Samen aanjagen van vernieuwing

SURF Model Processing Agreement

SURF Legal framework of standards for cloud and other services

Version: 3.0

Date: January 2019

Moreelsepark 48
3511 EP Utrecht, the Netherlands

Postbus 19035
3501 DA Utrecht, the Netherlands

+31 88 - 787 30 00
info@surf.nl
www.surf.nl

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;

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

- 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.

AND HAVE AGREED AS FOLLOWS:

ARTICLE 1. DEFINITIONS

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

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

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

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

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

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

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

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

1.8 Sub-processor: another processor, including but not limited to group companies, sister companies, subsidiaries and auxiliary suppliers, engaged by the Processor to 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.

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

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

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

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.

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.

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.

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.

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.

3.2 The provision of assistance and cooperation with regard to meeting the 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 the data subject can exercise his rights.

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

3.2.3 If the Processor offers the Service directly to the Data Subject, the Processor is obliged to inform the Data Subject on behalf of the Controller about the Processing of the Personal Data of the Data Subject in a manner that is in accordance with the rights of the Data Subject.

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

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

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

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

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

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

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

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 .

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

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

4.5 The Processor shall inform the Controller in the event of general consent In Writing 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.

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

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

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

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.

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.

ARTICLE 5. SECURITY

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

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.

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.

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.

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.

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.

6.4 At its request, the Controller is entitled to have an audit carried out by an expert authorised by the Controller with regard to the Processor's organisation, in order to demonstrate that the Processor complies with the provisions of the Processing Agreement, the GDPR and other applicable laws and regulations concerning the Processing of Personal Data. The Controller may, no more than once a year, exercise the right

to have an audit carried out at the Processor, as referred to in this paragraph, or more often in the event of a concrete suspicion that the Processor is in breach of the Processing Agreement and/or the GDPR and/or other applicable laws and regulations regarding the Processing of Personal Data. The Controller shall notify the Processor In Writing at least 14 (fourteen) days before the start of the audit. The audit must not unreasonably interfere with the normal business activities of the Processor.

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

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

ARTICLE 7. PERSONAL DATA BREACH

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

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

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.

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.

ARTICLE 8. TRANSFER OF PERSONAL DATA

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

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, except insofar as:

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

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

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

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.

ARTICLE 11. AMENDMENTS

11.1 the Processor is obliged to immediately inform the Controller of intended changes to the Service, the execution of the Agreement and the execution of the Processing Agreement that relate to the Processing of Personal Data and that (may) require a change to the Processing Agreement and/or the Annexes. This is in all cases understood to mean:

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

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

(iii) Engaging other Sub-processors;

(iv) Change in the transfer of Personal Data.

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

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

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

ARTICLE 12. DURATION AND TERMINATION

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

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

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

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

12.5 The Processor shall bear the costs of destruction, return and/or transfer of the Personal Data. The Controller may impose further requirements on the manner of destruction, return and/or transfer of the Personal Data, including requirements on the file format. The transfer of Personal Data is based on an open file format. The Parties will agree in joint consultation on a reasonable distribution of any additional costs for the further requirements.

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

ARTICLE 13. APPLICABLE LAW AND DISPUTE RESOLUTION

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

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

THUS AGREED BY THE PARTIES:

[NAME OF CONTROLLER] [NAME OF PROCESSOR]

_____/_____/_____ _____/_____/_____

Date *Date*

_____ _____

Name *Name*

_____ _____

Signature *Signature*

Annex A: Specification of the Processing of Personal Data

Version No 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.

Description of the Processing

Purposes of the Processing *(to be completed by the Controller*)

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

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

Frequency of audits *(to be completed by the Controller*)

Retention period of the Personal Data or the criteria for determining this *(only complete if applicable)* *(to be completed by the Controller*)

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**

Sub-processors

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

□ General permission to engage Sub-processors.

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

The Sub-processors engaged by the Processor are:

Sub-processor engaged by the Processor for the Processing of Personal Data	**Categories of Personal data processed by Sub-processor**	**Type of Processing**	**Country of Processing**	**Country of establishment of the Sub-processor**

<u>Transfers outside the European Economic Area</u>

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

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

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				

Annex B: Security measures

Version No 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 certificate	Declaration of applicability