case of one of the specific situations from Article 49(1) of the GDPR. These are:
   a. explicit consent of the data subject;
   b. the transfer is necessary for the conclusion or performance of an agreement (restrictive interpretation);
   c. the transfer is necessary for important reasons of public interest;
   d. the transfer is necessary for the establishment, exercise or defence of legal claims;
   e. the transfer is necessary in order to protect the vital interests of a person;
   f. for a register designated by law;
   g. the 'incidental transfer' described in Article 49(1)(g) of the GDPR.

Laws and regulations:

- Article 28(3)(a) and Articles 44 to 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 shall 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, unless:

(i) Disclosure and/or provision 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 provision of such Personal Data takes place with the prior Written authorisation of the other Party.

Although confidentiality extends beyond personal data (sensitive corporate data can also be confidential, for example), this Model Processing Agreement also contains a confidentiality clause. The Dutch Data Protection Authority also stated in a 2016 news item that a processing agreement must include duty of confidentiality.

See:
- https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-eist-betere-afspraken-over-digitaliseren-pati%C3%ABntdossiers.
- Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (OJEU 2016, L157) and the Dutch Trade Secrets Act.

ARTICLE 10. LIABILITY

10.1 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.

10.2 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.

Pursuant to the Dutch Civil Code, a party that fails to comply with an agreement, is liable for the loss resulting from this. In this Model Processing Agreement, the choice was made to connect with the liability provision of the master agreement between the parties. In two cases, however, it is not possible for a party to invoke any limitation of liability contained in the master agreement:

1. If the other party brings an action for recovery pursuant to Article 82 of the GDPR.
2. If the other party brings an action for damages under the processing 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(1), (2) and (4) of the GDPR provides that the data subject has the right to claim compensation from the institution as well as the supplier, regardless of who carries the blame. Paragraph 5 of this article introduces the possibility for the supplier and the institution to agree on a mutual right of recourse.

It is also important that the supplier has adequate insurance. Insurance policies can vary widely and not all policies are suitable for cloud suppliers. When assessing the supplier's insurance, it is important to pay particular attention to the following points:

- The amount of coverage.
- What is covered by the insurance and what is excluded from coverage (e.g. 'loss of data' and 'costs for reporting obligation').

Laws and regulations:

- Article 28(4) of the GDPR
- Article 82(1), (2) and (4) of the GDPR

ARTICLE 11. CHANGES

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 require or may require a change to the Processing Agreement and/or the Annexes. This is in all cases understood to mean:

(i) Changes that affect or 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 authorisation for such changes. A change to the Service is understood to mean a substantial change that may have implications for the Processing of Personal Data. In derogation of the foregoing, the Processor may, without the prior Written authorisation 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.

To perform the tasks of a controller, the institution must ensure that personal data is processed in accordance with the predetermined risk level. If the processing (the supplier's services) changes, the institution must be able to check prior to the change whether the processing takes place in accordance with the appropriate level.

Laws and regulations:

- Article 28(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. TERM 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 processing agreement. Upon termination of the agreement, the 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 processing agreement. In that case, it is advisable to agree on a separate duration of the 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 other existing 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 Sub-processors, will demonstrably permanently be deleted, unless storage of the Personal Data is required under Union or Member State law.

If the processing agreement is terminated, the GDPR stipulates two options:

1. The personal or other data processed will be destroyed by the supplier; or
2. The personal or other data processed will be returned to the institution by the supplier and existing copies will be destroyed.

This is at the discretion of the institution. Any other option will not offer appropriate protection of the personal or other data. An exception applies if the supplier is required by law to retain certain personal data.

Laws and regulations:

- Article 28(3)(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.

It is important for some articles to continue also after termination of the processing agreement. Examples include provisions on confidentiality, liability and choice of law.

ARTICLE 13. GOVERNING 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.

AGREED BY THE PARTIES:

[NAME OF CONTROLLER]

_____/_____/_____

Date

_____

Name

_____

Signature

[NAME OF PROCESSOR]

_____/_____/_____

Date

_____

Name

_____

Signature

Annex A: Specification of the Processing of Personal Data

Version number XX, Date of latest amendment: XX-XX-XX

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' [De AVG in een notendop] that has been published by the Dutch Data Protection Authority as a practical tool for completing this annex.

Laws and regulations:
- Article 28(3) and (9) of the GDPR

Description of the Processing

Include the name of the service here. For example: 'payroll processing'.

Purposes of the Processing (*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 individual the personal data is about. There can be various categories of data subjects, such as students, employees or contact persons.

Categories of Personal Data (*to be completed by the Controller*)

The level of detail of the personal data description 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, but also login details or exam results. Assess all personal data included in the service.

For more information, consult the website of the Dutch Data Protection Authority: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens.

Audit frequency (*to be completed by the Controller*)

The audit frequency depends on the type of personal data that is processed. See the explanation of Article 6 of the 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 data is not stored any longer than necessary for the processing.

Some personal data is processed for as long as the service is provided, in which case 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 are back-up storage and logging. The institution and supplier agree on how long this personal data is to be kept.

Laws and regulations:

- Article 5(1)(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 employees that have access to the personal data. These include administrators, help desk staff, etc.
- The type of personal data concerned.
- What employees can do with the personal data (the type of processing): e.g. 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 authorisation to engage Sub-processors.

□ Specific authorisation 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 of establishment of the Sub-processor

Article 4.3 of the processing agreement states that the institution shall give the supplier its prior written authorisation if it wants to engage a sub-processor. This could be general as well as specific authorisation. Check the applicable box above.

The above table needs to be completed. The following questions are answered there:

- Which sub-processors (auxiliary suppliers) the supplier will engage in the performance of the service.
- The personal data to which the sub-processor will gain access.
- The type of service the sub-processor will provide (administration or hosting, for example).
- 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 referred to in Article 8.1 of the processing agreement apply. More information can be found in the elaboration of Article 8.1.
- The country of establishment of the sub-processor. If the processing itself takes place within the EEA, but the company with which the institution concludes the agreement is established in a country outside the EEA, an assessment will still have to be made to determine whether any of the exceptions referred to in Article 8.1 of the processing agreement are applicable.

Transfers outside the European Economic Area

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

See the explanation of Article 8 of the processing agreement for the transfer of data.

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

Contact information

General contact information	**Name**	**Job title**	**E-mail address**	**Telephone number**
The Controller (*to be completed by the Controller)*				

The Processor				

Contact information in the event of a Personal Data Breach	**Name**	**Job title**	**E-mail address**	**Telephone number**
The Controller (*to be completed by the Controller)*				
The Processor				

The person to be contacted by the processor in the event of a possible data breach should be stated above. Fill in as many details as possible so as to give the processor several options to report the data breach as quickly as possible. In some cases, the contact person will be the Data Protection Officer, but this need not always be the case. In that case, it is possible to add another table that lists the contact details of the Data Protection Officer.

Annex B: **Security measures**

The GDPR provides that processors must take 'appropriate technical and organisational security measures' to secure personal data. A certification may 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 annex, the institution may, for example, request an ISO certification or the supplier's security policy. More information about appropriate security measures can be found in Article 5 of the processing agreement and the Security Measures Guide, Annex C Framework of Legal Standards: https://www.surf.nl/files/2019-01/surf_c-handreiking-beveiligingsmaatregelen---bijlage-c---versie-mei-2018.pdf.

Version number XX, Date of latest amendment: XX-XX-XX

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 the certificate	Declaration of applicability

It is important for an institution not only to ask for an ISO certificate, but also for a 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 for 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 to the certification.