Processor Agreement

SURF Model Agreement

Utrecht, 18 November 2016
Version: 1.1

About this publication

Processor Agreement
SURF Model Agreement

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

info@surf.nl
www.surf.nl/en

SURF is the collaborative organisation for higher education institutions and research institutes aimed at breakthrough innovations in ICT.
This publication is online available through www.surf.nl/en/publications

Changes compared to version 1.0 (January 2016)

1. ***Linguistic amendments***

   Use of capital letters, rectification of incorrect references, enhanced readability, addition of definitions applied

2. ***Confidentiality provision added***

   While confidentiality extends further than personal data (business-sensitive data may also be confidential, for example), a confidentiality provision has been included in this model processor agreement for the sake of completeness. This provision is to apply in the event that this topic has not been provided for in the main agreement. In addition, the Dutch Data Protection Authority indicated in a press release of May 2016 that a confidentiality obligation must form part of a processor agreement.

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

3. ***Indemnification with respect to auxiliary suppliers***

   Clause 3 (engagement of auxiliary suppliers) contained an indemnification provision identical to the general indemnification provision in the processor agreement (Clause 10). As this led to confusion, and the general provision covers auxiliary suppliers as well, it was decided to delete the provision in Clause 3.

4. ***Obligations that continue after the expiry of the processor agreement***

   A paragraph has been added to Clause 13 (term and termination) regarding obligations that continue to apply after termination of the processor agreement.

5. ***Amendment of Clause 8 (Investigation requests)***

   The following sentence has been removed from Clause 8.3: "At variance with the provisions in this Processor Agreement, the Processor shall be deemed a controller if it decides, without any substantive intervention by the Controller, to grant access to Personal Data to or provide Personal Data to a supervisory authority or government agency." This sentence led to confusion and discussion arose about its value.

Parties

- **[NAME OF INSTITUTION],** having its registered office at [ADDRESS] in [CITY], Chamber of Commerce number [COC] and duly represented by **[REPRESENTATIVE]** (hereinafter: "**the Controller**");

- **[NAME OF SUPPLIER],** having its registered office at [ADDRESS] in [CITY], Chamber of Commerce number [COC] and duly represented by **[REPRESENTATIVE]** (hereinafter: "**the Processor**");

whereas

- The Controller wants to have Personal Data processed by the Processor for the purpose of the performance of the agreement concluded with the Processor on XX-XX-XX (hereinafter: "the Agreement");
- The Processor who processes Personal Data in the context of the performance of the Agreement with the Controller can be considered a processor within the meaning of the Dutch Personal Data Protection Act ('*Wet bescherming persoonsgegevens*') (PDPA) and the Institution can be considered a controller within the meaning of the PDPA;
- the Processor and the Controller (hereinafter: "the Parties"), partly in view of the requirement from Article 14(5) of the PDPA, wish to record their rights and obligations in writing by means of this processor agreement (hereinafter: "the Processor Agreement");
- the general provisions from the Processor Agreement apply for all Processing in the performance of the Agreement;

have agreed as follows

CLAUSE 1. DEFINITIONS

1.1 Data Subject is the person to whom Personal Data pertains.

1.2 Processor Agreement is the present agreement.

1.3 Special data are Personal Data within the meaning of Article 16 of the PDPA.

1.4 Data breach is a security breach within the meaning of Article 13 in conjunction with Article 34a of the PDPA.

1.5 Service is the service to be provided by the Supplier under the Agreement.

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

1.7 Auxiliary Supplier is a party engaged by the Processor to assist in the performance of the Service. If the Auxiliary Supplier processes Personal Data on the instructions of the Processor, the Auxiliary Supplier can also be considered a Subprocessor.

1.8 Personal Data are any data regarding an identified or identifiable natural person, which are or will be processed by the Processor in any way whatsoever in the context of the Agreement.

1.9 Subprocessor is an Auxiliary Supplier that processes Personal Data on the instructions of the Processor.

1.10 Processing is any activity or combination of activities involving Personal Data, in any event including the collecting, recording, organising, storing, updating, amending, accessing, consulting, using, providing by way of forwarding, distributing or any other form of supplying, compiling, linking, as well as safeguarding, deleting or destroying of data.

CLAUSE 2. GENERAL

2.1 The Processor undertakes to process Personal Data on the terms and conditions of this Processor Agreement on the instructions of the Controller. The Processor shall process the Personal Data properly, with due care and in accordance with the PDPA and other applicable legislation and regulations relating to the processing of Personal Data.

2.2 The Processor shall only effect Processing to the extent necessary to provide the Service to the Controller as described in the Agreement. For the performance of the Service, only the Personal Data categories specified in Annex A will be processed.

2.3 It is described in Annex A for each Service which (groups of) employees have access to the Personal Data and which Processing by employees is permitted.

2.4 The Processor shall not retain Personal Data made available to it in the context of the Agreement any longer than is necessary (i) for the performance of this Agreement; or (ii) to comply with any of its statutory obligations. In Annex A it is specified for each (part of the) Service how long Personal Data will be retained.

2.5 The Processor shall only process the Personal Data on and in accordance with the instructions of the Controller. The Processor may not process the Personal Data for its own benefit, for the benefit of third parties, and/or for its own purposes or advertising purposes or other purposes, notwithstanding any of its obligations to the contrary under mandatory law.

2.6 The Processor is obligated to immediately inform the Controller regarding any future changes in the performance of the Agreement, so that the Controller can monitor compliance with arrangements made with the Processor. This also includes the engagement of (new) Auxiliary Suppliers, without prejudice to the provisions in Clause 3 (Use of Auxiliary Suppliers) and Clause 12 (Change).

CLAUSE 3. USE OF AUXILIARY SUPPLIERS

3.1 Without the prior written permission from the Controller, the Processor shall not grant access to the Personal Data to third parties, including Auxiliary Suppliers and group companies to which the Processor belongs, such as subsidiaries or affiliates. The Controller shall not withhold such permission on unreasonable grounds. When granting permission, the Controller is entitled to attach conditions or restrict the permission in time.

3.2 In any event the following conditions will be attached to the Controller's permission to engage Auxiliary Suppliers for the provision of the Service:

- The Processor has a written agreement with the relevant Auxiliary Supplier, which agreement shall in any event include the following:
  - an obligation that the Auxiliary Supplier shall act in accordance with all the provisions from the Processor Agreement including the Annexes relating to the Processing of Personal Data;
  - an obligation that the Auxiliary Supplier shall follow all of the Controller's and the Processor's instructions relating to the processing of Personal Data;
  - an undertaking from the Auxiliary Supplier to only process the Personal Data on and in accordance with the instructions of the Processor;
  - an undertaking from the Auxiliary Supplier to not engage any sub-processors itself without the Controller's prior written permission;
  - an undertaking that the Auxiliary Supplier shall enable the Processor (and consequently the Controller) to fulfil its obligations in the event of a suspected or actual Data Breach.
- The Processor shall only grant the Auxiliary Supplier access after permission from the Controller; and

- The Controller has the possibility to request the arrangements made between the Processor and the Auxiliary Supplier.

The permission granted by the Controller does not affect the Processor's responsibility and liability for the performance of the Processor Agreement.
3.3 If the Controller grants general written permission to engage Auxiliary Suppliers for the provision of the Service, such general permission is included in Annex A. If new Auxiliary Suppliers are engaged, or changes are made, then the Processor must inform the Controller in advance and set a term for making an objection. The Processor warrants that the conditions from Clause 3.2 have been observed with each Auxiliary Supplier. The Controller must at all times be able to request a list from the Processor of the Auxiliary Suppliers engaged.

CLAUSE 4. SECURITY

4.1 The Processor shall implement appropriate technical and organisational measures to secure Personal Data against loss or any form of unlawful processing. Taking into account the state of the art and the costs of their implementation, these measures guarantee an appropriate security level given the risks associated with Processing and the nature of the Personal Data to be protected. The measures are, in part, aimed at preventing unnecessary collection and further Processing. The Processor shall record the measures in writing and shall ensure that the security as referred to in this paragraph meets with the security requirements under the PDPA. In Annex A the security measures are described that the Processor shall apply in any event.

4.2 On request, the Processor shall immediately provide the Controller with written information relating to (the organisation) of the security of Personal Data.

CLAUSE 5. OBLIGATION TO REPORT DATA BREACHES AND SECURITY BREACHES

5.1 In the event of a suspected or actual (i) Data Breach; (ii) breach of security measures; (iii) breach of the confidentiality obligation or (iv) loss of confidential data, the Processor shall notify the Controller immediately, but no later than 24 hours after the incident was first discovered. The Processor shall take all measures reasonably necessary to prevent or limit (further) unauthorised examination, change, and provision or otherwise unlawful processing and to stop and prevent any future breach of security measures, breach of the confidentiality obligation or further loss of confidential data, without prejudice to any right the Controller might have to damages or other measures. This provision applies to incidents at the Processor and its Auxiliary Suppliers, if any.

5.2 The Processor's obligation to provide information in any event includes the data described in Annex B, in so far as applicable. The Processor warrants that the information provided is complete, correct and accurate.

5.3 At the Controller's request, the Processor shall cooperate in informing the competent authorities and Data Subject(s).

5.4 The Processor shall make written arrangements with Auxiliary Suppliers about the reporting of incidents to the Processor, which will enable the Processor and the Controller to comply with obligations in the event of an incident as described in Clause 5.1. These arrangements must in any event include the obligation that the Auxiliary Supplier shall notify the Processor immediately, but no later than 18 hours after the first discovery of an incident as described in Clause 5.1, and at the Controller's request shall cooperate in informing the competent authorities and the Data Subject(s).

CLAUSE 6. AUDIT

6.1 The Processor is required, periodically or upon request from the Controller, to have an independent IT auditor or expert to be designated by the Processor conduct an audit regarding the organisation of the Processor in order to have it established that the Processor complies with the provisions regarding the protection of confidentiality, integrity, availability and security of Personal Data and confidential information as defined in the Agreement and Processor Agreement. The frequency of the audit is once every two years for the 'medium' risk class, with the exception of high-risk Processing where an audit is requested of the Processor annually. A high risk shall in any event apply where special Personal Data within the meaning of the PDPA are being processed. If only public Personal Data are processed, there is a 'low' risk and no obligation to carry out a periodic audit applies. The risk is described in Annex A.

6.2 Upon request, the Processor is obliged to make the findings of the IT auditor or expert available to the Controller in the form of a Third Party Memorandum.

6.3 The Processor shall compile a monthly report on security management within five working days after the beginning of the next calendar month, which must at least include the following aspects:

- Number, status, progress and analysis of security incidents;
- Measures taken in the area of security management in connection with security incidents;
- General measures taken in the area of data security.

6.4 The costs of the periodic audit will be borne by the Processor. The costs of the audit upon request will be borne by the Controller, unless the findings of the audit show that the Processor failed to comply with the provisions from the Processor

Agreement. In that case, the Processor shall bear the costs. This provision does not diminish the Controller's other rights, including the right to damages.

6.5 If it is established during an audit that the Processor has failed to comply with the provisions of the Agreement and the Processor Agreement, the Processor shall take all reasonably necessary measures to ensure compliance as yet.

CLAUSE 7. INTERNATIONAL TRAFFIC

7.1 The Processor warrants that every processing of Personal Data in connection with the performance of the Agreement performed by or for the Processor, including the third parties engaged by it, will take place within the European Economic Area (EEA) or to or from countries that guarantee an appropriate level of protection in accordance with the applicable privacy regulations. Consequently, without the prior written authorisation of the Controller the Processor may not transmit or store any Personal Data to or in a country outside the EEA or make Personal Data accessible from an non-EEA country, unless that country has an appropriate level of protection. The Controller may attach conditions to that authorisation, including, without limitation, the obligation for the Processor to demonstrate that the statutory requirements with regard to data traffic involving non-EEA countries have been complied with.

7.2 If the technical characteristics of a transmission medium render such a guarantee impossible, data will only be transmitted in encrypted form, using advanced encryption technology (that is at least as advanced as is common market practice). Prior to concluding the Processor Agreement, the Processor shall provide insight into the location(s) where the Processing will take place.

CLAUSE 8. INVESTIGATION REQUESTS

8.1 If the Processor receives a request or order from a Dutch or foreign supervisory authority, government agency or investigation, prosecution or national security agency to provide (access to) Personal Data, the Processor shall immediately notify the Controller. When handling the request or order, the Processor shall observe all of the Controller's instructions (including the instruction to leave the handling of the request or order in full or in part to the Controller) and provide all reasonably required cooperation to the Controller.

8.2 If the request or order prohibits the Processor from complying with its obligations on the basis of the above, the Processor shall promote the Controller's reasonable interests. In any event, the Processor shall to that end:

a. Procure a legal review as to what extent (i) the Processor is required by law to comply with the request or order; and (ii) the Processor is de facto prohibited from complying with its obligations to the Controller on the basis of the above;

b. Only cooperate with the request or order if it is required by law to do so and where possible object (by legal action) to the request or order or injunction enjoining it from informing the Controller in this respect or from following its instructions;
c. Not provide any more or any other Personal Data than is strictly necessary to comply with the request or order;
d. If data is transmitted to a non-EEA country: examine the possibilities to comply with Articles 76 and 77 of the PDPA;
e. Inform the Controller immediately once this is permitted.

8.3 In this clause, “by law” refers not only to Dutch law but to foreign laws and regulations as well.

CLAUSE 9. INFORMING DATA SUBJECTS

9.1 The Processor shall fully cooperate, so that the Controller can comply with its legal obligations in the event that a Data Subject exercises its rights under the PDPA or other applicable regulations concerning the processing of Personal Data.

9.2 If a Data Subject, in relation to the execution of its rights under the PDPA, contacts the Processor directly, the Processor shall not initially respond (substantively) - unless expressly instructed otherwise by the Controller - but shall immediately report this to the Controller, with a request for further instructions.

9.3 If the Processor offers the Service directly to the User whose Personal Data are processed, the Processor is required, exclusively at the Controller’s request, to provide information to the User in an easily accessible and permanently available manner by means of a privacy policy that includes the following:

a. the name and address of the Controller and Processor;
b. the purposes for which Personal Data are processed;
c. the Personal Data categories processed by the Processor;
d. the third parties to whom Personal Data are made accessible;
e. the countries to which Personal Data are transferred;
f. the right to access, correct and delete Personal Data.

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

CLAUSE 10. INDEMNIFICATION

The Processor indemnifies the Controller from and against all claims by third parties, including Data Subjects, asserted against the Controller due to a breach of the PDPA or other applicable regulations concerning the processing of Personal Data that is attributable to the Processor or Auxiliary Suppliers engaged by the Processor.

CLAUSE 11. MEASURES BY SUPERVISORY AUTHORITY

If the supervisory authority, in the context of its duties as enforcer, imposes a measure or fine on the Controller and if the cause of the measure or fine being imposed is attributable to the Processor's failure to comply with the arrangements made in the Processor Agreement, the Controller can recover all costs for this measure or fine from the Processor. Furthermore, the Controller has the right to terminate the Agreement with immediate effect in the above situation without the Controller being entitled to any form of damages.

CLAUSE 12. CHANGE

12.1 If a change in the Personal Data to be processed or a risk analysis of the processing of Personal Data gives reason to do so, upon the Controller's first request the parties shall consult on amending the arrangements made in the Processor Agreement.

12.2 The arrangements to be newly made must be recorded in writing and form part of the Processor Agreement prior to their application.

12.3 The changes can never have the effect that the Controller cannot comply with the PDPA and other relevant laws and regulations relating to Personal data.

CLAUSE 13. TERM AND TERMINATION

13.1 The term of the Processor Agreement is equal to the term of the Agreement. The Processor Agreement cannot be terminated separately from the Agreement.

13.2 In the event of termination of the Agreement for any reason, or upon the Controller's first request during the term of the Agreement, the Processor shall - at a reduced fee not exceeding the costs reasonably and demonstrably incurred by the Processor - ensure that, at the discretion of the Controller, in a manner that is easily usable for the Controller, (i) all or part of the Personal Data as determined by the Controller made available in the context of the Service, will be destroyed at all locations, (ii) all or part of the Personal Data as determined by the Controller made available in the context of the Service, will be 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 or part of the Personal Data as determined by the Controller made available in the context of the Service. Where necessary, the Controller may set additional requirements on the manner of making available, including requirements on the file format, or destruction.

13.3 The Processor shall at all times ensure the data portability described in the previous paragraph in such a manner that there will be no loss of functionality or (parts of) data.

13.4 Obligations which, by their nature, are intended to continue after termination of this Processor Agreement, will continue to apply after termination of the Processor Agreement. These obligations include those ensuing from the provisions concerning Confidentiality, Indemnification and liability, and Applicable Law.

CLAUSE 14. CONFIDENTIALITY

14.1 In the event that the confidentiality of data is not provided for in the Agreement or elsewhere, the Parties shall keep confidential all (Personal) data and other information, the confidential nature of which they are aware of or can reasonably suspect, and that have come to their attention or to which they obtained access in the context of the performance of the Agreement or the Processor Agreement, and shall refrain from disclosing these internally or externally and/or providing these to third parties, except in so far as:

a. disclosure and/or provision of said (Personal) data and other information is necessary in the context of the performance of the Agreement or the Processor Agreement;
b. any mandatory statutory provision or court decision requires the Parties to disclose and/or provide said (Personal) data or other information, in which case the Parties shall first notify the other Party;
c. disclosure and/or provision of said (Personal) data and other information takes place with the prior written consent of the other Party; or
d. it concerns information that has already been legitimately disclosed in a manner other than through the acts or omissions of one of the Parties.

14.2 The Parties shall contractually require the persons working for them (including employees) who are involved in the processing of confidential (Personal) data to keep said (Personal) data and other information confidential.

14.3 Upon the other Party's request, the Parties shall cooperate in the exercise of supervision by or on behalf of the other Party on the safekeeping and use of confidential (Personal) data and other information by the other Party.

14.4 Upon the other Party's first request, the Parties shall provide the other Party with all (Personal) data and other information they hold in the context of the performance of the Agreement, including any copies.

CLAUSE 15. GOVERNING LAW AND DISPUTES

15.1 The Processor Agreement and its performance are governed by the laws of the Netherlands.

15.2 Any dispute which might arise between the Parties in connection with the Processor Agreement shall be submitted to the competent court in the place in which the Controller has its registered office.

NAME OF THE INSTITUTIO	**NAME OF THE SUPPLIER**
_____/_____/_____	_____/_____/_____
date	*date*
_____	_____
name	*name*
_____	_____
signature	*signature*

Annex A: Specification processing personal data

In this Annex, the following is set out regarding the Service provided by the Processor:

- Data Subject categories
- The Personal Data (categories) to be processed;
- Job roles and/or job groups and their Processing;
- Security measures taken;
- Auxiliary Suppliers;
- Contact details.

If the Processor offers multiple separate services to the Controller, the information may be included in separate Annexes to be numbered as follows: “Annex A1”, “Annex A2”, etc.

These Annexes will be attached to the Processor Agreement.

Annex A1: <NAME OF SERVICE>

Version number XX, Date of most recent update: XX-XX-XX

Data Subject categories

<Provide details as to who can be considered Data Subjects in the service.>

The personal data (categories) to be processed

The Processor will process the following Personal Data (categories) for the Controller. The Personal Data is not limited to what the Controller provides directly to the Processor, but includes Personal Data supplied by the User when using the Service.

<Fill in Personal Data (categories)>

The following risk class applies to the Agreement: <Fill in the applicable risk class, with an explanation if necessary>.

The Processor shall not retain Personal Data any longer than is necessary for the performance of this Agreement or to comply with any of its statutory requirements. The following retention periods apply for the Personal Data processed for the proper operation of the Service (logging, back-up facilities, etc.):

<Fill in the applicable retention periods>

Job roles/ job groups and their Processing

Table 1 sets out the job roles and/or job groups that have access to certain Personal Data, followed by the type of Processing they may perform with regard to the Personal Data.

Job (group)	Personal Data (category)	Type of Processing

Table 1: Groups of employees and their Processing

Security measures taken

<Additional details to be provided.>

Auxiliary Suppliers
The Processor has the Controller's permission to engage the following Auxiliary Suppliers in the performance of the Service:

Name of organisation: **<Name>**
Brief description of services: <fill in>
Extent of Personal Data Processing: <fill in>
Place/Country of Processing: <fill in>

Name of organisation: **<Name>**
Brief description of services: <fill in>
Extent of Personal Data Processing: <fill in>
Place/Country of Processing: <fill in>

Contact details
For questions on this Annex and/or the Service provided, please contact:
Name: **<name> (Supplier)**
Job: <fill in>
Email address: <fill in>
Telephone number: <fill in>

Name: **<name> (Institution)**
Job: <fill in>
Email address: <fill in>
Telephone number: <fill in>

To report a Data Breach within the meaning of Clause 5, please contact:
Name: **<name> (Institution)**
Job: <fill in>
Email address: <fill in>
Telephone number: <fill in>

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

Version number XX, Date of most recent update: XX-XX-XX

If the Processor must inform the Controller pursuant to Clause 5, it shall provide the following information:

Contact details of reporter

Name, job, email address, telephone number

Information on the Data Breach

- Provide a summary of the incident, in which the breach of the security of Personal Data occurred
- Of how many persons are Personal Data involved in the breach? (Fill in the numbers.)
  a) Minimum: (fill in)
  b) Maximum: (fill in)
- Describe the group of people whose Personal Data are involved in the breach
- When did the breach take place? (Choose one of the following options and supplement where necessary.)
  a) On (date)
  b) Between (start date of period) and (end date of period)
  c) Not yet known
- What is the nature of the breach? (You can check more than one option.)
  a) Reading (confidentiality)
  b) Copying
  c) Changing (integrity)
  d) Removing or destroying (availability)
  e) Theft
  f) Not yet known
- What type of Personal Data is involved? (You can check more than one option.)
  a) Name and address details
  b) Telephone numbers
  c) Email addresses or other addresses for electronic communication
  d) Access or identifying information (e.g. log-in name/password or client number)
  e) Financial information (e.g. account number, credit card number)
  f) Citizen Service Number (BSN) or tax and social security number
  g) Copies of passport or other identification documents
  h) Gender, date of birth and/or age
  i) Special Personal Data (e.g. race, ethnicity, criminal information, political conviction, trade union membership, religion, sex life, medical details)

j) Other information, namely (supplement)

- What consequences can the breach have for the privacy of the data subjects? (You can check more than one option.)
  a) Stigmatisation or exclusion
  b) Damage to health
  c) Exposure to (identity) fraud
  d) Exposure to spam or phishing
  e) Other, namely (provide details)

Follow-up actions in response to the Data Breach

- What technical and organisational measure did your organisation take to address the breach and to prevent further breaches?

Technical protection measures

- Have the Personal Data been encrypted, hashed or made incomprehensible or inadmissible to unauthorised persons in any other way? (Choose one of the following options and supplement where necessary.)
  a) Yes
  b) No
  c) Partly, namely: (supplement)
- If all or part of the Personal Data was made incomprehensible or inaccessible, in what manner was this done? (Answer this question if you chose option a or option c for the previous question. If you used encryption, also explain the manner of encryption.)

International aspects

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