

(annotated versions w/ comments + variants available on request)

[Unilateral Datasharing Agreement](#)

[Mutual Datasharing Agreement](#)

[Joint Controller Agreement](#)

[Data Processing Agreement - as Processor](#)

[Data Processing Agreement - as Data Controller](#)

Unilateral Datasharing Agreement

Vrije Universiteit Brussel, established at 1050 Brussels, Pleinlaan 2, BE 449.012.406, represented by prof. dr. Jan Danckaert, rector, who entrusts the execution of this Agreement to [.....],

hereinafter referred to as "**Exporter**"

AND

[.....], established at ... , BE [.....], represented by [.....], acting in his/her capacity as [.....],

hereinafter referred to as "**Importer**"

The above entities are individually referred to as "the Party" and collectively as "the Parties".

CONSIDERING

- [The Parties have concluded an agreement *[e.g. a cooperation agreement]* on [.....], concerning [.....] *[name and project reference]*, hereinafter "the Principal Agreement"]
- Exporter will transfer personal data (hereinafter "the Personal Data") to Importer within the framework of the Principal Agreement (hereinafter "the Sharing"). Importer will process the Personal Data for his own account and under his own responsibility (hereinafter "the Processing").
- In the present Agreement, the Parties make arrangements regarding the Sharing and the Processing, taking into account the applicable legislation, in particular the [General Data Protection Regulation \(EU\) 2016/679 of 27 April 2016](#) (hereinafter "the GDPR") and the [Belgian law on the protection of personal data of 30 July 2018](#) (hereinafter jointly "the Privacy Legislation").
- All terms used in this Agreement that are defined in the Privacy Legislation, are to be understood in that sense.

HAVE AGREED

Article 1. Nature of the Personal Data *(possibly: and modalities of the Processing)*

The Personal Data listed in the schedule hereafter / in annex 1 will be shared:

Persons	Data

[optional: the Processing is submitted to the following conditions and/or limitations:]

[or: The modalities of the Processing are listed in annex 1.]

Article 2. Guarantees

2.1. Exporter guarantees that:

- the Personal Data are collected legitimately
- the Personal Data are correct
- the Sharing is lawful, on the basis of:
 - *express consent of the data subjects*
 - *legal obligation*
 - *entering into or executing an agreement*
 - *vital interest of the data subject*
 - *general interest, namely:*
 - *necessary for the purposes of the legitimate interests of the Parties, namely:*

[possibly: Concerning the following sensitive data:, the Parties rely on:

- *express consent of the data subjects*
- *vital interest of the data subjects*
- *personal data have already been disclosed by the data subjects*
- *substantial public interest, namely:*
- *archiving in the public interest, for scientific or historical research or for statistical purposes*
- *...*
- he will only share Personal Data to the extent that this is necessary for the execution of the Principal Agreement [possibly: and to the Personal Data listed in annex 1]

2.1. Importer guarantees that:

- the Processing is lawful, on the basis of:
 - *express consent of the data subjects*
 - *legal obligation*
 - *entering into or executing an agreement*
 - *vital interest of the data subject*
 - *general interest, namely:*
 - *necessary for the purposes of the legitimate interests of the Parties, namely:*

[possibly: Concerning the following sensitive data:, the Parties rely on:

- *express consent of the data subjects*

- *vital interest of the data subjects*
- *personal data have already been disclosed by the data subjects*
- *substantial public interest, namely:*
- *archiving in the public interest, for scientific or historical research or for statistical purposes*
- *...]*
- *[possibly: he will request the consent of the data subjects for the Processing*
- he will only process the Personal Data to the extent that this is necessary for the execution of the Principal Agreement *[possibly: and to the acts listed in annex 1]*
- *[possibly: he will respect the conditions and limitations of the Processing, as listed in article 1]*
- he will take the necessary technical and organisational measures to protect the Personal Data, including:
 - measures to ensure that the data are only accessible to authorised personnel
 - measures to protect the data against accidental or unlawful destruction, loss or alteration and against unauthorised storage, processing or disclosure
 - *[possibly: pseudonymisation and encryption, ...,]*

[possibly: These measures are listed in annex 2.]

- *[possibly: he will not disclose the Personal Data to third parties without the consent of Exporter and, if need be, he will apply procedures so that third parties observe and maintain the confidentiality and security of the Personal Data.]*

This provision does not apply to persons who are given access to the Personal Data on the basis of legal or regulatory provisions.]

- *[possibly: he will inform Exporter as soon as possible of infringements, such as loss of Personal Data and unauthorised access, provide Exporter with all the necessary information and documents to assess the situation, and will immediately, at his own expense, take all measures to correct the shortcomings in security that resulted in the Incident and to limit its consequences*
- *[possibly: he will not keep the Personal Data longer than necessary for the execution of the Principal Agreement.]*

2.3. Both Parties guarantee that:

- they will comply with their obligation of transparency, and they dispose of a privacy statement, which can be consulted here:
 - Exporter: [Privacy Statement | Vrije Universiteit Brussel](#)
 - Importer: *.....*
- they will inform the other Party as soon as possible of questions and requests of the authorities or data subjects (e.g. erasure of data or restriction of processing), which (also) concern the other Party
- they will provide the other Party, on request, with the necessary cooperation in dealing with questions and requests from authorities or data subjects

Article 3. Liability and indemnification

The Parties shall indemnify each other against the consequences of infringements of this Agreement and of the Privacy Legislation, including damages *[and lawyers' fees]*.

The Parties shall however in no case be liable for any indirect, incidental or consequential damages (including without limitation, lost business or profits, loss of data or loss of use of equipment) suffered by the other Party.

Article 4. Duration and termination

This Agreement shall commence on the date of signature by both Parties and shall remain in force until

[Or: This Agreement shall commence on the date of signature by both Parties, and shall remain in force until the termination of the Principal Agreement.]

Clauses which by their nature are intended to continue after the end of the contract, shall remain in force. These include clauses relating to:

- liability and indemnification
- settlement of disputes and applicable law.

Both parties may terminate this Agreement with immediate effect by registered letter, if the other party fails to fulfil its obligations and has not remedied this within 30 days of being served with a notice of default.

Article 5. Contacts

The contact persons of the Parties are:

- for Exporter:
- for Importer:

(names, positions, email addresses and telephone numbers)

Article 6. Return of the Personal Data

Within ten days after the expiry of the current Agreement, Importer shall hand over all Personal Data and all copies thereof to Exporter, or, at Exporter's option, destroy them and confirm the destruction in writing.

This does not apply to data that need to be retained in application of the Privacy Legislation, or in application of regulations concerning the safeguarding of scientific integrity.

Article 7. Disputes and applicable law

This Agreement is governed by Belgian law.

All disputes relating to this Agreement will be submitted to the court that has jurisdiction under the Principal Agreement [or: to the competent Dutch-language court in the district of Brussels].

Agreed and signed at _____ on _____

On behalf of the Exporter

.....

On behalf of Importer

.....

prof. dr. Jan Danckaert
rector

.....
.....

(possibly) Annex 1 - Modalities of Processing

Description of the Personal Data	Purpose of Secondary Processing	Proportionality	Frequency and other modalities of Transfer
e.g. names and national registration numbers	create accounts that give access to an online learning environment		one-off, monthly, ...

(possibly) Annex 2 - Technical and organisational measures

Mutual Datasharing Agreement

Vrije Universiteit Brussel, established at 1050 Brussels, Pleinlaan 2, BE 449.012.406, represented by prof. dr. Jan Danckaert, rector, who entrusts the execution of this Agreement to [.....],

hereinafter referred to as "**VUB**"

AND

....., established at ... , BE , represented by , acting in his/her capacity as,

hereinafter referred to as "**X**"

The above entities are individually referred to as "the Party" and collectively as "the Parties".

CONSIDERING

- [The Parties have concluded an agreement *[e.g. a cooperation agreement]* on , concerning
[name and project reference], hereinafter "the Principal Agreement"]
- The Parties will exchange personal data (hereinafter "the Personal Data") within the framework of the Principal Agreement (hereinafter "the Sharing") and process the Personal Data for their own account (hereinafter "the Processing").
 - In the present Agreement, the Parties make arrangements regarding the Sharing and the Processing, taking into account the applicable legislation, in particular the [General Data Protection Regulation \(EU\) 2016/679 of 27 April 2016](#) (hereinafter "the GDPR") and the [Belgian law on the protection of personal data of 30 July 2018](#) (hereinafter jointly "the Privacy Legislation").
- All terms used in this Agreement that are defined in the Privacy Legislation, are to be understood in that sense.

HAVE AGREED

Article 1. Nature of the Personal Data and purpose of the Processing

[X/VUB] wishes to make use of data, including Personal Data, with which [VUB/X] carries out an initial processing and is initially responsible.

[The Parties shall limit the Sharing and the Processing to what is necessary for the execution of the Principal Agreement.]

[or: The nature of the Personal Data that Parties may transfer to each other and the purpose of the Processing are set out in the table in Annex 1.]

Article 2. Obligations of the Parties

Each Party shall comply with the Privacy Legislation in the Sharing and Processing, and guarantees in particular:

a) that it has a privacy statement, which can be consulted here:

- VUB: [Privacy Statement VUB | Vrije Universiteit Brussel](#)
- X:

b) that the Sharing and the Processing are lawful, on the basis of:

- *consent of the data subjects*
- *legal obligation*
- *entering into or executing an agreement*
- *vital interest of the data subject*
- *general interest, namely:*
- *necessary for the purposes of the legitimate interests of the Parties, namely:*

[possibly: concerning the following sensitive data:, the Parties rely on:

- *express consent of the data subjects*
- *vital interest of the data subjects*
- *personal data have already been disclosed by the data subjects*
- *substantial public interest, namely:*
- *archiving in the public interest, for scientific or historical research or for statistical purposes*
- *...]*

c) in the case of processing based on the consent of the data subjects

- a. to comply with its obligation of transparency and, in particular, to inform the data subjects about the Sharing
- b. to inform the other Party of the conditions of the consent, if any, such as the duration and the purposes of the Processing, pseudonymisation, ...
- c. to take into account any conditions attached to the authorisation.

d) that the shared Personal Data are correct

e) to treat the Personal Data as strictly confidential

f) to limit the Processing to a minimum, in particular not share more Personal Data than necessary and not to perform unnecessary processing acts

g) not to disclose the Personal Data to third parties without the consent of the other Party and, if need be, to apply procedures so that third parties observe and maintain the confidentiality and security of the Personal Data.

This provision does not apply to persons who are given access to the Personal Data on the basis of legal or regulatory provisions.

h) to take the necessary technical and organisational measures to protect the Personal Data, including:

- measures to ensure that the data are only accessible to authorised personnel
- measures to protect the data against accidental or unlawful destruction, loss or alteration and against unauthorised storage, processing or disclosure
- [possibly: pseudonymisation and encryption, ..,]

[possibly: These measures are listed in Annex 2.]

- i) [possibly: to keep the Personal Data no longer than necessary for the execution of the Principal Agreement.]
- j) to provide the other Party with the necessary cooperation in dealing with requests from authorities or from data subjects (e.g. erasure of data or restriction of processing)
- k) to inform the other Party as soon as possible of infringements, such as loss of Personal Data and unauthorised access, to provide the other Party with all the necessary information and documents to assess the situation, and to cooperate in the handling of the infringements
- l) to inform the other Party of any request by the data subject for the exercise of his/her rights.

Article 3. Liability and indemnification

Each party is solely responsible for its own processing of the Personal Data.

The Parties shall indemnify each other against the consequences of infringements of this Agreement and of the Privacy Legislation, including damages [and lawyers' fees].

Article 4. Duration and termination

This Agreement shall commence on the date of signature by both Parties and shall remain in force until

[Or: This Agreement shall commence on the date of signature by both Parties, and shall remain in force until the termination of the Principal Agreement.]

Clauses which by their nature are intended to continue after the end of the contract, shall remain in force. These include clauses relating to:

- liability and indemnification
- settlement of disputes and applicable law.

Both parties may terminate this Agreement with immediate effect by registered letter, if the other party fails to fulfil its obligations and has not remedied this within 30 days of being served with a notice of default.

Article 5. Contacts

The contact persons of the Parties are:

- for the VUB:
- for X:

(names, positions, email addresses and telephone numbers)

Article 6. Disputes and applicable law

This Agreement is governed by Belgian law.

All disputes relating to this Agreement will be submitted to the court that has jurisdiction under the Principal Agreement [or: to the competent Dutch-language court in the district of Brussels].

Agreed and signed at _____ on _____

On behalf of the VUB

.....

On behalf of X

.....

prof. dr. Jan Danckaert
rector

.....
.....

(possibly) Annex 1 - Modalities of Processing

Description of the Personal Data	Purpose of Secondary Processing	Proportionality	Frequency and other modalities of Transfer
e.g. names and national registration numbers	create accounts that give access to an online learning environment		one-off, monthly, ...

(possibly) Annex 2 - Technical and organisational measures

Joint Controller Agreement

PARTIES

Vrije Universiteit Brussel, established at 1050 Brussels, Pleinlaan 2, BE 449.012.406, represented by prof. dr. Jan Danckaert, rector, who entrusts the execution of this agreement to [.....], hereinafter "VUB"

AND

....., established at, VAT or company registration number, represented by, acting in her/his capacity as,
Hereinafter "X"

Individually hereinafter referred to as "Party" and together as "Parties"

CONSIDERING

- The Parties have entered into an agreement [e.g. a cooperation agreement] on, regarding [name and project reference, if any], hereinafter "the Principal Agreement".
- The Parties will share and process personal data (hereinafter "Personal Data") within the framework of the Principal Agreement (hereinafter "Processing") and jointly determine the purposes and means of the Processing. They are therefore joint controllers.
- The Parties agree in the present contract on the Processing and their respective responsibilities in this regard, taking into account the applicable law, including the [General Data Protection Regulation \(EU\) 2016/679 of 27 April 2016](#) (hereinafter "the GDPR"), in particular article 26, and the [Belgian law on the protection of personal data of 30 July 2018](#) (hereinafter jointly referred to as "the Privacy Legislation").
- All terms used in this agreement that are defined in the Privacy Legislation are to be understood in that sense.

HAVE AGREED

Article 1: Object of the agreement

1.1. Description of the Personal Data:

- data subjects:
- data:

1.2. Legal grounds for the Processing:

.....

1.3. Purposes of the Processing:

.....

1.4. Storage period of the Personal Data or criteria determining the period:

.....

Article 2: Task distribution

2.1. Storage

VUB / X is responsible for the storage of the Personal Data.

[Or: Each Party is responsible for its storage of the Personal Data.]

The Personal Data are stored in a secure database, the storage systems provide sufficient guarantees against data loss and there are adequate backup and recovery facilities.

2.2. Technical and organisational measures

VUB / X / Each Party shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, take the necessary technical and organisational measures to protect the Personal Data, including, where appropriate, the measures listed in Article 32.1 GDPR, such as pseudonymisation and encryption.

[optional: These measures are listed in Annex 1.]

2.3. Transparency

VUB / X / Each Party shall ensure that the data subjects are informed of the Processing, in accordance with Article 13 and/or Article 14 of the GDPR.

2.4. Rights of data subjects

VUB / X is responsible for dealing with requests from data subjects / Each party is responsible for dealing with requests from data subjects that it receives, in accordance with Articles 15 to 22 of the GDPR (erasure of data, restriction of processing, etc.).

2.5. Questions from authorities

VUB / X is responsible for dealing with questions from authorities / Each party is responsible for dealing with questions from authorities that it receives.

2.6. Audits

VUB / X guarantees / Both Parties guarantee the handling of audits by third parties.

2.7. Register

Each Party is responsible for keeping a register of processing activities, in accordance with Article 30 of the GDPR.

2.8. Agreements with processors

VUB / X / Both Parties shall be responsible for negotiating and drawing up any data processing agreements. These agreements shall be signed by both parties.

2.9. Infringements

Each Party shall draw up a plan for dealing with infringements (loss of data, unauthorised access, etc.), take action in response to infringements, and keep a detailed log of all infringements and of the measures taken.

In the event that one party discovers a data breach, it shall notify the other party without delay.

The duty to report to the supervisory authority rests with the party that discovered and dealt with the data breach. If the causes of the data breach lie within the responsibilities of another party, that other party shall take over the handling of the data breach, without exceeding the statutory reporting deadlines.

Any costs incurred in resolving the infringement shall be borne by the Party that is responsible for the infringement.

2.10. Data protection impact assessment (DPIA)

VUB / X / Both Parties shall ensure that a data protection impact assessment is carried out, if the Processing represents a high risk to the rights and freedoms of the data subjects, in accordance with Article 35 of the GDPR.

2.11. Destruction of the Personal Data

Each party shall be responsible for the destruction of the Personal Data upon expiry of this agreement and/or the expiry of the storage periods.

The parties shall account to each other for such destruction afterwards.

2.12. Information, assistance and consultation

Both parties undertake to inform each other as soon as possible of any questions raised by interested parties and authorities and of any possible infringements, to provide each other with the necessary

assistance so that they can carry out their tasks properly, and to consult with each other where appropriate. Each party shall provide the other, upon request, with information on the performance of its tasks, and copies of related documents.

Article 3: Obligations of the Parties

Each party guarantees:

- 3.1. that it collects the Personal Data lawfully and that the legal basis for the Processing is legitimate
- 3.2. that it will only process the Personal Data as described in Article 1, to the extent necessary to perform the Principal Agreement, and in accordance with the Privacy Legislation
- 3.3. that it will limit the Processing to a minimum, in particular not collect more Personal Data than necessary, not perform unnecessary processing acts and anonymize or pseudonymize the Personal Data as soon as possible
- 3.4. that the possible transfer of Personal Data to the other Party will offer adequate protection, taking into account the nature and sensibility of the Personal Data, and the risks involved for the data subjects
- 3.5. that it will limit as much as possible the access to the Personal Data by employees, and that it has implemented procedures so that any employee who has access to the Personal Data will observe their confidentiality and security, and will comply with the present agreement.

This provision does not apply to persons authorised by law to have access to the Personal Data

- 3.6. that it will not transfer the data to third parties without the consent of the other party. In case of transfer to countries outside the EU or to other countries than those recognised by the European Commission to have an equivalent level of protection¹, the guarantees imposed by the [Standard contractual clauses](#) of the EU will apply.
- 3.7. that it will properly fulfil the tasks assigned to it in Article 2.

Article 4. Audit

Each party may verify the compliance of the other party with this agreement. The party concerned shall cooperate fully with the other party or its appointed auditor, and shall provide all useful information and documents. The audit will be announced at least seven working days in advance.

If an inspection reveals that the other party is not fulfilling its obligations, it shall bear the costs of the inspection.

Article 5: Duration

This Agreement shall commence on the date of signature by both Parties and shall remain in force until

[Or: This Agreement shall commence on the date of signature by both Parties, and shall remain in force until the termination of the Principal Agreement.]

¹ see [Adequacy decisions | European Commission \(europa.eu\)](#)

[Or: This Agreement shall commence on the date of signature by both Parties, and shall remain in force until the termination of the storage period indicated in article 1.4.]

Clauses which by their nature are intended to continue after the end of the contract, shall remain in force. These include clauses relating to:

- liability and indemnification
- settlement of disputes and applicable law.

Article 6. Indemnification

Each party indemnifies the other party against all consequences of its infringements of this agreement and of the Privacy Legislation, including fines, damages [and lawyers' fees].

Article 7. Contacts

The contact persons for the implementation of this agreement are:

- for VUB:
- for X:

(names, email addresses and telephone numbers)

Article 8. Termination

Both parties may terminate this agreement with immediate effect by registered letter, if the other party fails to fulfil its obligations, and has not remedied this within 30 days of being served with a notice of default.

[And/or: If the Principal Agreement ends for any reason, this agreement shall also end automatically.]

Article 9: Applicable law and competent court

This agreement is governed by the law that governs the Principal Agreement [or: by Belgian law].

All disputes relating to this agreement will be submitted to the court that has jurisdiction under the Principal Agreement [or: to the competent Dutch-language court in the district of Brussels].

Agreed and signed at _____ on _____

VUB
prof. dr. Jan Danckaert
rector

X

.....
.....

optional: **Annex 1 - Technical and Organisational
Measures**

Data Processing Agreement - as Processor

PARTIES

....., established at ... VAT or company registration number, represented by, acting in his/her capacity as,

hereinafter referred to as "the Controller"

AND

Vrije Universiteit Brussel, established at 1050 Brussels, Pleinlaan 2, BE 449.012.406, represented by prof. dr. Jan Danckaert, rector, who entrusts the execution of this Agreement to [.....],

hereinafter referred to as "the Processor"

CONSIDERING

- The parties have concluded an agreement [e.g. a cooperation agreement] on, concerning [name and reference of the project], hereinafter referred to as "the Principal Agreement".
- The Processor will process personal data (hereinafter "the Personal Data") under the Principal Agreement in the name of, on behalf of, and as instructed by the Controller (hereinafter "the Processing").
- In the present Agreement, the Parties make arrangements regarding the Processing, taking into account the applicable legislation, in particular the [General Data Protection Regulation \(EU\) 2016/679 of 27 April 2016](#) (hereinafter "the GDPR") and the [Belgian law on the protection of personal data of 30 July 2018](#) (hereinafter jointly "the Privacy Legislation").
- All terms used in this Agreement that are defined in the Privacy Legislation are to be understood in that sense.

HAVE AGREED

Article 1. Responsibility of the Controller

The Controller guarantees that he/she collects the Personal Data in accordance with the Privacy Legislation.

He/she shall make available to the Processor only the Personal Data that the latter needs for the performance of the Principal Agreement, and to the extent permitted by the Privacy Legislation.

Article 2. Processing

2.1. The Processor shall only process the Personal Data to the extent necessary to execute the Principal Agreement.

2.2. The Personal Data and the instructions and modalities for processing are listed in Annex 1, which will be updated whenever necessary by mutual agreement between the Parties.

2.3. The Processor shall treat all data as strictly confidential and shall respect the Privacy Legislation.

2.4. If, in the opinion of the Processor, instructions of the Controller are contrary to the Privacy Legislation, he will immediately inform the Controller. To the extent that the instructions are indeed unlawful, the Processor may refuse to comply with them.

Article 3. Staff

3.1. The Processor shall only grant access to the Personal Data to staff members to the extent necessary for the performance of the Principal Agreement.

3.2. The Processor warrants that the persons referred to in point 3.1 are subject to a duty of confidentiality and will comply with the present Agreement.

Article 4. Protection

4.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall take the necessary technical and organisational measures to protect the Personal Data, including, where appropriate, the measures listed in Article 32.1 GDPR, such as pseudonymisation and encryption.

4.2. *[optional: In particular, the Processor undertakes to take the measures described in Annex 2.]*

Article 5. Third parties

[Either: The Processor shall not communicate any Personal Data and shall not outsource the Processing in whole or in part to third parties, without the prior written consent of the Controller.]

Or: The Controller gives the Processor a general authorisation to entrust the Processing in whole or in part to the sub-processors listed in Annex 3. The Processor shall notify the Controller of any change to this list in advance, and the Controller may object to the change within one month.

Or: The Controller gives the Processor a specific authorisation [optionally: precise] to entrust the Processing in whole or in part to the sub-processors listed in Annex 3. Any additional sub-processor requires the explicit consent of the Controller.]

The Processor confirms the existence of procedures so that any third party who is granted access to the Personal Data will respect the confidentiality and security thereof, and ensures that the third parties are bound by obligations no less than those set out in the present Agreement.

This provision does not apply to persons authorised by law to have access to the Personal Data.

Article 6: Transfer to other countries

The Processor may only transfer the Personal Data to countries outside the EU and outside the countries recognised by the European Commission as having an equivalent level of protection², after prior written consent of the Controller.

Article 7: Infringements

7.1. The Processor will inform the Controller as soon as possible of infringements in connection with the Personal Data (e.g. loss, illicit access), and provide the Controller with all information and documents necessary to assess the situation.

² see [Adequacy decisions | European Commission \(europa.eu\)](https://european-council.europa.eu/media/en/press-communications/inline-2021/01/10/Pages/adequacy-decisions.aspx)

7.2. It is the responsibility of the Controller to take action in the event of infringements. The Processor will provide the Controller with all necessary cooperation in this regard.

7.3. The Processor shall have a plan for dealing with infringements and shall provide the Controller with a copy of the plan or the latest version of the plan upon request.

7.4. The Processor shall keep a detailed log of all infringements and of the measures taken and shall provide the Controller with a copy thereof upon request.

Article 8. Requests from authorities and data subjects

8.1. If the Processor receives a request from a data subject in the exercise of one of its rights, the Processor shall forward the request to the Controller as soon as possible.

8.2. The Controller will deal with the requests, unless the parties agree that the Processor will deal with a particular request, or unless the Processor is required to do so by law.

8.3. The Processor shall store the Personal Data in a structured, commonly used and machine-readable form, in order to guarantee their portability.

Article 9. Assistance

The parties shall assist each other as necessary to fulfil their obligations under the Privacy Legislation, including for the execution of a possible data impact assessment.

Article 10. Audit

10.1. The Controller may verify compliance with this agreement or have it verified. The Processor shall provide the Controller or his/her appointed auditor with all cooperation and all useful information and documents. The Controller will give at least seven working days' notice of the audit.

10.2. If an audit reveals that the Processor is not complying with its obligations, the Processor shall bear all costs of the audit and of the corrective measures.

Article 11. Duration and termination

This Agreement shall commence on the date of signature by both parties and shall remain in force until

[Or: This Agreement shall commence on the date of signature by both parties, and shall remain in force until termination of the Principal Agreement.]

Clauses which by their nature are intended to continue after the end of the contract, shall remain in force. These include clauses relating to:

- liability and indemnification
- settlement of disputes and applicable law.

Both parties may terminate this Agreement with immediate effect by registered letter, if the other party fails to fulfil its obligations and has not remedied this within 30 days of being served with a notice of

default.

Article 12. Return of Personal Data

Within ten days after the expiry of the current Agreement, the Processor shall hand over all Personal Data and all copies thereof to the Controller, or, at the Controller's option, destroy them and confirm the destruction in writing.

This does not apply to data that need to be retained in application of the Privacy Legislation, or in application of regulations concerning the safeguarding of scientific integrity.

Article 13. Contacts

The contact persons for the implementation of this Agreement are:

- for the Processor:
- for the Controller:

(names, positions, email addresses and telephone numbers)

Article 14. Indemnification

The Processor shall indemnify the Controller against fines, administrative and corrective measures, damages **and lawyers' fees**, insofar as they result from a contractual default, a failure to comply with the Controller's lawful instructions, or an infringement of the Privacy Legislation on the part of the Processor.

Article 15. Disputes and applicable law

This Agreement is governed by Belgian law.

All disputes relating to this Agreement will be submitted to the court that has jurisdiction under the Principal Agreement [or: to the competent Dutch-language court in the district of Brussels].

Agreed and signed at _____ on _____

For the Controller

.....
.....
.....

For the Processor

.....
prof. dr. Jan Danckaert
rector

Annex 1 - Processing instructions

Data subjects	Personal Data	Processing	Purpose
e.g. patients, students, citizens of ...	e.g. Name, email address, age	Database storage and analysis	Survey on eating habits
	e.g. Age, geolocation	Movement tracking/monitoring	Mobility survey
	e.g. Mail traffic	Hosting	Hosting mailbox
	e.g. Name, answers/opinions on political landscape, image/voice	Interview recordings (and possible transcription)	Political research

The Personal Data will be processed and stored at [location].

Annex 2 - Technical and Organisational Measures

The Processor shall take at least the following measures:

I Privacy protection

The Processor acts in accordance with the GDPR and will never share the data with third parties, unless explicit permission has been granted by users.

In the event of an incident, both parties are obliged to make an effort to limit the damage as much as possible, for example by rapid direct communication and good coordination of all analysis and reports.

II Organisation

The Processor has appointed a DPO, namely Andries Hofkens.

The Processor shall only grant access to Personal Data to its staff to the extent necessary for compliance with and performance of this Agreement, and to the extent that such staff need access for the performance of their own duties, in function of compliance with this Agreement.

The Processor has ensured contractually binding confidentiality obligations towards its own staff.

The Processor has adopted internal procedures for the correct and timely fulfilment of its legal and contractual obligations, among others:

- for the reporting of data breaches,
- for the application of the principle of "data protection by design and by default", as set out in Article 25 of the GDPR,
- for responding to requests from data subjects,
- for carrying out data protection impact assessments,
- for the use by staff and external service providers of the IT infrastructure and other devices provided.

The Processor shall perform quarterly checks on the status of the security measures applied.

The Processor shall perform penetration tests at least once a year and shall communicate the results, including vulnerabilities by type (high, medium, low), to the Controller.

III Storage

All data is stored in a secure database.

The storage systems used offer sufficient guarantees against data loss.

IV Backup

The Processor shall ensure adequate backup and recovery facilities to guarantee the availability of the service (and data).

A daily backup is made that allows the entire application to be restored for up to 30 days. Restoring the application is done after consultation between the parties.

The recovery time objective (RTO) in the event of an incident is 12 hours.

V Security

The Personal Data is stored and processed on systems located in a data centre that meets market standards for security.

Data in transit and in storage, including backup, is AES 256-bit encrypted.

Applications that are served via a secure connection (TLS 1.2) have a Qualys SSL Labs rating of at least "A-".

The software with which the environment is built is secured according to relevant standards such as NCSC guideline (ICT security guidelines for web applications) and OWASP top 10.

The Processor shall ensure that security patches of the underlying platform are updated and implemented in a timely manner. Critical security patches are installed as soon as possible, but within 24 hours at the latest.

Annex 3 - Sub-processors

[illegible]

Annex 4 - Standard Contractual Clauses (non-EU/EEZ transfers)

To be added if necessary: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32010D0087>

Data Processing Agreement - as Data Controller

PARTIES

Vrije Universiteit Brussel, established at 1050 Brussels, Pleinlaan 2, BE 449.012.406, represented by prof. dr. Jan Danckaert, rector, who entrusts the execution of this Agreement to [.....], hereinafter referred to as "the Controller"

AND

....., established at ... VAT or company registration number, represented by, acting in his/her capacity as,

hereinafter referred to as "the Processor"

CONSIDERING

- The parties have concluded an agreement *[e.g. a cooperation agreement]* on, concerning *[name and reference of the project]*, hereinafter referred to as "the Principal Agreement".
- The Processor will process personal data (hereinafter "the Personal Data") under the Principal Agreement in the name of, on behalf of, and as instructed by the Controller (hereinafter "the Processing").
- In the present Agreement, the Parties make arrangements regarding the Processing, taking into account the applicable legislation, in particular the [General Data Protection Regulation \(EU\) 2016/679 of 27 April 2016](#) (hereinafter "the GDPR") and the [Belgian law on the protection of personal data of 30 July 2018](#) (hereinafter jointly "the Privacy Legislation").
- All terms used in this Agreement that are defined in the Privacy Legislation are to be understood in that sense.

HAVE AGREED

Article 1. Responsibility of the Controller

The Controller guarantees to collect the Personal Data in accordance with the Privacy Legislation.

The Controller shall only make the Personal Data available to the Processor that the latter needs for the performance of the Project, and to the extent permitted by the Privacy Legislation.

Article 2. Processing

2.1. The Processor shall only process the Personal Data to the extent necessary to execute the Principal Agreement.

2.2. The Personal Data and the instructions and modalities for processing are listed in Annex 1, which will be updated whenever necessary by mutual agreement between the Parties.

2.3. The Processor shall treat all data as strictly confidential and shall respect the Privacy Legislation.

2.4. If, in the opinion of the Processor, instructions of the Controller are contrary to the Privacy Legislation, he will immediately inform the Controller. To the extent that the instructions are indeed unlawful, the Processor may refuse to comply with them.

Article 3. Staff

3.1. The Processor shall only grant access to the Personal Data to staff members to the extent necessary for the performance of the Principal Agreement.

3.2. The Processor warrants that the persons referred to in point 3.1 are subject to a duty of confidentiality and will comply with the present Agreement.

Article 4. Protection

4.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall take the necessary technical and organisational measures to protect the Personal Data, including, where appropriate, the measures listed in Article 32.1 GDPR, such as pseudonymisation and encryption.

4.2. *[optional: In particular, the Processor undertakes to take the measures described in Annex 2.]*

Article 5. Third parties

[Either: The Processor shall not communicate any Personal Data and shall not outsource the Processing in whole or in part to third parties, without the prior written consent of the Controller.]

Or: The Controller gives the Processor a general authorisation to entrust the Processing in whole or in part to the sub-processors listed in Annex 3. The Processor shall notify the Controller of any change to this list in advance, and the Controller may object to the change within one month.

Or: The Controller gives the Processor a specific authorisation [optionally: precise] to entrust the Processing in whole or in part to the sub-processors listed in Annex 3. Any additional sub-processor requires the explicit consent of the Controller.]

The Processor confirms the existence of procedures so that any third party who is granted access to the Personal Data will respect the confidentiality and security thereof, and ensures that the third parties are bound by obligations no less than those set out in the present Agreement.

This provision does not apply to persons authorised by law to have access to the Personal Data.

Article 6: Transfer to other countries

The Processor may only transfer the Personal Data to countries outside the EU and outside the countries recognised by the European Commission as having an equivalent level of protection³, after prior written consent of the Controller.

Article 7: Infringements

7.1. The Processor will inform the Controller as soon as possible and at the latest within 24 hours, of infringements in connection with the Personal Data (e.g. loss, illicit access), and provide the Controller with all information and documents necessary to assess the situation.

³ see [Adequacy decisions | European Commission \(europa.eu\)](https://european-council.europa.eu/media/en/press-room/pages/press-room.aspx?pid=14387)

7.2. It is the responsibility of the Controller to take action in the event of infringements. The Processor will provide the Controller with all necessary cooperation in this regard.

7.3. The Processor shall have a plan for dealing with infringements and shall provide the Controller with a copy of the plan or the latest version of the plan upon request.

7.4. The Processor shall keep a detailed log of all infringements and of the measures taken and shall provide the Controller with a copy thereof upon request.

Article 8. Requests from authorities and data subjects

8.1. If the Processor receives a request from a data subject in the exercise of one of its rights, the Processor shall immediately [and in any event within two working days] forward the request to the Controller.

8.2. The Controller will deal with the requests, unless the parties agree that the Processor will deal with a particular request, or unless the Processor is required to do so by law.

8.3. The Processor shall store the Personal Data in a structured, commonly used and machine-readable form, in order to guarantee their portability.

Article 9. Assistance

The parties shall assist each other as necessary to fulfil their obligations under the Privacy Legislation, including for the execution of a possible data impact assessment.

Article 10. Audit

10.1. The Controller may verify compliance with this agreement or have it verified. The Processor shall provide the Controller or his/her appointed auditor with all cooperation and all useful information and documents. The Controller will give at least seven working days' notice of the audit.

10.2. If an audit reveals that the Processor is not complying with its obligations, the Processor shall bear all costs of the audit and of the corrective measures.

Article 11. Duration and termination

This Agreement shall commence on the date of signature by both parties and shall remain in force until

[Or: This Agreement shall commence on the date of signature by both parties, and shall remain in force until termination of the Principal Agreement.]

Clauses which by their nature are intended to continue after the end of the contract, shall remain in force. These include clauses relating to:

- liability and indemnification
- settlement of disputes and applicable law.

Both parties may terminate this Agreement with immediate effect by registered letter, if the other party fails to fulfil its obligations and has not remedied this within 30 days of being served with a notice of default.

Article 12. Return of Personal Data

Within ten days after the expiry of the current Agreement, the Processor shall hand over all Personal Data and all copies thereof to the Controller, or, at the Controller's option, destroy them and confirm the destruction in writing.

This does not apply to data that need to be retained in application of the Privacy Legislation, or in application of regulations concerning the safeguarding of scientific integrity.

Article 13. Contacts

The contact persons for the implementation of this Agreement are:

- for the Processor:
- for the Controller:

(names, positions, email addresses and telephone numbers)

Article 14. Indemnification

The Processor shall indemnify the Controller against fines, administrative and corrective measures, damages **and lawyers' fees**, insofar as they result from a contractual default, a failure to comply with the Controller's lawful instructions, or an infringement of the Privacy Legislation on the part of the Processor.

Article 15. Disputes and applicable law

This Agreement is governed by Belgian law.

All disputes relating to this Agreement will be submitted to the court that has jurisdiction under the Principal Agreement [or: to the competent Dutch-language court in the district of Brussels].

Agreed and signed at _____ on _____

For the Controller

For the Processor

.....

.....

prof. dr. Jan Danckaert
rector

.....
.....

Annex 1 - Processing instructions

Data subjects	Personal Data	Processing	Purpose
e.g. patients, students, citizens of ...	e.g. Name, email address, age	Database storage and analysis	Survey on eating habits
	e.g. Age, geolocation	Movement tracking/monitoring	Mobility survey
	e.g. Mail traffic	Hosting	Hosting mailbox
	e.g. Name, answers/opinions on political landscape, image/voice	Interview recordings (and possible transcription)	Political research

The Personal Data will be processed and stored at [location].

Annex 2 - Technical and Organisational Measures

The Processor shall take at least the following measures:

I Privacy protection

The Processor acts in accordance with the GDPR and will never share the data with third parties, unless explicit permission has been granted by users.

In the event of an incident, both parties are obliged to make an effort to limit the damage as much as possible, for example by rapid direct communication and good coordination of all analysis and reports.

II Organisation

The Processor has appointed a DPO [or: Privacy Coordinator], namely [...].

The Processor shall only grant access to Personal Data to its staff to the extent necessary for compliance with and performance of this Agreement, and to the extent that such staff need access for the performance of their own duties, in function of compliance with this Agreement.

The Processor has ensured contractually binding confidentiality obligations towards its own staff.

The Processor has adopted internal procedures for the correct and timely fulfilment of its legal and contractual obligations, among others:

- for the reporting of data breaches,
- for the application of the principle of "data protection by design and by default", as set out in Article 25 of the GDPR,
- for responding to requests from data subjects,
- for carrying out data protection impact assessments,
- for the use by staff and external service providers of the IT infrastructure and other devices provided.

The Processor shall perform quarterly checks on the status of the security measures applied.

The Processor shall perform penetration tests at least once a year and shall communicate the results, including vulnerabilities by type (high, medium, low), to the Controller.

III Storage

All data is stored in a secure database.

The storage systems used offer sufficient guarantees against data loss.

IV Backup

The Processor shall ensure adequate backup and recovery facilities to guarantee the availability of the service (and data).

A daily backup is made that allows the entire application to be restored for up to 30 days. Restoring the application is done after consultation between the parties.

The recovery time objective (RTO) in the event of an incident is 12 hours.

V Security

The Personal Data is stored and processed on systems located in a data centre that meets market standards for security.

Data in transit and in storage, including backup, is AES 256-bit encrypted.

Applications that are served via a secure connection (TLS 1.2) have a Qualys SSL Labs rating of at least "A-".

The software with which the environment is built is secured according to relevant standards such as NCSC guideline (ICT security guidelines for web applications) and OWASP top 10.

The Processor shall ensure that security patches of the underlying platform are updated and implemented in a timely manner. Critical security patches are installed as soon as possible, but within 24 hours at the latest.

Annex 3 - Sub-processors

[illegible]

Annex 4 - Standard Contractual Clauses (non-EU/EEZ transfers)

To be added if necessary: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32010D0087>