Tilburg University Model Processor Agreement

Version: 3.0

Date: October 2021

THE UNDERSIGNED:

**Tilburg University[[1]](#footnote-1),** with its registered office at Warandelaan 2in Tilburg (Netherlands), Chamber of Commerce number **41095855** and legally represented by **<REPRESENTATIVE>** (hereinafter referred to as: “**the Controller**”);

and

**<NAME PROCESSOR>,** with its registered office at <ADDRESS>in <CITY>, Chamber of Commerce number <COC> 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> (hereinafter: “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, < PROCESSOR’S NAME> is to be regarded as the Processor within the meaning of the GDPR and <INSTITUTION’S NAME> is to be regarded as the Controller within the meaning of the GDPR;
* The Parties wish to handle the Personal Data that are 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 the Personal Data of Data Subjects in writing in this Processor Agreement.

AND HAVE AGREED AS FOLLOWS:

**ARTICLE 1.**  **DEFINITIONS**

In this Processor Agreement, capitalised terms have the meaning given in the GDPR or, in case a meaning in the GDPR is missing, 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.

**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 Third Party**: a natural or legal person, public authority, agency or body other than the Data Subject, the Controller or the Processor, or the person who, under the direct authority of the Controller or Processor, is authorised to process Personal Data, as referred to in Article 4 at 10) GDPR.

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

**1.4 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.

**1.5 In Writing**: in writing or electronically, as referred to in Book 6, Article 277a of the Dutch Civil Code.

**1.6 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.

**1.7 Applicable Laws and Regulations regarding the Processing of Personal Data**: the applicable laws and regulations and/or (further) treaties, regulations, directives, decrees, policy rules, instructions and/or recommendations from a competent public body concerning the Processing of Personal Data, also including future amendments of and/or supplements thereto, including laws of the Member States implementing the GDPR and the Telecommunications Act.

**ARTICLE 2.**  **OBJECT OF THE PROCESSOR AGREEMENT**

2.1 The Processor Agreement forms an addition to the Agreement. In the event of any conflict between the provisions of the Processor Agreement and the Agreement, the provisions of the Processor Agreement shall prevail.

2.2 The provisions of the Processor 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 Processor Agreement.

2.3 The Controller assigns and instructs the Processor to process the Personal Data on behalf of the Controller. The Controller’s instructions are described in more detail in the Processor Agreement and the Agreement. To this end, amongst other things, Annex A will be filled in. The Controller may issue reasonable supplementary or deviating instructions In Writing.

2.4 The Processor shall process the Personal Data exclusively on the orders of the Controller and on the basis of the instructions of the Controller. The Processor shall only process the Personal Data to the extent that the processing is necessary for the performance of the agreement, and never for its own benefit, 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 the Processing, unless such legislation prohibits such notification for important reasons of public interest.

2.5 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.

**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:

1. The security of Personal Data;
2. Performing checks and audits;
3. Performing DPIAs;
4. Prior consultation with the Supervisory Authority;
5. Responding to requests from the Supervisory Authority or another government body;
6. Responding to requests from Data Subjects;
7. Reporting Personal Data Breaches.

3.2 The provision of assistance and cooperation with regard to meeting the requests from Data Subjects is understood to include, but is not limited to, the following obligations for 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, in relation to the exercise of his rights, a Data Subject contacts the Processor directly, the Processor shall not (substantively) respond to this - unless expressly instructed otherwise by the Controller - but shall 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 Data Subject’s Personal Data 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 is understood to include, but is not limited to, the following obligations for the Processor:

3.3.1 If the Processor receives a request or order concerning Personal Data from a Dutch and/or foreign public body, including but not limited to a request from the Supervisory Authority, the Processor shall immediately notify the Controller in so far as this is permitted by law. When handling the request or order, the Processor shall observe all of the Controller’s instructions and provide to the Controller all reasonably required 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’s. 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 posslbie, 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.

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

4.3 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.

4.4 The general or specific consent of the Controller for engaging Sub-processors shall not affect the obligations of the Processor arising from the Processor 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 Processor Agreement, the GDPR and/or other Applicable Laws and Regulations regarding the Processing of Personal Data.

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

The Processor guarantees that the persons authorized 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.

4.6 At the request of the Controller, the Processor shall provide evidence that the Processor, Sub-processors engaged by the Processor, the persons authorized to process the Personal Data and other Recipients of Personal Data comply with Article 4.5.

4.7 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 Processor 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 describe the technical and organisational measures and Processor shall review and assess these measures, as included in Annex B.

5.2 As proof of compliance with the technical security measures set forth in Annex B, the Processor shall submit a recent (not older than 12 months) IT Security report[[2]](#footnote-2), executed by a renowned IT-security company, possibly under a Non Disclosure Agreement. If the Processor does not want to or cannot deliver such a report, the Processor must inform the Controller’s General contact person and the IT Security Officer of this with reasons. The Controller will then decide whether the report can be omitted.

5.3 In assessing the appropriate level of security, the Processor shall take into account the state of the art, the costs 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.

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

5.5 Adherence to an approved code of conduct as referred to in Article 40 GDPR or an approved certification mechanism as referred to in Article 42 GDPR may be used as an element to demonstrate compliance with the requirements referred to in this Article.

**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 Agreement, the Processor 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 as referred to in Article 6.1 at least once a year.

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. The Controller determines whether there is a low risk, taking into account the Guidelines for Supplier Audit Obligations (Appendix of the SURF Framework of Legal Standards for (Cloud) Services).

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 Processor 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 Processor 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 Processor 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 Processor Agreement and/or the GDPR and/or other Applicable Laws and Regulations concerning the Processing of Personal Data.

6.7 If it is established during an audit that the Processor is not complying with the provisions of the Processor 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 or a reasonable suspicion of a Personal Data Breach without unreasonable delay and within 24 hours after discovery 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 policy and procedures in place to ensure that it can detect Personal Data Breaches at the earliest possible stage, inform the Controller of this in accordance with Article 7.1, respond adequately and immediately to this, 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 consent In Writing 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 must be treated as such.

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

1. Disclosure and/or providing of the Personal Data is necessary in the context of the performance of the Agreement or the Processor Agreement;
2. Any rule of mandatory Union or Member State law or a judicial decision of a competent judicial body 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;
3. 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 Processor 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 Processor 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 defense 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 Processor Agreement that relate to the Processing of Personal Data and that (may) require a change to the Processor Agreement and/or the Annexes.

11.2 The Processor is only authorised to make a change as referred to in Article 11.1 if the Controller has given prior Written consent for such 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 In the event of nullity or voidability of one or more provisions of the Processor Agreement, the other provisions shall remain in full force and effect.

**ARTICLE 12. DURATION AND TERMINATION**

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

12.2 The Controller is entitled to dissolve the Processor Agreement if the Processor fails to comply or can no longer comply with the Processor Agreement without the Processor being entitled to 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 for the 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 Processor Agreement which by their nature are intended to continue after termination of this Processor Agreement shall continue to apply after termination of the Processor Agreement.

**ARTICLE 13. APPLICABLE LAW AND DISPUTE RESOLUTION**

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

13.2 All disputes arising 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.

THUS AGREED BY THE PARTIES:

**Tilburg University  [NAME OF THE PROCESSOR]**

**<Fill in date>  <Fill in date>**

**<Fill in name> <Fill in name>**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Signature Signature*

**Annex A: Specification of the Processing of Personal Data**

Version number 1, Date of most recent update: XX-XX-XX

*PLEASE 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 Processor Agreement.*

|  |
| --- |
| **Description of the Processing** *(to be completed by the Processor)* |
|  |

|  |
| --- |
| **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)* |
|  |
|  |
|  |

|  |
| --- |
| ***Risk class****Low (Public level): Public Personal Data (e.g. business email address on the internet)Normal: Non-public Personal Data but not including Special categories of Personal Data (e.g. enrollment as a student)High: Special categories of Personal Data(to be completed by the Controller)* |
|  |

|  |
| --- |
| **Frequency of audits and motivation if no audit is required when taking into account the Guidelines for Supplier Audit Obligations (as referred to in Article 6.1-6.2)***(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** *(to be completed by the Processor)*

|  |  |  |  |
| --- | --- | --- | --- |
| **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 [*where applicable to be selected by the Controller*]:

□ General consent for the engagement of Sub-processors (as referred to in Article 4.2).

□ Specific consent for the engagement of 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** | **(category of) Personal Data processed by the Sub-processor** | **Type of Processing** | **Country of Processing** | **Country where Sub-processor’s registered office is located** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Transfers outside the European Economic Area**

The Controller has given the Processor specific permission for the following transfers to third parties 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 details**

**General contact person:**

Controller

Name: <to be completed>

Position: <to be completed>

Email address: <to be competed>

Telephone number: <to be completed>

Processor:

Name: <to be completed>

Position: <to be completed>

Email address: <to be completed>

Telephone number: <to be completed>

*If a (suspicion of a) Personal Data Breach occurs, the Processor shall inform the General Controller’s contact person as well as the Controller’s Data protection officer.*

**Data protection officer (DPO):**

Controller:

Name: M.R.G. Herregodts

Position: DPO

Email address: fg@tilburguniversity.edu

Telephone number: +31 13 466 3359

Telephone number outside office hours/in emergency

(through the Computer Emergency Response Team): +31 13 466 3095

Processor:

Name: <to be completed>

Position: <to be completed>

Email address: <to be completed>

Telephone number: <to be completed>

Telephone number outside

office hours / in emergency: <to be completed>

**Annex B: Security Measures**

Version number 1, Date of most recent update: XX-XX-XX

The Processor describes the security measures implemented. The Controller will verify if these measures comply with the Guidelines for Security Measures (appendix to the [SURF Framework of Legal Standards for (Cloud) Services](https://www.surf.nl/en/knowledge-base/2013/surf-framework-of-legal-standards-for-cloud-services.html)) and the [Security Technical IT Checklist (STITCH)](https://www.surf.nl/files/2020-07/scirt-stitch1.0-english.pdf). The Processor proves by submitting an IT Security report from an independent tester that the STITCH requirements have been met.

For the testing of the technical and organizational security measures, the internal Procedure Security Check is followed.[[3]](#footnote-3) The assessment of the test is recorded in this Annex under a.

1. **Assessment test security measures**

|  |
| --- |
| **Assessment (color code):**  |

1. **SURFconext-connection**

Credentials (user name and password) in (web) applications are only sent or received in encrypted form. The basic principle is that use is made of SURFconext (which provides a Single Sign On (SSO) environment), unless this is impossible or not proportionate. Processor does not store Controller's credentials.

|  |
| --- |
| **Does the Processor use the SSO environment of the Controller?***(to be completed by the Processor)* |
| Yes/No |
| **If No, please explain:** |
|  |

**Maintenance and duration**

The security requirements apply continuously, for as long as the software is used. The Processor shall actively ensure that vulnerabilities are remedied within a reasonable period. Tilburg University CERT is the Computer Emergency Response Team of the Controller that periodically checks for vulnerabilities and monitors the SSL configuration of the software and/or service.

**Annex C: Adjustments to standard text << OPTIONAL >>**

Preferably, the entire text of the model agreement will be maintained, with the exception of Annexes A and B, which must be completed specifically for each agreement.

If additional changes to the text are nevertheless necessary (following negotiations between the Controller and Processor), then the changes can be described in this Annex, stating

* Article number,
* Relevant text from the model that has been deleted
* New replacement text
* Reason for change (e.g., N/A, requirement not acceptable to Processor, negotiated, etc.)

|  |  |  |  |
| --- | --- | --- | --- |
| **Art.** | **Text deleted** | **Replacement text** | **Reason**  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Tilburg University was established by the Stichting Katholieke Universiteit Brabant [↑](#footnote-ref-1)
2. This does not refer to a ISO 27001 certification. [↑](#footnote-ref-2)
3. See [Procedure Security Check](https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security/secure-software/security-requirements). [↑](#footnote-ref-3)