



Processing Agreement

The undersigned:

Stichting Fontys, established at Rachelsmolen 1, Eindhoven, duly represented by <<name>>, <<position>>, to be referred to as: the "Client", hereinafter called the "Controller"

and

<<name of the Processor>>, established at <<place name>>, duly represented by <<name>>, <<position>>, to be referred to as: the "Contractor", hereinafter called the "Processor"

jointly to be referred to as the 'Parties',

Whereas:

- The Controller considers it necessary to have various activities relating to the processing of Personal Data carried out by the Contractor in its capacity of Processor;
- The Parties have agreed to comply with the following stipulations in respect of the processing of those Personal Data by the Processor;

by signing the present Processing Agreement have agreed on the following.

Article 1. Definitions.

1.1 **General Data Protection Regulation** (GDPR) means Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), which became applicable throughout the EU on 25 May 2018.

1.2 **Data subject** means the identified or identifiable natural person to whom the Personal Data relate, as defined in the GDPR.

1.3 **Processor** means the Contractor, being the party which processes Personal Data on behalf of the Controller, without being under the latter's direct authority.

1.4 **Processing Agreement** means the present Agreement.

1.5 **Appendices** means appendices to the Agreement which form part of the present Agreement.

1.6 **Special Categories of Personal Data**: Personal data are data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and/or genetic and biometric data, data concerning health, a person's sex life or criminal record.

1.7 **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed as referred to in Article 4(12) of the GDPR;

1.8 **Employee** means the employees and other persons engaged by the Processor whose activities fall under the latter's responsibility and who are engaged by the Processor in order to execute the Agreement.

1.9 **Recipient** means a natural or legal person, public authority, agency or another body, to which the Personal Data are disclosed, whether a third party or not (Article 4(9) of the GDPR).

1.10 **Norms and Standards** means the safety standard ISO 27001/2 adhered to by the Controller

1.11 **Personal data** means any information relating to a Data Subject; any data relating to an identified or identifiable natural person which is or will be processed by the Processor in any way whatsoever for the purposes of the Agreement.

1.12 **Sub-processor** means the party processing Personal Data on the instructions of the Processor.

1.13 **Controller** means Stichting Fontys, also referred to as the Client, being the legal person which determines the purposes and means of the processing of personal data.

1.14 **Processing of Personal Data** means any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Article 2 Subject of this Agreement

2.1 The Processor shall undertake vis-à-vis the Processing of Personal Data to process the Personal Data of the Controller fairly and with due care.

2.2 The present Processing Agreement shall replace any previous agreements between the Parties in respect of the Processing of Personal Data.

2.3 The Parties shall record the way in which the Personal Data are made available to the Processor and which operations the Processor shall perform in respect of Personal Data.

2.4 The Processor shall be responsible for ensuring that Employees of the Processor and anyone else engaged by the Processor adhere to the provisions of privacy Legislation and the provisions of the present Agreement, if and in so far as they are in any way involved in the Processing of Personal Data.

2.5 The Processor shall not keep Personal Data made available to it for any longer than is necessary (i) to perform the activities for the Controller, or (ii) to comply with a legal obligation incumbent on it.

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

Article 3. Duration and Termination

3.1 The Processor shall bear the costs of destruction, return and/or transfer of the Personal Data once the activities for the Controller have ended. The Controller may impose further requirements regarding the manner of destruction, return and/or transfer of the Personal Data, including requirements regarding the file format.

3.2 Obligations which by their nature are intended to continue after termination of this Processing Agreement shall continue to apply after its termination. Examples of such obligations include those arising from the provisions concerning confidentiality, indemnity and liability, and applicable law.

Article 4. Obligations of the Controller

4.1 The Controller shall be responsible for data processing within the meaning of the relevant privacy legislation.

4.2 The Controller declares that it shall notify the Processor of any changes related to processing within 14 working days, and shall also inform the Processor of any implications a change may have.

Article 5. Obligations of the Processor

5.1 Before the Processing Agreement is entered into, the Processor shall provide the Controller with a full and truthful specification of the Processing Operations it will be performing in Appendix 1. The Processor shall be entitled to perform only the Processing Operations specified in Appendix 1.

5.2 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. The Processor shall in any event provide the Controller with all reasonable measures, assistance and cooperation relating to (a) the security of Personal Data; (b) Performing checks and audits; (c) Performing Privacy Impact Assessments; (d) Prior consultation with the Supervisory Authority; (e) Responding to requests from the Supervisory Authority or another public authority; (f) Responding to requests from Data Subjects; (g) Reporting Personal Data Breaches.

5.3 The Processor shall notify the Controller without delay if the Processor considers that an instruction of the Controller breaches the GDPR and/or other applicable laws and regulations concerning the Processing of Personal Data and shall enable the Controller to meet its obligations under privacy legislation within the statutory deadlines at all times, in particular those pertaining to the rights of Data Subjects, including but not limited to requests for access to, rectification, supplementation, removal or protection of Personal Data and to have an objection that has been lodged and accepted dealt with.

5.4 The Processor shall not deal substantively with arguments of a Data Subject relating to the exercise of the latter's rights, but shall notify the Controller and request further instructions.

5.5 The Processor shall, at the request of the Controller, immediately submit to the Controller all data originating from the Controller and/or data processed on the instructions of the Controller relating to this Agreement.

5.6 The Processor shall, at the request of the Controller, immediately destroy all duplicates and copies of data originating from the Controller and/or data processed on the instructions of the Controller and relating to the Controller.

5.7 The services provided by the Processor shall demonstrably comply with the sectoral standards for information security and privacy, including:

- [the security measures set out in appendix 6 \(based on the Surf Legal Standards Framework Cloud Services, the SURF Security Baseline for Education and Research, version 2.0 \(September 2024\) \(link to SURF PDF\), and, and](#)

- the SURFaudit Information Security Assessment Framework.

Article 6. Access to and disclosure of Personal Data

6.1 The Processor shall restrict access to Personal Data by Employees, sub-processors, third parties and other recipients of Personal Data to a necessary minimum and with the knowledge of the Controller. The Processor shall give access only to those Employees who require access to Personal Data in order to be able to perform the activities for the Controller.

6.2 The Processor shall be entitled to subcontract the execution of the Agreement in whole or in part only with the prior written permission of the Controller. The Controller cannot reasonably withhold permission. The Controller may attach conditions to its permission, including but not limited to the preparation of a written agreement with a third party setting out the third party's obligation to act solely on, and in accordance with, the instructions of the Processor and in accordance with all the provisions of this Agreement, in the area of secrecy and security and to ensure compliance with the obligations of this Agreement. The Processor shall at all times remain the contact point and be responsible for compliance with the provisions of this Agreement.

6.3 The Processor shall notify the Controller without delay if the Processor and/or legal or other persons engaged by the Processor breach the Processing Agreement.

Article 7. Disclosure of Personal Data

7.1 The Processor shall not be permitted to disclose Personal Data unless this is done at the written request of the Controller or the Controller has given written permission for such disclosure by the Processor. The Processor shall be obliged to confirm in writing that such disclosure has taken place, stating precisely which Personal Data were disclosed, the Data Subject or Data Subjects, the Recipient or Recipients and the time of disclosure. The Controller shall retain data disclosed in derogation of the provisions for three years.

7.2 If a statutory provision requires the Processor to disclose personal or other data, the Processor shall verify the basis of the request and the identity of the party making the request and shall inform the Controller without delay, where possible before the disclosure.

Article 8. Security

8.1 The Processor shall secure the Processing of Personal Data in accordance with the provisions laid down by or pursuant to privacy legislation and by or pursuant to other (special) legislation pertaining to the processing of Personal Data. In addition, the Processor shall adhere to the Norms and Standards of the Controller, with the security standard ISO27001/2 being the reference standard.

8.2 The Processor shall ensure that its security policy and the implementation of its security policy at least meet the criterion of an "appropriate level of security" and appropriate technical and organisational measures shall be taken by the Processor to protect Personal Data against loss or any form of unlawful processing.

8.3 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, as well as the risk of varying likelihood and severity for the rights and freedoms of persons, in particular as a result of the destruction, loss, alteration or unauthorised disclosure of or unauthorised access to data transmitted, stored or otherwise processed.

8.4 The Processor shall make every effort to secure and keep secured the Personal Data to be processed against intruders and external contingencies, as well as careless, inexperienced or unauthorised use, and shall record its security policy in writing and provide the Controller with access to the security policy.

8.5 The Processor shall permit the Controller to give instructions regarding the application by the Processor of measures to secure Personal Data.

Article 9. Audit

9.1 The Processor shall be obliged to have an independent external expert carry out a periodic audit of the organisation of the Processor in order to demonstrate that the Processor is complying with the provisions of the main or other agreement, the Processing Agreement, the GDPR and other applicable laws and regulations concerning the Processing of Personal Data.

9.2 The Processor shall carry out a periodic audit at least once every two years, unless Special Categories of Personal Data are being processed, in which case the Processor shall carry out a periodic audit at least once a year.

9.3 The Processor shall be obliged to make the findings of the independent external expert available to the Controller upon request.

9.4 An audit may also be carried out at the request and expense of the Controller. The costs of an audit requested by the Controller shall be borne by the Processor if the findings of the audit show that the Processor has failed to comply with the provisions of the Processing Agreement, such being without prejudice to the right of the Controller to compensation.

9.5 If it is established during an audit that the Processor is not complying with the provisions of the Processing Agreement, the Processor shall immediately take all reasonably necessary measures to ensure its compliance.

Article 10. Personal Data Breach

10.1 The Processor shall notify the Controller of a Personal Data Breach or a reasonable suspicion of a Personal Data Breach immediately upon the discovery thereof. The notification to the Controller shall in any case include the nature of the breach, the authorities from which further information about the breach may be obtained and the measures recommended to mitigate the adverse effects of the breach.

10.2 The notification to the Controller of a Personal Data Breach or a reasonable suspicion of a Personal Data Breach shall also contain a description of the established or suspected effects of the Breach on the Processing of Personal Data and the measures the Processor has taken or intends to

take to remedy those effects. At the request of the Controller, the Processor shall participate in the Controller's Duty to Notify a Personal Data Breach Protocol, where a Personal Data Breach has occurred within the responsibility of the Processor.

10.3 The Processor shall undertake to notify the Controller in writing without delay of an incident (through the contact person named in Appendix 1) if a person who is not authorised to access Personal Data has obtained disposal over some or all of it, or has had (permanent or temporary) access to it. The Processor shall take all reasonably necessary measures at its own expense to prevent or limit any further unauthorised processing and to put an end to the situation and prevent the recurrence of any such situation, without prejudice to the Controller's right to compensation.

Article 11. Confidentiality

11.1 The Processor shall be obliged to keep confidential all Personal Data and information it processes as a result of this Agreement, except to the extent that those data or that information manifestly lack or lacks a secret or confidential nature, or is or are already common knowledge.

11.2 If and in so far as the Controller expressly requests such in writing, the Processor shall take measures in respect of the data or information in question in order to safeguard them or it, which measures may include the destruction of the data or information concerned as soon as the Processor no longer requires access to it.

11.3 In its agreements with Employees of the Processor, subcontractors and anyone else acting under the responsibility of the Processor, the Processor shall stipulate that those persons must maintain confidentiality in the same manner as provided for in Articles 10.1 and 10.2 in respect of all data and information they process in connection with their activities for the Processor. The Processor shall warrant to the Controller that the persons concerned will comply with the aforementioned stipulations.

11.4 Following the termination of this Agreement, Article 10 and the confidentiality referred to in it shall remain in force and all Personal Data in the possession of the Processor shall be transferred to the Controller and removed from the Processor's data carriers.

Article 12. Transfer of Personal Data/International Flows

12.1 The Processor shall guarantee that all Processing of Personal Data which is performed by or on behalf of the Processor, including by third parties it has engaged in connection with the execution of the Agreement will take place within the European Economic Area (EEA). The Processor shall not transfer, store, or make Personal Data accessible from any country outside the EEA.

12.2 If the technical characteristics of a transmission medium require data to be transmitted, such transmission shall be conducted exclusively in encrypted form, with advanced (that is, at least as advanced as is customary on the market) technologies used for the encryption. Before entering into the Processing Agreement, the Processor shall provide information about the location or locations where Processing is to take place.

Article 13. Liability

13.1 If the Processor fails to fulfil its obligations under this Agreement, the Processor shall be in default after the period given for written notice of default has expired.

13.2 The Processor shall be liable for all loss or damage arising from the failure to comply with, or the breach of, the provisions under or pursuant to privacy legislation and/or the failure to comply with, or the breach of, the provisions in this Agreement, without prejudice to claims based on other statutory rules. The Processor shall be liable for loss or damage to the extent that such was caused by its activities and also to the extent that such can be attributed to a fault in the security features, the security level and/or the security of the Processor's system.

13.3 The Processor shall also be liable for all loss or damage arising from invasions of the privacy of Data Subjects caused by its activities.

13.4 The Processor shall indemnify the Controller against loss as a result of claims by third parties, penalties and/or measures of third parties, including Data Subjects and the Supervisory Authority,

based on non-compliance with the provisions under or pursuant to privacy legislation or other laws and regulations and this Processing Agreement by the Processor.

13.5 If the Processor fails to comply with the obligations set out in this Agreement in time, the Processor shall be liable to pay a penalty of €25,000 per breach, without a demand or other prior declaration being required. Any such penalty cannot be set off or suspended and shall be without prejudice to the Controller's right to compliance and compensation.

Article 14. Property rights

14.1 All industrial or intellectual property rights relating to the Personal Data to be processed or which have been processed under this Agreement shall be vested at all times in the Controller.

14.2 All external data carriers, including but not limited to, CD-ROMs, USB sticks or paper, containing data or Personal Data shall be regarded as fully owned by the Controller. The Processor shall never claim any right in respect of the data concerned nor be entitled to any form of exploitation other than provided for in this Agreement.

Article 15. Other provisions

15.1 The complete or partial invalidity of one or more provisions of this Agreement shall not render the entire agreement null or void. In so far as the aforesaid invalidity pertains to an essential element of the relationship between the Parties, the Parties shall establish by negotiation which amendments in the Agreement necessarily arise as a result of the invalidity, and the amendment shall as far as possible reflect the intention of the Parties as shown in this Agreement.

15.2 This Agreement may be amended only by means of a written document which expressly states that the document is intended to introduce such an amendment and that it has been signed by representatives of the Parties authorised to do so.

Article 16. Disputes, applicable law and jurisdiction

16.1 Disputes, applicable law and jurisdiction shall be ruled on by the Court at East Brabant.

Date:

.....

Controller

.....

Processor

Stichting Fontys

.....

Appendix 1A-1: Concerning the Processing

(to be completed by the Processor (with the assistance of the Controller, if applicable)).

Description and purpose of the Processing

.....

Categories of Data Subjects (persons who personal data are processed)

.....

The (categories of) personal data to be processed (type of personal data being processed, e.g. name, address, etc.)

.....

Security measures taken

.....

Categories of Employees

Categories of employees (job roles/job groups) of the Processor who process Personal Data	(category) Personal Data processed by Employees	Type of Processing	Country of Processing

Sub-processors

Sub-processor engaged by the Processor for the Processing of Personal Data	(category) Personal Data processed by Sub-processor	Type of Processing	Country of Processing	Country of Establishment of Sub-processor

Transfers outside the European Economic Area

.....

Controller's contact person or persons

General contact details	Name	Function/role	E-mail address	Phone number
Datacontroller				
Processor				

Contact details in case of a Personal Data Breach	Name	Function/role	E-mail address	Phone number
Datacontroller	1st line: 2nd line: 3rd line:			
Processor				