Annex D - DATA PROCESSING AGREEMENT

between

Stichting Bevolkingsonderzoek Nederland

and

[Contractor's name]

Version: [version number] Date: [date]

DATA PROCESSING AGREEMENT

THE UNDERSIGNED:

1) Stichting Bevolkingsonderzoek Nederland, having its registered office and place of business in Utrecht (3511 DT) at Godebaldkwartier 435 (Gebouw Janssoenborch, 9th floor), registered in the trade register of the Chamber of Commerce under number 80204716, hereinafter referred to as: "**Controller**", duly represented in this matter by Ms A.H.J. Prieckaerts, in her capacity as director of Stichting Bevolkingsonderzoek Nederland,

and

2) **[Contractor's name]** having its registered office in [city/town] ([postcode]) at [street name and number], hereinafter referred to as: "**Processor**" and duly represented in this matter by [representative's name];

Stichting Bevolkingsonderzoek Nederland and the Contractor being collectively referred to as: "**Parties**" or separately as: "**Party**",

WHEREAS:

(A) The Centre for Population Screening of the Dutch National Institute for Public Health and the Environment (hereinafter: "RIVM-CvB") oversees the national implementation of all population screenings on behalf of the Dutch Minister of Health, Welfare and Sport. Stichting Bevolkingsonderzoek Nederland conducts population screenings under RIVM-CvB's direction.

(B) Stichting Bevolkingsonderzoek Nederland is responsible for how the population screening supply chain functions. Stichting Bevolkingsonderzoek Nederland can be regarded as the 'controller' as meant in the General Data Protection Regulation (hereinafter: "GDPR") with regard to the personal data that are processed in connection with population screenings for breast cancer, bowel cancer and cervical cancer;

(C) On [DATE], the Parties concluded an agreement concerning [description of the engagement] (hereinafter: "Principal Agreement"). This Data Processing Agreement governs the processing of personal data in connection with the population screenings. This Data Processing Agreement constitutes an Annex to the Principal Agreement and as such forms an integral part of the Principal Agreement;

(D) For the purposes of performing the Principal Agreement, the Processor will have personal data at its disposal or will be granted access to said data;

(E) The Processor is regarded as a 'processor' as meant in the GDPR;

(F) Under the GDPR, the Controller is required to conclude a Data Processing Agreement such as the present agreement with the Processor;

(G) As the Processor of the personal data, the Processor is required to provide sufficient guarantees that it will implement appropriate technical and organisational measures in such a manner that the processing of the personal data meets the requirements of the applicable law and the protection of the rights of the data subjects is ensured;

DECLARE TO HAVE AGREED AS FOLLOWS:

Article 1 Definitions

a. *Dutch Data Protection Authority*: the independent supervisory authority for the GDPR (and the Dutch Act Implementing the GDPR), as described in Article 51 of the GDPR;
b. *GDPR:* General Data Protection Regulation;
c. *Data Subject*: a natural person to whom Personal Data relates, as described in Article 4(1) of the GDPR;
d. *Processor*: a natural or legal person, public authority, agency or other body that processes Personal Data on behalf of the Controller and that does not fall under the direct authority of the Controller, as described in Article 4(8) of the GDPR, which in the present case is the Contractor;
e. *Data Processing Agreement*: the present agreement, which is part of the Principal Agreement;
f. *Special Personal Data*: Personal Data as meant in Article 9 of the GDPR;
g. *Data Breach*: a breach involving Personal Data as meant in Articles 4(12), 33 and 34 of the GDPR;
h. *Third Party*: any party that is not a Data Subject, nor the Controller, the Processor or a Sub-Processor, nor a person working under the direct authority of the Controller, the Processor or a Sub-Processor who is authorised to process the Personal Data;
i. *Data Protection Officer*: the data protection officer as meant in Articles 37-39 of the GDPR;
j. *Principal Agreement*: the agreement as described at C in the recitals;
k. *Recipient*: a recipient as described in Article 4(9) of the GDPR;
l. *Engagement*: the engagement described at C in the recitals and Article 2(2) of this Data Processing Agreement, which is performed by the Processor at the Controller's instruction;
m. *Personal Data*: any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, as described in Article 4(1) of the GDPR;
n. *Sub-Processor:* a party that processes Personal Data for the Controller at the Processor's instruction;
o. *Consent of the Data Subject*: any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her, as described in Article 4(11) of the GDPR;
p. *Processing/to Process*: any operation or set of operations which is performed on Personal Data or on sets of 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, as described in Article 4(2) of the GDPR;
q. *Controller*: a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data, as described in Article 4(7) of the GDPR, which in the present case is Stichting Bevolkingsonderzoek Nederland.

Article 2 General

1. Based on the terms of this Data Processing Agreement, the Processor undertakes to Process Personal Data exclusively at the Controller's written instructions. The Processor will Process the Personal Data in an appropriate and careful manner and in accordance with the GDPR and other applicable regulations on the Processing of Personal Data.
2. The Processor will Process Personal Data exclusively in so far as is necessary and in connection with the performance of the Contract, which is the QA-tool with secure data storage and related services.
3. If a statutory provision requires the Processor to perform any Processing activity, the Processor will notify the Controller of that statutory provision prior to said Processing activity, unless the law prohibits said notification.
4. If the Processor is of the opinion that an instruction given by the Controller is incompatible with the GDPR or any other applicable laws, the Processor will immediately notify the Controller accordingly.
5. The following information must be included and described in Annex A;
    a. the Personal Data that may be Processed for the purposes of performing the Engagement;
    b. the retention period for the Personal Data;
    c. a description of the workers (or groups of workers) with access to the Personal Data;
    d. what Processing activities may be done by which workers (or groups of workers);
    e. a list of the category or categories of Data Subjects;
    f. a description of the minimum security measures that the Processor will implement;
    g. a list of the Recipient or Recipients of the Personal Data;
    h. a list of the Sub-Processors permitted by the Controller;
    i. the risk categories must be described in Annex A, broken down by type of Personal Data.
6. If the Principal Agreement covers multiple engagements or separate parts of a single engagement, Annex A must include the Personal Data referred to at a. in the preceding paragraph for each engagement or separate part of a single engagement.
7. For the purposes of performing the Engagement, only the Personal Data described in Annex A may be Processed.

Article 3 Duty of disclosure

1. The Processor must notify the Controller immediately about any and all changes in the performance of the Principal Agreement, to ensure that the Controller can monitor compliance with the arrangements made with the Processor, including the engagement of Sub-Processors, as described in more detail in Article 5 of this Data Processing Agreement.
2. The Processor must notify the Controller immediately in writing of any questions or complaints that the Processor receives from Data Subjects, as described in more detail in Article 8 of this Data Processing Agreement.

Article 4 Processor's obligations

1. The Processor may not Process the Personal Data made available in connection with the Principal Agreement for longer than is necessary:
    a. for the performance of this Data Processing Agreement; or
    b. to fulfil its legal obligations.
2. The Processor may only Process the Personal Data at the Controller's instruction and in accordance with the written directions given by the Controller. The Processor is not permitted to Process the Personal Data for its own benefit or for the benefit of third parties, nor for its own advertising or other purposes, except where it is subject to obligations of mandatory law that dictate otherwise.

3. The Processor must lend its cooperation to the Controller's Data Protection Officer where the Data Protection Officer requires said cooperation to perform their duties.
4. The Processor will cooperate in every way requested by the Controller and/or data protection officer for the purposes of performing data protection impact assessments and any prior consultation with the supervisory authority.

Article 5 Use of Sub-Processors

1. Without the Controller's prior written permission, the Processor may not grant third parties, including companies belonging to the same group of which the Processor forms part such as subsidiaries and sister companies, access to the Personal Data, nor will the Processor engage the services of Sub-Processors.
2. If the Controller grants the above-referenced permission, it is entitled to impose requirements or to make its permission subject to a time limit.
3. The Processor is required to impose on Sub-Processors the same obligations that apply to the Processor under this Data Processing Agreement.
4. The Processor will draft a written contract with the third parties in question that reflects to terms of the preceding paragraph and the provisions of applicable laws and regulations.
5. The Controller is entitled to request what arrangements have been made between the Processor and Sub-Processors and other third parties. If and when the Controller so requests, the Processor must immediately make said arrangements available to the Controller in writing.
6. If the Controller grants general written permission to engage the services of Sub-Processors, that general permission will be included in this Data Processing Agreement.
7. If paragraph 6 applies and the services of new Sub-Processors are engaged or if any changes occur, the Processor must give the Controller advance written notice of the new Sub-Processors (and provide the other information described in Annex D) and afford the Controller a period of at least 30 days to object and, without prejudice to its other rights, put forward an alternative party.
8. The Controller will in all instances receive a list from the Processor of the Sub-Processors that it has engaged. A list of the Sub-Processors that is current on the effective date of the Principal Agreement is provided to the Controller in Annex D.
9. If the Processor engages the services of a Sub-Processor, the Processor will remain fully responsible and liable for the fulfilment of its obligations under the Principal Agreement and this Data Processing Agreement.

Article 6 Security

1. The Processor will take all appropriate technical and organisational measures with regard to Personal Data to guarantee an appropriate level of protection in accordance with the GDPR, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the Processing activities, as well as the risks of varying likelihood and severity for the rights and freedoms of Data Subjects, including the potential risks of Data Breaches including, but not limited to:
    a. damage to or loss of Personal Data;
    b. unauthorised alterations of Personal Data;
    c. misappropriation of Personal Data;
    d. unauthorised access to Personal Data.
2. The Processor will record the measures in writing and will ensure that the security as meant in this article satisfies the security requirements under the GDPR. Annex A contains a description of the minimum security measures that the Processor will implement.

3. If the Controller so requests, the Processor will promptly provide written information about the security of Personal Data (and how it is organised).

Article 7 Duty to report Data Breaches and security breaches

1. The Processor will maintain appropriate procedures to detect and take action against all potential Data Breaches, including procedures for preventive and remedial measures, and to prevent the recurrence of any Data Breaches.
2. In the event of a suspected or actual (i) Data Breach; (ii) breach of the security measures; (iii) breach of the duty of disclosure; or (iv) loss of confidential data, the Processor must notify the Controller promptly, though no later than 24 hours after the incident was first discovered, by contacting the Controller's liaison officer (or their deputy) as listed in Annex C. If the Processor is unable to contact the Controller directly and immediately, the Processor must make all reasonable effort to contact an appropriate person at the Controller's organisation directly.
3. The Processor must immediately take all reasonably necessary measures to prevent or limit any further unauthorised access, alterations and disclosure or other unlawful Processing and to end breaches of security measures, breaches of the duty of disclosure or further loss of confidential data and prevent future recurrences of the same, without prejudice to any of the Controller's rights to damages or other measures, and the Processor must provide the Controller with all reasonable information and lend its full assistance to enable the Controller to comply with its legal obligations.
4. At the Controller's request, the Processor will cooperate in informing the competent authorities and the Data Subject or Subjects.
5. The Processor must make written arrangements with the Sub-Processor or Sub-Processors about their duty to notify the Processor of any incidents, including Data Breaches, which will enable the Processor and the Controller to comply with their obligations in the event of an incident as described in paragraph 1 of this article. Those arrangements must include at a minimum the obligation that the Sub-Processor will notify the Processor of any incident as described in paragraph 1 of this article promptly, though no later than 18 hours after an incident was first discovered, by contacting the Processor's liaison officer (or their deputy) as listed in Annex C. Those arrangements must also include at a minimum that, if the Controller so requests, the Sub-Processor must cooperate in informing the competent authorities and the Data Subject or Subjects.
6. The Controller is responsible for reporting Data Breaches to the Dutch Data Protection Authority and, where applicable, the Data Subject or Subjects.

Article 8 Obligations with regard to Data Subjects

1. The Processor will lend its full cooperation to ensure that the Controller can comply with its legal obligations where Data Subjects wish to exercise their rights under the GDPR or other applicable regulations on the Processing of Personal Data.
2. If a Data Subject contacts the Processor directly with a view to exercising their rights regarding their Personal Data, the Processor will in the first instance not respond to the details of the request – unless the Controller explicitly gives other instructions – but will instead notify the Controller of the request and ask for further instructions.
3. The Processor will inform the Controller where that information is published, or hand over all relevant correspondence received.

Article 9 Audit

1. If and when the Controller so requests, the Processor will render every assistance to enable the Controller to check and audit (either directly or through a representative) whether the Processing of the Personal Data is taking place as agreed and whether the Processor has in fact taken all appropriate technical and organisational measures to ensure security against loss or against any form of unlawful Processing, and/or whether the Processor is in compliance with its obligations arising from this Data Processing Agreement, and/or whether the Processor is in compliance with its obligations arising from the applicable laws and regulations, and/or whether the Processor is in compliance with the provisions on the protection of the confidentiality, integrity, availability and security of Personal Data as described in the Principal Agreement and this Data Processing Agreement.
2. In addition to the foregoing, the Processor will also conduct its own audit (a 'regular audit') with regard to these matters once every two years. The Processor must conduct annual regular audits with regard to any Processing activity involving high-risk Personal Data. A situation is any case deemed to involve a high risk if it involves Processing Special Personal Data.
3. If and when so asked, the Processor must provide the findings from the regular audits, in the form of a third-party statement, to the Controller and/or the Processor.
4. For each month, within five business days after the start of the following calendar month the Processor must prepare a report on its security management, which includes at a minimum the following information:
    a. the number, status, progress and analysis of incidents;
    b. the security management measures that have been taken in response to incidents;
    c. the general data protection measures that have been taken.
5. The audit costs will be borne by the Controller, unless the audit findings show that the Processor has failed to comply with its obligations, in which case the costs will be borne by the Processor. This provision does not prejudice the Controller's other rights, including the right to claim performance and/or damages.
6. If it is established during an audit that the Processor has failed to comply with its obligations, the Processor must take all reasonably necessary measures to ensure compliance.

Article 10 International traffic

1. The Processor warrants that all Processing of Personal Data performed by or on behalf of the Processor, including any Sub-Processors that it engages, in connection with the performance of the Principal Agreement will take place in the European Economic Area (EEA) or from countries that guarantee an appropriate level of protection in accordance with the applicable privacy regulations.
2. Without explicit and prior written permission, the Processor is not permitted to transfer Personal Data to, store them in or make them accessible from any country outside the EEA. Under no circumstances whatsoever are such transfers permitted if the country in question does not have an appropriate level of protection in place as meant in the GDPR.
3. The Controller is entitled to attach conditions to its permission, including, but not limited to, the obligation for the Processor to demonstrate its compliance with the legal obligations regarding data traffic with countries outside the EEA.
4. If the technical features of a transfer medium render this impossible to guarantee, the transmission of data will only take place in encrypted form, using advanced technologies (which are at least as advanced as is common in the market).
5. Before concluding this Data Processing Agreement, the Processor must disclose the location or locations where the Processor and the Sub-Processors will Process data.

Article 11 Requests and orders from authorities and bodies

1. If the Processor receives a request or order from a Dutch or foreign supervisory authority, government body or investigation, prosecution or national security agency to provide Personal Data (or access to Personal Data), the Processor must notify the Controller promptly, meaning within 24 hours. The Processor must also establish whether that request is lawful.
2. When dealing with the request or order, the Processor must comply with all the Controller's instructions (including, where applicable, any instruction to let the Controller handle the request or order in whole or in part) and provide all reasonably necessary assistance.
3. If a request or order prohibits the Processor from complying with its obligations as described in paragraphs 1 and 2 of this article, the Processor must act in accordance with the Controller's reasonable interests. To that end, the Processor will at a minimum:
    a. have a legal review conducted into (i) the extent to which the Processor is legally required to comply with the request or order; and (ii) whether the Processor is in fact not permitted to comply with its obligations in respect of the Controller based on the above;
    b. only cooperate with the request or order if it is legally required to do so and, where possible, object (if necessary at law) to the request or order or to the prohibition on informing the Controller about the matter or following the Controller's instructions;
    c. not provide more or other Personal Data or further information than is strictly necessary to ensure compliance with the request or order;
    d. in the event of a transfer to a country outside the EEA: examine the possibilities for complying with Chapter V of the GDPR;
    e. immediately inform the Controller about the request or order and what action was taken as soon as that is permitted.
4. In the present Data Processing Agreement 'legal' and 'legally' refer to the laws and regulations not only of the Netherlands, but also of other countries.

Article 12 Non-disclosure

1. All Personal Data that are Processed in connection with this Data Processing Agreement and/or the Principal Agreement are confidential data.
2. The Processor will impose the obligations, including the security and non-disclosure obligations, recorded in this Data Processing Agreement and the Principal Agreement on the workers that it involves and on other persons that it appoints, in so far as they are not already bound by an appropriate legal duty of non-disclosure. The Processor must ensure that said workers and other persons whom it appoints will comply with all obligations arising from this Data Processing Agreement and the Principal Agreement.

Article 13 Liability and indemnity

1. Without prejudice to the Processor's liability on other potential grounds, the Processor is independently liable for all loss/damage that arises from non-compliance with this Data Processing Agreement or any rules laid down in applicable laws and/or regulations including, but not limited to, the GDPR. The Processor indemnifies the Controller against any and all associated loss/damage and costs, including but not limited to the costs of legal assistance.
2. If the Controller is held liable by a Data Subject or a third party for loss/damage that the Data Subject or third party claims to have suffered in connection with the Processing of the Personal Data, the Controller will be entitled to take recourse against the Processor if the Processor failed to comply with any of its obligations under the law or this Data Processing Agreement. The Processor indemnifies the Controller against all associated claims of Data Subjects and third parties, including fines and due and payable damages.

Article 14 Amendments

1. If the Controller is of the opinion that a change in the Personal Data that are to be Processed or a risk analysis of the Processing of Personal Data gives cause to do so, if and when the Controller so requests the Parties will discuss the possibilities for amending the arrangements recorded in this Data Processing Agreement.
2. Before the new arrangements are applied, they must first be recorded in writing and become part of this Data Processing Agreement.
3. Under no circumstances may the amendments render it impossible for the Controller and/or the Processor to comply with the GDPR or other relevant laws and regulations on the Processing of Personal Data.

Article 15 Duration and termination

1. This Data Processing Agreement will take effect on the same date as the Principal Agreement takes effect and will also end at the same time and in the same manner as the Principal Agreement.
2. It is not possible to cancel or otherwise terminate this Data Processing Agreement separately from the Principal Agreement.
3. Obligations which by their nature are intended to remain in effect after this Data Processing Agreement is terminated will continue to apply after this Data Processing Agreement has been terminated. This includes, but is not limited to, the obligations arising from the provisions regarding non-disclosure; liability and indemnity; and governing law and dispute resolution.
4. On termination of the Principal Agreement for whatever reason and in whatever manner, at the Controller's discretion the Processor (without charging any fee or costs) will take the following action:
    a. destroy all Personal Data provided to it in connection with the Engagement, or else some of the Personal Data as determined by the Controller, regardless of their location,
    b. transfer all Personal Data provided to it in connection with the Engagement, or else some of the Personal Data as determined by the Controller, to a successor to the role of processor or to the Controller; or
    c. give the Controller the opportunity to withdraw the Personal Data, or else some of the Personal Data as determined by the Controller, from the Engagement.
5. The Controller is entitled to impose further requirements as to how the Personal Data are made available, including requirements with regard to the file format, or the destruction.
6. The Processor will make the Personal Data available in a readable and commonly used digital file format if the Controller so requests and at any time the Controller so desires after the Data Processing Agreement has ended.

Article 16 Governing law and dispute resolution

1. In the event of any inconsistencies between the provisions of the Principal Agreement and those of this Data Processing Agreement, the provisions of this Data Processing Agreement will prevail, unless the Controller wishes to invoke the provisions of the Principal Agreement.
2. This Data Processing Agreement and its performance are governed by Dutch law.
3. The Processor's general terms of supply or other general or specific terms and conditions do not apply to this Data Processing Agreement.

Any and all disputes that arise between the Parties in connection with this Data Processing Agreement will be brought before the competent Court of the Hague.

AGREED, AND DRAWN UP AND SIGNED IN DUPLICATE IN [CITY/TOWN] ON [DATE]

Ms A.H.J. Prieckaerts	[name of the Controller's representative]
Stichting Bevolkingsonderzoek Nederland	[Processor]

Annex A

Overview of the Services and associated Processing activities

Description of the Services: [to be filled in by the Controller and the Processor]

Personal Data Processing activities:
The Processor will Process the Personal Data as follows:

[List of Personal Data]

Description of the systems:

[description of the systems]

Description of the Processing activities:

Purposes for which the Personal Data are Processed	[ ]		
Duration of the Processing activities	[ ]		
Categories of Data Subjects	[ ]		
Personal Data Processed by the Processor, where applicable differentiated according to their sensitivity	[ ]		
Groups of Workers that the Processor engages and that have (or may have) access to the Personal Data	[ ]	[ ]	[ ]
Actions that those persons may conduct with those Personal Data	[ ]	[ ]	[ ]

Description of the Personal Data (or categories of Personal Data) Processed by the Processor:
Categories of Personal Data that are Processed and entered by the Processor:
[ ]

The following data may be stored in:
[ ]

The following data are taken from:

[ ]

AGREED, AND DRAWN UP AND SIGNED IN DUPLICATE IN [CITY/TOWN] ON [DATE]

Ms A.H.J. Prieckaerts	[name of the Controller's representative]
Stichting Bevolkingsonderzoek Nederland	[Processor]

Annex B

Reliability requirements and security measures

Where applicable, differentiated according to the sensitivity of the Personal Data (or categories of Personal Data) listed in Annex A.

Applicable reliability requirements

Below, the Controller establishes the requirements that must be satisfied with regard to the availability, integrity and confidentiality of the Processing of data. With due observance of the requirements listed below, the Processor must ensure an appropriate level of security.

	Low	Medium	High
Availability			X
Integrity			X
Confidentiality			X

Further details in the shape of concrete technical and organisational measures

General measures

- The responsibilities for information security have been assigned.
- The Processor has selected workers who are trained and experienced in the field of information security.
- The Processor is certified to professionally offer and support its services and products in respect of the Controller (ISO27001, ISO9001, ISO13485, CE-certification of products).
- The Processor will periodically conduct its own internal audits to guarantee the required proof of its compliance with the standards and requirements.
- The Processor has agreed on appropriate communication, support and management procedures with the Controller, and agrees to act in accordance with those procedures.
- A security policy has been adopted and implemented.
- Business continuity management, continuity plans.

Availability

Project work may not disrupt the activities. The availability level of the new system to be supplied must be “High” starting as soon as it is put into use. While project work is being carried out, the availability of the new system that is to be supplied will not impact the activities.

The following measures must be taken with regard to the availability requirement:

- Example: Back-up SQL database
- Example: Redundant archiving of the data over 2 data centres

Integrity

The following measures must be taken with regard to the integrity requirement:

- Example: Testing of the tools (including migration tools) before data are migrated to the new system that is to be supplied

Confidentiality

The following measures must be taken with regard to the reliability requirement:

- Example: Data must be stored in the Processor's secure data centre
- Example: System access must be based exclusively on personal accounts
- Example: Automatic logging
- Example: Logical access control with regard to 2-step verification

AGREED, AND DRAWN UP AND SIGNED IN DUPLICATE IN [CITY/TOWN] ON [DATE]

Ms A.H.J. Prieckaerts	[name of the Controller's representative]
Stichting Bevolkingsonderzoek Nederland	[Processor]

Annex C

Liaison officers (and their deputies)

Controller	Liaison officer 1	Liaison officer 2 (deputy)
Liaison officer's name and job title	Ms S. Blauw, Data Protection Officer	Mr P. de Raad National Security Officer
Telephone number	06 49 31 24 51	06 13 36 88 26
Other details, including email address	Sandra.blauw@bevolkingsonderzoeknederland.nl	Patrick.deraad@bevolkingsonderzoeknederland.nl

Processor	Liaison officer 1	Liaison officer 2 (deputy)
Liaison officer's name and job title	[Name] [job title]	[Name] [job title]
Telephone number	[telephone number]	[telephone number]
Other details, including email address	[email address]	[email address]

Annex D

Sub-Processors

List of Sub-Processors that the Processor has engaged

Most recent update: [date]

#	Full legal name of Sub-Processor	Location	Type of service (Processing of data)	Technical and organisational measures to ensure compliance with the GDPR
1				
2				
3				