Processor Agreement

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

Utrecht, October 2016
Version number: 1.1

Credits

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

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

info@surf.nl
www.surf.nl

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

Changes with respect to version 1.0 (January 2016)

1. ***Language changes***

   Capitalisation, correction of inaccurate references, improvement of readability, addition of used definitions

2. ***Confidentiality clause added***

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

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

3. ***Disclaimer against subcontractors***

   Article 3 on the use of subcontractors included a disclaimer provision identical to the general disclaimer provision in Article 10 of the processor agreement. This caused confusion as the general provision also includes the subcontractors, so it was decided to remove the provision from Article 3.

4. ***Obligations that persist after the processor agreement***

   Article 13 on duration and termination was expanded with a paragraph on obligations that persist after the end of the processor agreement.

5. ***Changes to Article 8 on search requests***

   The following sentence was removed from Article 8, paragraph 3: "Notwithstanding the provisions of this Processor Agreement, the Processor shall be considered the controller if it allows a regulator or government body to access or receive Personal Data without the Controller's involvement in terms of content." This sentence caused confusion and there was some discussion about its value.

The Parties

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

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

taking into account that:

- The Controller wants to have Personal Data processed by the Processor in execution of the agreement concluded with the Processor on XX-XX-XX (hereinafter referred to as "the Agreement").
- The Processor processes Personal Data in execution of its Agreement with the Controller and is regarded as the processor in the sense of the Dutch Personal Data Protection Act. The institution is regarded as the controller in the sense of the Personal Data Protection Act.
- The Processor and Controller (hereinafter referred to as "the Parties") wish to define their rights and obligations in this processor agreement (hereinafter referred to as the "Processor Agreement"), taking into account the requirements of Article 14, paragraph 5 of the Personal Data Protection Act.
- The general provisions of the Processor Agreement apply to all Processing in the execution of the Agreement.

have agreed as follows:

ARTICLE 1. DEFINITIONS

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

1.2 The Processor Agreement is this agreement.

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

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

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

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

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

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

1.9 The Subprocessor is a Subcontractor who processes Personal Data at the Processor's request.

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

ARTICLE 2. GENERAL

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

2.2 The Processor shall only process the Personal Data if it is required to provide the Service to the Controller as described in the Agreement. Only the categories of Personal Data specified in Annex A can be processed during the execution of the Service.

2.3 Annex A describes which (groups) of employees have access to the Personal Data per Service and which types of Processing employees can engage in.

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

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

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

ARTICLE 3. USE OF SUBCONTRACTORS

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

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

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

The Controller's approval is without prejudice to the Processor's responsibility and liability for complying with the Processor Agreement.
3.3 If the Controller provides a general written approval of the engagement of Subcontractors to deliver the Service, this general approval shall be included in Annex A. If new Subcontractors are engaged or if any changes occur, the Processor shall inform the Controller in advance and offer a time limit for any objections. The Processor guarantees that each Subcontractor shall respect the conditions of Article 3, paragraph 2. The Processor must be able to provide an overview of the engaged Subcontractors at all times at the Controller's request.

ARTICLE 4. SECURITY

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

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

ARTICLE 5. DUTY TO REPORT DATA BREACHES AND SECURITY BREACHES

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

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

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

5.4 The Processor makes written arrangements with the Subcontractors for incident reporting to the Processor. These arrangements enable the Processor and Controller to meet their obligations in the event of an incident as described in Article 5, paragraph 1. These arrangements shall always include the Subcontractor's obligation to inform the Processor of an incident immediately and certainly within 18 hours after discovering the incident, as described in Article 5, paragraph 1, and to help inform the competent authorities and Data Subject(s) at the Controller's request.

ARTICLE 6. AUDIT

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

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

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

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

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

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

ARTICLE 7. INTERNATIONAL TRAFFIC

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

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

ARTICLE 8. SEARCH REQUESTS

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

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

a. have a legal assessment performed of (i) the extent to which the Processor is obliged to comply with the request or order; and (ii) the extent to which the Processor is actually prohibited from meeting its obligations to the Controller pursuant to the above provisions;

b. cooperate to comply with the request or order only if it is legally obliged to do so and (legally) oppose the request, order or ban from notifying the Controller or from following its instructions where possible;

c. refrain from providing any Personal Data beyond or other than what is strictly necessary to comply with the request or order;

d. investigate the possibilities to comply with Articles 76 and 77 of the Personal Data Protection Act in the event data is transferred to a country outside the EEA;

e. inform the Controller immediately as soon as this is permitted.

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

ARTICLE 9. INFORMING THE DATA SUBJECTS

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

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

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

a. the name and address of the Controller and Processor;

b. the purpose of processing the Personal Data;

c. the categories of Personal Data processed by the Processor;

d. the third parties receiving access to the Personal Data;

e. the countries to which Personal Data is transferred;

f. the right to access, correct and remove Personal Data.

The Processor shall inform the Controller where this information is published.

ARTICLE 10. DISCLAIMER

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

ARTICLE 11. REGULATOR MEASURES

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

ARTICLE 12. CHANGE

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

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

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

ARTICLE 13. DURATION AND TERMINATION

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

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

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

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

ARTICLE 14. CONFIDENTIALITY

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

a. when disclosure and/or provision of this (Personal) Data and other information is necessary in connection with the execution of the Agreement or Processor Agreement;

b. when any mandatory legal statutory or court ruling forces the Parties to disclose and/or provide the (Personal) Data or other information, in which case the Parties shall inform the other party first;

c. when the (Personal) Data is announced and/or provided with the other party's prior approval in writing; or

d. when the information was already lawfully considered public for a reason other than the actions of one of the Parties or its failure to act.

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

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

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

ARTICLE 15. APPLICABLE LAW AND DISPUTE RESOLUTION

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

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

INSTITUTION NAME	**SUPPLIER NAME**
_____/_____/___________	_____/_____/___________
Date	*Date*
______________________	______________________
Name	*Name*
______________________	______________________
Signature	*Signature*

Annex A: Personal Data Processing Specifications

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

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

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

These Annexes are attached to the Processor Agreement.

Annex A1: <SERVICE NAME>

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

Data Subject categories

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

Personal Data to be processed (categories)

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

<Enter Personal Data (categories)>

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

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

<Enter which retention periods are valid>

Job roles/job groups and their Processing

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

Role (group)	Personal Data (category)	Processing type

Table 1: Employee groups and their Personal Data Processing

Affected security measures

<To be completed further>

Subcontractors

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

Organisation name: **<Name>**

Brief description of the Service: <Complete>

Extent of Personal Data Processing: <Complete>

Processing place/country: <Complete>

Organisation name: **<Name>**

Brief description of the Service: <Complete>

Extent of Personal Data Processing: <Complete>

Processing place/country: <Complete>

Contact details

In the event of any questions about this Annex and/or the supplied Service, please contact:

Name: **<name> (Supplier)**

Role: <Complete>

E-mail address: <Complete>

Telephone number: <Complete>

Name: **<name> (institution)**

Role: <Complete>

E-mail address: <Complete>

Telephone number: <Complete>

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

Name: **<name> (institution)**

Role: <Complete>

E-mail address: <Complete>

Telephone number: <Complete>

Annex B1: <SERVICE NAME>

Information that must be provided in the event of a Data Breach

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

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

Reporter contact details

Name, role, e-mail address, telephone number

Data Breach details

- Provide a summary of the incident during which the security of the Personal Data was breached.

- How many individuals have Personal Data that is involved in the breach? (Please enter the numbers.)

a) At least: (Complete)

b) At most: (Complete)

- Describe the group of people whose Personal Data is involved in the breach.

- When did the breach take place? (Choose one of the following options and complete where necessary.)

a) On (date)

b) Between (period start date) and (period end date)

c) Not known yet

- What is the nature of the breach? (You can tick several options.)

a) Reading (confidentiality)

b) Copying

c) Altering (integrity)

d) Removal or destruction (availability)

d) Theft

f) Not known yet

- What type of Personal Data is involved? (You can tick several options.)

a) Name, address and city

b) Telephone numbers

c) E-mail addresses or other addresses used for electronic communication

d) Access or identification data (for example login names/passwords or customer numbers)

e) Financial information (for example account numbers, credit card numbers)

f) Dutch social security numbers, referred to as citizen service numbers (BSN) or Sofi numbers

g) Copies of passports or other proof of identification

h) Gender, date of birth and/or age

i) Sensitive Personal Data (for example race, ethnicity, criminal information, political beliefs, trade union membership, religion, sex life, medical information)

j) Other data: (Complete)

- Which consequences may the breach have on the Data Subjects' private lives? (You can tick several options.)

a) Stigma or exclusion

b) Damage to health

c) Exposure to (identity) fraud

d) Exposure to spam or phishing

e) Other: (Complete)

Data Breach response

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

Technical protection measures

- Is the Personal Data encrypted, hashed or made inaccessible or incomprehensible to unauthorised users in another way? (Choose one of the following options and complete where necessary.)

a) Yes

b) No

c) Partly: (Complete)

- If the Personal Data has been made fully or partly inaccessible or incomprehensible, how was this done? (Answer this question if you selected options a or c in response to the previous question. If you used encryption, please also explain the encryption method.)

International aspects

- Does the breach concern persons in other EU countries? (Choose one of the following options.)

a) Yes

b) No

c) Not known yet