SURF Model Data Processing Agreement 4.0

STRUCTURE OF THIS DOCUMENT AND NOTES

1. This SURF Model Data Processing Agreement can be used for *all* situations in which a SURF member engages a processor, i.e. for education, educational logistics, research and business operations.*
   When is a party a 'processor' as defined by the GDPR? That is the case if the SURF member:
   - engages a third party,
   - who, on the SURF member's instructions
   - and on their behalf, processes personal data,
   - for purposes and using resources that are determined solely by the SURF member (and therefore not also by the processor), and
   - for which the processor is allowed to determine non-essential resources (such as the hardware or software used to process the data) for the data processing activities.
2. Please contact the Legal Affairs department or your own institution's Privacy Office for more support, particularly for risk assessment of transfers outside the EEA. The institution may make use of the SURF Assessment Framework ((https://www.surf.nl/toetsingskader) as a tool to assess a transfer.
3. This model was drafted in compliance with the *EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR (07 July 2021)* and comprises all obligations included in Article 28(3) of the GDPR.
4. The model is a stand-alone document and contains a reasonable division of tasks and risks concerning the processing of personal data. However, certain situations may warrant the selection of variants or optional provisions. These variants and optional provisions are included in boxes and highlighted in red. It is up to the SURF member to make an informed choice based on a risk assessment of the processing. The SURF member must delete any unselected red text before sending the draft agreement out.
5. The model also contains a number of passages marked in yellow. Here the SURF member should add specific variable information or make an informed choice. The appendices must also be filled out and completed.

The model allows for the possibility to permit the processor to use the personal data for very specific purposes ('of their own'). In that case, the processor is considered the data controller for its own data processing activities. These processing activities must be explicitly described in the agreement itself.

* *Secondary vocational education (MBO) has its own model processing agreement tailored to the education sector. The SURF Model Data Processing Agreement replaces the MBO Model and may not be used alongside the MBO Model.*

Delete the text on this page (the header, the notes up to and including this bar) and select the text in red in the document before sending out a draft or final agreement based on this model. Replace the logo in the header.

Data Processing Agreement

THE UNDERSIGNED PARTIES:

<NAME OF INSTITUTION>, domiciled in <ADDRESS> in <TOWN/CITY>, and legally represented by <REPRESENTATIVE> (hereinafter: **"The Controller")**

and

<NAME OF SUPPLIER/PROCESSOR>, domiciled in <ADDRESS> in <TOWN/CITY>, and legally represented by <REPRESENTATIVE> (hereinafter: **"The Processor"**)
hereinafter jointly referred to as: "**The Parties**" and individually as: **"The Party";**

WHEREAS:

- the Parties entered into an agreement (in writing or by electronic means through an electronic ordering process) on <DATE> with regard to <SUBJECT OF THE AGREEMENT> (hereinafter: "**the Agreement**");
- the Processor processes personal data for the Controller in the course of performing this Agreement;
- the Parties wish to put down in writing their rights and obligations with respect to the processing of personal data of data subjects, in accordance with the General Data Protection Regulation (GDPR), in this processing agreement (hereinafter: **"Data Processing Agreement"**)

HAVE AGREED AS FOLLOWS:

ARTICLE 1 DEFINITIONS AND MISCELLANEOUS

1.1 The terms in capitalized letters in this Data Processing Agreement have the same meaning as those in Article 4 GDPR, unless defined otherwise.

1.2 The provisions of this Processing Agreement apply to all Personal Data Processing activities conducted by the Processor for the Controller in the context of the services he provides to the Controller based on the Agreement. This Personal Data and these Processing activities are listed and described in more detail in Annex A.

1.3 The appendices to this document and any later modifications or additions are part of this Data Processing Agreement.

ARTICLE 2 PURPOSE OF THE AGREEMENT

2.1 The Processor only processes Personal Data:

(i) on the instructions of the Controller,
(ii) according to his reasonable written instructions, and
(iii) as far as the Processing activities are necessary to perform the Agreement and this Data Processing Agreement.

OPTIONAL - ALLOW FOR OPTION TO PROCESS FOR ADDITIONAL, OWN DEFINED PURPOSES

2.1.1 The Processor may also process the Personal Data for own internal purposes:

(ii) EXAMPLE: [to improve their own service provisioning including further specification/elaboration],
(ii) EXAMPLE: [to analyse the use of their own service including further specification/elaboration],
(iii) EXAMPLE: ....

For these Processing activities, the Processor is considered the Controller as defined under the GDPR. The obligations included in Articles 2.2 and 6.1 apply accordingly to these Processing activities.

2.2 The Processor carries out all Processing activities of Personal Data in accordance with the GDPR and other applicable data protection legislation and regulations, such as the GDPR Implementation Act and the Telecommunications Act (hereinafter: "Applicable Legislation").

2.3 The Processor informs the Controller immediately if:

(i) an instruction by the Controller is in violation of the GDPR and/or Applicable Legislation;
(ii) the Processor is no longer able to comply with this Data Processing Agreement;
(iii) the Processor has a statutory obligation to process the Personal Data unless provision of that information is prohibited by law.

ARTICLE 3 RENDERING COOPERATION

3.1 At the Controller's request, the Processor shall cooperate immediately to comply with the Controller's obligations in relation to the processing of Personal Data based on the GDPR and Applicable Legislation. This cooperation, defined in more detail for several topics in this Data Processing Agreement, includes the following:

(i) to comply with requests by Data Subjects;
(ii) to implement Data Protection Impact Assessments (DPIAs) and prior consultation with the Supervisory Authorities;
(iii) to implement Data Transfer Impact Assessments (DTIAs);
(iv) to comply with requests by national or international governments.

3.2 If the Processor receives a request from a national or international government related to the processing of Personal Data, then:

(i) the Processor shall immediately contact the Controller, and
(ii) the Processor shall follow the Controller's instructions.

ARTICLE 4 SUB-PROCESSORS

4.1 The Controller grants the Processor general authorization to engage another processor as defined in Article 28(4) of the GDPR (hereinafter: **"Sub-processor"**). The Sub-processors engaged by the Processor are listed in Annex A. The Processor shall follow the procedure in Article 11.3 for the intended modifications by Sub-processors.

4.2 The Processor shall remain fully liable to the Controller for the Sub-processors' compliance with obligations.

4.3 The Processor contractually imposes the obligations of this Data Processing Agreement on the Sub-processors. The Processor shall, on request, provide the Controller with a copy of those obligations set out in a contract. The Processor is permitted to omit competition-sensitive information from the copy he provides to the Controller.

ARTICLE 5 CONFIDENTIALITY

5.1 The Processor is obligated to maintain the confidentiality of the Personal Data. Individuals working for the Processor have signed a confidentiality agreement or are otherwise bound by a duty of confidentiality. The Controller may request proof of this.

5.2 Confidentiality may be breached if this is necessary for the performance of the Agreement or this Data Processing Agreement, pursuant to Applicable Law, a ruling by a Dutch court or a court in another EU member state. In the event of a court ruling from a third country, the Processor shall first consult with the Controller before providing any Personal Data.

ARTICLE 6 SECURITY

6.1 The Processor takes appropriate technical and organizational measures as defined in Article 32 of the GDPR to protect the Personal Data. The measures implemented by the Processor are included in Annex B.

6.1.1 The Processor evaluates and updates the security measures periodically to ensure these remain compliant with the latest technology and provide an appropriate protection level. The Processor guarantees that the modifications to the security measures will not result in a lower protection level than agreed at the commencement of the Data Processing Agreement or as subsequently agreed in writing. The Processor is entitled to unilaterally amend Annex B unilaterally to the most recent security standards. The Processor informs the Controller in writing about any modifications to Annex B.

6.2 The Processor documents its security policy in writing and, upon request by the Controller, provides evidence of the implemented measures. The Controller shall treat this information as confidential except where disclosure is required by a court order or at the request of a Supervisory Authority.

ARTICLE 7 PERSONAL DATA BREACH

7.1 If the Processor experiences a personal data breach (hereinafter: "Breach") or has a reasonable suspicion thereof, the Processor shall inform the Controller Option: immediately \ within 24 hours \ within 48 hours of the Breach. The Processor shall, when providing information, at a minimum, provide the information set out in Annex C to the contact person mentioned in that annex. If it is not possible for the Processor to provide all this information immediately, the Processor shall supply this information to the Controller in stages.

7.2 The Processor shall not notify the Supervisory Authority and/or the affected Data Subjects of any Data Breaches, unless explicitly requested in writing by the Controller.

7.3 The Processor shall take measures as soon as possible to address the causes of the Breach and to mitigate or remedy any potential adverse consequences of the Breach to the greatest extent possible.

7.4 The Parties keep the contact details in Annex C up to date and shall always immediately send any updated version to the other Party.

OPTIONAL - THIS BLOCK CONTAINS FURTHER DETAILS ON BREACHES

7.5 The Processor has policy and procedures in place to: (i) detect Breaches as early as possible, (ii) inform the Controller pursuant to Article 7.1, (iii) respond promptly to a Breach, (iv) prevent and mitigate unauthorized access, alteration or dissemination of the Personal Data and (v) prevent a recurrence of the Breach.

7.6 The Processor shall provide information about this policy and these procedures upon request by the Controller.

7.7 The Processor shall maintain a register of all Breaches related to the Processing of the Personal Data, containing details of the Breach, its consequences, and the (corrective) measures taken. The Processor shall provide a copy of this register upon request.

ARTICLE 8 AUDIT

8.1 The Processor submits to the Controller all information necessary to demonstrate compliance with the obligations set out in this Data Processing Agreement. The Processor shall annually prepare an audit report demonstrating compliance with the obligations of this Data Processing Agreement and shall provide this report upon request. The report shall be prepared by an independent and qualified third party and shall include a statement confirming that the findings accurately reflect the reality. If specific circumstances, in the opinion of the Controller, warrant it, or if the Controller suspects that the Processor is failing to fulfil its obligations, the Controller may conduct or commission its own audit. The Processor shall cooperate with such an audit, amongst others by granting access to systems and documents. The costs of such an audit shall be borne by the Controller unless the audit reveals that the Processor has failed to meet its obligations under this Data Processing Agreement.

8.3 The Controller announces the audit at least fourteen (14) days in advance. The audit shall not unreasonably disrupt the Processor's normal business activities.

8.4 The Controller handles all information from the audit in confidence and only shares it with those partners for who that knowledge is reasonably required. Neither the Controller nor the partners referred to above shall disclose or share the outcome of the audit with third parties unless compelled by law.

8.5 If the audit shows that the Processor failed to comply with the obligations of this Data Processing Agreement, the Processor shall immediately take all reasonable measures at his own cost to ensure compliance with these obligations.

ARTICLE 9 CROSS BORDER TRANSFER OF PERSONAL DATA

9.1 The Processor may only transfer Personal Data to a country outside the European Economic Area or to an international organization if: (i) the requirements of Articles 44 through 49 of the GDPR have been met, and (ii) the Controller has been informed in writing in a timely manner before the transfer begins. The transfers that occur are documented in Annex A. For any intended change to the transfers listed in Annex A, the Processor shall follow the procedure outlined in Article 11.3.

9.2 If a transfer occurs based on an adequacy decision by the European Commission, standard contractual clauses, or binding corporate rules, the Parties shall refer to the specific relevant documents in Annex A or attach them as an appendix to this Data Processing Agreement.

9.3 If there is a change or addition to the requirements regarding cross border data transfers, for example due to court rulings, new or amended adequacy decisions or standard contractual clauses issued by the European Commission, or recommendations from Supervisory Authorities, the Processor shall take measures to comply with these revised or supplemented requirements.

ARTICLE 10 INDEMNITY AND LIABILITY

ONE OF THE FOLLOWING 3 OPTIONS MUST BE SELECTED

OPTION 1: If the Agreement contains a comprehensive provision on indemnity, liability and compensation (including damages resulting from breaches of data protection and information security obligations)

10.1 The provisions on indemnity, liability and compensation in the Agreement shall apply in full to this Data Processing Agreement.

OPTION 2: If the Agreement does not contain, or does not provide, a comprehensive provision on indemnity, liability and compensation

10.1 The Processor shall indemnify the Controller against all claims, fines, losses, damages, and expenses arising from, or related to, the Processor's breach of this Data Processing Agreement. This indemnity shall take precedence over the provisions on indemnity, liability and compensation set forth in the Agreement.

OPTION 3: If the Agreement does not contain, or does not provide, a comprehensive provision on indemnity, liability and compensation

10.1 The Processor shall be liable for all damages suffered by the Controller (excluding lost profits), including fines imposed on the Controller by the Supervisory Authorities resulting from the Processor's breach of this Data Processing Agreement. This liability provision takes precedence over the provisions on indemnity, liability and compensation set forth in the Agreement.

For options 2 and 3, the following provision may optionally be included.

10.2 The Processor shall maintain a valid liability insurance policy for the liability as referred to in Article 10.1 with a coverage amount of EUR 1,000,000 (one million euros) per incident and EUR 2,000,000 (two million euros) per year. Upon request from the Controller, the Processor shall provide a copy of (the certificate of) the insurance policy and its terms and conditions.

ARTICLE 11 AMENDMENT

11.1 The Parties may amend or supplement this Data Processing Agreement only by means of a written agreement signed by both Parties, except for the modifications to the annexes described in this Data Processing Agreement.

11.2 Amendments or additions to this Data Processing Agreement shall not contravene Applicable Law.

11.3 In the event of proposed changes to Sub-processors and data transfers outside the EEA, the Processor shall observe the following:

a. The Processor shall inform the Controller in writing at the earliest opportunity about the intended modifications.

b. The Processor shall update Annex A with the proposed changes.

c. Upon receipt of the change request and the updated Annex A, the Controller shall have one (1) month to submit a written, substantiated objection.

d. In the event of an objection, the Parties shall enter into consultations. The proposed changes shall not take effect until the Parties have reached an agreement.

e. If no solution is found within two (2) months following the objection, the Controller may terminate the Agreement with one (1) months' notice, without being obligated to compensate costs or damages.

f. If the Controller does not object within the specified period mentioned under clause 3, the proposed changes shall be deemed accepted after the expiration of this objection period.

OPTIONAL - THIS BLOCK CONTAINS A PROVISION ON CHANGE OF CONTROL

11.3 In the event of a change in the control over the Processor, for example through a merger, acquisition or change in the ownership structure, the Processor shall inform the Controller of this as soon as possible. In such a case, the Controller shall have the right to terminate the Agreement in writing, subject to a notice of at least three (3) months.

ARTICLE 12 EFFECTIVE DATE, DURATION AND TERMINATION

12.1 This Data Processing Agreement shall come into force upon signature by the Parties. If the Processing of Personal Data commenced prior to the signing this Data Processing Agreement, this Data Processing Agreement shall apply retroactively as of the date on which the Processing began.

12.2 This Data Processing Agreement cannot be terminated independently of the Agreement.

12.3 Within one (1) month after the termination of the Agreement, regardless of the reason for such termination, the Processor shall destroy or return all Personal Data (including any copies held by Sub-processors). If the Controller opts for the return of the data, the Processor shall transfer the data in a commonly used format to the Controller or to another party designated by the Controller. If Annex A

specifies a different retention period for specific Processing activities of Personal Data, that period shall prevail over the period in mentioned this article.

12.4 The Processor's obligations under this Data Processing Agreement shall remain in effect until such time as the Processor no longer processes any Personal Data.

12.5 The Processor shall confirm in writing to the Controller that it has complied with all obligations in Article 12.3 upon request.

ARTICLE 13 APPLICABLE LAW, DISPUTE RESOLUTION AND HIERARCHY

13.1 This Data Processing Agreement is subject to the same law as the Agreement.

13.2 Disputes arising from this Data Processing Agreement shall be submitted to the competent court as specified in the Agreement.

13.3 The original text of this Data Processing Agreement is written in Dutch. In the event of differences in interpretation, the Dutch version shall prevail.

13.4 In the event of any conflict between this Data Processing Agreement and the Agreement concerning the Processing of Personal Data, the provisions of this Data Processing Agreement shall prevail.

THUS, AGREED BY THE PARTIES:

Fill out all yellow highlights before signing this agreement and delete this bar.

[NAME CONTROLLER]	**[NAME PROCESSOR]**
_____/_____/_____	_____/_____/_____
Date	*Date*
_____	_____
Name	*Name*
_____	_____
Signature	*Signature*

Annex A: Specification of Personal Data Processing Activities

Description of processing ('What are you going to do?')	Purpose of the processing activities ('Why are you going to do this?')	Data Subjects	Personal Data	Retention periods of Personal Data
1 ….				
2 ….				
3 ….				

The Sub-processors engaged by the Processor are:

Sub-processor (name including domicile)	The Personal Data processed by this Sub-processor	Specification of reason for sub-processing	Country of processing and relevant transfer mechanism

The transfers to third countries for these Processing activities are:

Transfer to third countries (name of party + which third country)	Purpose of transfer (cost savings, economies of scale or security improvements)	Transfer instrument	Additional measures for transfer to a third country (if applicable)

Contact details

General contact details	Name	Job title	Email address	Telephone number
Controller				
Processor				

Date appendix: [DATE]

Annex B: Security measures

ONE OF THE FOLLOWING TWO OPTIONS MUST BE SELECTED

OPTION 1: If the Processor has adequate certificates

The Processor holds the following valid certificates or statements from an independent third party demonstrating that the Processor complies with its obligation to adequately secure the Personal Data it processes on behalf of the Controller:

Name or number	Scope of application	Period of validity
For example, ISO 27001, NEN 7510, SOC 2		

The Processor shall ensure that throughout the term of this Data Processing Agreement it continues to hold the aforementioned certificates or an equivalent successor thereof with a renewed validity period.

OPTION 2: If the Processor does not have adequate certificates

In the table below, the Processor lists the security measures implemented by the Processor to adequately protect the Personal Data that it processes on behalf of the Controller.

Where the Processor has not fully implemented a specific measure, this is indicated in the column 'Explanatory notes'.

#	Subject	Measure	Explanatory notes
1	Information security and privacy policy	The Processor has an information security and privacy policy in place that complies with the GDPR and any other guidelines of the Dutch Data Protection Authority and that aligns with general standards such as ISO 27001/2/18, NOREA of CoBIT. The Processor has communicated this policy internally and implemented it through documented procedures.	The Processor may also refer in this table to the specific location in a document showing that and how a measure was implemented (such as a section or paragraph in an internal policy document).
2	Encrypted storage and transfer of data	The Processor applies up-to-date and generally accepted secure encryption methods to data for storage ('at rest') and transfer ('in transit') to minimize the risk of unauthorized individuals accessing the contents of the data.	

#	Subject	Measure	Explanatory notes
3	Access management	The Processor applies the principles of 'least privilege' and 'need-to-know' to its employees and authorized Sub-processors. The Processor shall promptly revoke or modify user access in case of any change to the status of its or the Sub-processors' employees. The Processor uses up-to-date and widely recognized secure encryption methods for identification, authentication and authorization.	
4	Staff	The Processor informs its staff about their responsibilities regarding information security and ensures that its employees comply with their obligations.	
5	Contract management Sub-processors	The Processor shall enter into a written agreement with each authorized Sub-processor, contractually obliging the Sub-processor to comply with the same obligations regarding the Processing as those to which the Processor is bound under this Data Processing Agreement. The Processor shall closely monitor the Sub-processors' compliance with their obligations.	
6	Security incident detection & response	The Processor has documented policies that are adequate to detecting, resolving and reporting Breaches.	
7	Vulnerability / patch management	The Processor regularly or continuously searches for vulnerabilities within the used and provided applications, systems and networks. The Processor installs and implements security patches immediately or as soon as possible after their release.	
8	Network and system security	The Processor has implemented measures to prevent and detect misuse of, and malware on the Processor's network and systems (such as firewalls and antivirus software from reliable vendors).	
9	Physical access control	The Processor takes appropriate measures (such as locks, cameras, and alarm systems) to secure the premises where data may be processed against unauthorized access.	
10	Logging and monitoring	Logging and monitoring are used to demonstrate that only legitimate users and/or applications access the data. In the	

#	Subject	Measure	Explanatory notes
		event that non-legitimate users and/or applications are detected, appropriate action shall be taken.	
11	Demonstrating location	The Processor is able to demonstrate the physical location/geography of the stored data.	
12	Business continuity & disaster recovery	The Processor has implemented policies, procedures and processes to ensure that the services or products provided, and the data processed remain available in the event of unforeseen circumstances and disasters, or they are fully restored as quickly as possible.	
13	Secure application development	The Processor uses industry standards (e.g. OWASP, BSIMM, ACS, NIST) to integrate security into application development.	
14	Independent control	The Processor permits an external party to conduct audits, vulnerability scans and periodic penetration tests on its applications and networks, on behalf of the Controller and in consultation with the Processor. Preferably, the Processor itself regularly engages qualified external parties to perform audits, vulnerability scans and periodic penetration tests on its applications and networks. Ideally, the Processor also has policies and procedures in place for identifying and reporting security vulnerabilities by independent security researchers (such as a responsible disclosure policy and/or a bug bounty program). Rewarding parties who responsibly report significant security vulnerabilities is considered a positive practice.	

As far as the above table refers to the Processor's documents, the Processor shall always make the most recent document available to the Controller.

Last modified: [DATE]

Annex C: Reporting a breach

To report a Breach, contact:

Contact details in the case of a Breach	**Name**	**Job title**	**Email: address**
Controller			
Processor			

The Processor shall, when reporting a Breach, at least provide the information as described in the most recent version of the 'Data Breach Notification Desk' of the Dutch Data Protection Authority, available at: datalekken.autoriteitpersoonsgegevens.nl/, detailed in the 'Questionnaire data breach form': autoriteitpersoonsgegevens.nl/documenten/vragenlijst-meldformulier-datalekken.

Last modified: [DATE]