Your Research

Annex 2

PROCESSOR AGREEMENT

Increase participant retention

Improve study team efficiency

Build a base of reliable data

www.yourresearch.com

Document information

This Processor agreement is a supplement to and forms an inseparable part of the general terms and conditions of Your Research B.V. Your Research B.V. is responsible for the (version) management of this document.

Version history

Versie	Datum	Auteur	Wijzigingen
1.0	01-06-2022	Menno Weij	First version
1.1	10-10-2022	Kees van Ooik	Final version
1.2	01-08-2023	Elin Zwier	Review
1.3	14-12-2023	Kees van Ooik	Added sub-processors
1.4	05-04-2024	Kees van Ooik	Added information to Annex 1 for more information about data classification and retention Added information to Annex 2 for more information about security measures

Assumptions

- The Controller is a research organization/healthcare institution and uses the services of the Processor in that context;
- The Processor provides the Controller with a license for the software developed by the Processor ("Your Research Software"), and in this capacity can process (special) personal data for the Controller;
- The Processor will only gain access to personal data for the purpose of making analyses of the (proper) operation of the Your Research Software with the express consent of the Controller. The Processor may process special or other personal data for the Controller as part of its normal intended use. Furthermore, upon the Controller's explicit request, the Processor can also correct (medical) personal data if these have been placed with the wrong patient by a user of the Controller; in this latter case, the Parties will also agree on an additional assignment for this purpose. The above is under the full ultimate responsibility of the Controller;
- The Parties acknowledge that the Processor has no or insufficient knowledge of the medical content data;
- The Controller and the Processor have entered into an Agreement, of which this Processing Agreement forms part;
- With regard to the processing of personal data, the Controller is to be regarded as the controller within the meaning of Article 4 recitals and under 7 of the General Data Protection Regulation ("GDPR");
- With regard to storing and processing the personal data for the Controller, the Processor is to be regarded as a processor within the meaning of Article 4 opening words and under 8 of the GDPR;
- The Parties wish - partly in implementation of the provisions of Article 28, paragraph 3 of the GDPR - to lay down a number of conditions in the present agreement which are applicable to their relationship in connection with the aforementioned activities for and on the instructions of the Controller, and the processing of personal data as part of those activities.

Declare that they have agreed as follows:

Article 1 Definitions

1.1 In this Processing Agreement, the following terms, always written with a capital letter, will have the following meanings whether they are used in the plural or singular:

- Annex: annex to the Processing Agreement, which forms an integral part of the Processing Agreement;
- Agreement: the agreement concluded between the Controller and the Processor and the accompanying appendices and further (general) terms and conditions;
- Personal Data: all data that can be directly or indirectly traced back to a natural person as referred to in Article 4, opening words and under 1 of the GDPR;
- Subprocessor: the subcontractor engaged by the Processor, who, in the context of this Processing Agreement, processes Personal Data on behalf of the Controller as referred to in Article 28, paragraph 4 of the GDPR;
- Processing: the processing of Personal Data as referred to in Article 4, opening words and under 2 of the GDPR;
- Processing Agreement: the present agreement which forms part of the Agreement, including Annex.

1.2 The provisions of the Agreement apply in full to the Processing Agreement. Insofar as the Agreement contains provisions regarding the processing of personal data, the provisions of this Processing Agreement prevail.

Article 2 Controller and Processor of the data

2.1 The Processor undertakes to process Personal Data on the Controller's instructions in the context of this Processing Agreement. An overview of the type of Personal Data, the categories of data subjects, and the purposes for which the Processing of Personal Data takes place is included in Annex 1. The Controller warrants that the data described in this Annex 1 are complete and correct, and indemnifies the Processor against claims resulting from an incorrect representation.

2.2 The Parties agree that, in principle, the Processor has no direct access to the Personal Data. The Processor and persons working for it will only gain access to the Personal Data if they have been explicitly instructed to do so by the Controller unless the Processor cannot reasonably be expected to ask the Controller for permission first because access is strictly necessary to resolve malfunctions, which the Controller instructs the Processor to do by means of this Processing Agreement.

2.3 The Processor is only responsible for the Processing of the Personal Data under this Processing Agreement, in accordance with the Controller's lawful instructions and under the express (ultimate) responsibility of the Controller. The Processor is not responsible for any other Processing of Personal Data, including but not limited to the collection of the Personal Data by the Controller, Processing for purposes not notified to the Processor, Processing by third parties, and/or for other purposes. The responsibility for these Processing operations rests exclusively with the Controller.

2.4 The Controller is liable for the Processing of Personal Data within the framework of the Agreement and guarantees that the content and the Processing (and the order to so process) of those Personal Data complies with all applicable laws and regulations and does not infringe any rights of third parties. The Controller indemnifies the Processor against all claims of third parties, in particular of the supervisory authority, that in any way follow from non-observance of this guarantee.

2.5 The Processor undertakes to Process Personal Data only for the purposes of the activities referred to in this Processing Agreement and/or the Agreement. The Processor guarantees that, without the explicit and written consent of the Controller, it will not use the Personal Data Processed under this Processing Agreement unless a legal provision applicable to the Processor obliges it to do so. In such event, the Processor will notify the Controller of the statutory provision prior to the Processing, unless such legislation prohibits such notification for important grounds of public interest.

Article 3 Technical and organizational measures

3.1 As far as reasonably possible, taking into account the state of the art, the implementation costs, as well as the nature, scope, context, and processing purposes and the different risks for the rights and freedoms of persons in terms of probability and severity, the Processor will implement appropriate technical and organizational measures to ensure a risk-adjusted security level. These measures will at least include the measures to be taken on the basis of the current security policy of the Controller. The Controller is familiar with the Processor's certifications for ISO 27001 and NEN 7510. See Annex 2 for an overview of measures taken by the Processor.

3.2 Insofar as the Processing of Personal Data is carried out by or on behalf of the Controller itself via the Your Research Telemonitoring Platform, the Controller guarantees that it has taken appropriate policy and organizational measures to prevent unlawful Processing of Personal Data. The Processor is entitled to check the security measures taken by the Controller before proceeding with Processing.

Article 4 Confidentiality

4.1 In accordance with the Agreement, the Processor will impose secrecy on all its employees with regard to the Personal Data.

Article 5 Transfer

5.1 The transfer of Personal Data by the Processor outside the European Economic Area is only permitted in compliance with the applicable legal obligations.

Article 6 Third parties and subcontractors

6.1 The Processor is permitted to make use of Subprocessors in the context of this Processing Agreement and the Agreement. Any future Subprocessors will be listed in Annex 3. The current Subprocessors are listed in Annex 2.

6.2 If the Processor wishes to engage a Subprocessor or another Subprocessor, the Processor will inform the Controller of the intended changes. The Controller must object to these changes within 10 working days.

6.3 The Processor contractually obliges any new/other Subprocessor to comply with similar obligations in respect of data protection as those set out in this Processing Agreement, except in the case of a Subprocessor as referred to in 6.4. In that case, the provisions in Article 6.4 will apply.

6.4 In deviation from Article 6.3, the Processor may rely on the provisions of the agreement between the Processor and the Subprocessor as listed in Annex 3, if and insofar as relevant under this Processing Agreement, including in any case the confidentiality obligations, notification obligations, and security measures. The Controller explicitly agrees with both the content of and the method of online or other references to the relevant terms and conditions of this Subprocessor.

Article 7 Liability

7.1 With regard to the liability of Processor under the Processing Agreement, as well as with regard to the indemnification obligations for the Processor included in the Processing Agreement, the Processor's liability is limited to the liability arrangement in the Agreement.

7.2 Without prejudice to Article 7.1 of this Processing Agreement, the Processor is only liable for the loss caused by the Processing in case this Processing did not comply with the GDPR's obligations specifically geared towards the Processor or if the Processor has acted in conflict with the Controller's lawful instructions.

7.3 To avoid misunderstanding: the provisions in the Processing Agreement and/or the Agreement regarding liability are without prejudice to the mandatory provisions of Article 82 of the GDPR.

Article 8 Incidents

8.1 If the Processor becomes aware of an incident that may have a (material) impact on the security of Personal Data, it will i) notify the Controller without unreasonable delay and ii) take all reasonable measures to prevent or limit (further) violation of the GDPR.

8.2 Insofar as is reasonable, the Processor will cooperate with the Controller and support the Controller in the performance of its legal obligations in respect of the identified incident.

8.3 Insofar as is reasonable, the Controller will support the Processor in its obligation to report the personal data breach to the Dutch Data Protection Authority ("Dutch DPA") and/or the data subject, as referred to in Article 33, paragraph 3 and Article 34, paragraph 1 of the GDPR. The Processor is never obliged to independently notify a personal data breach to the Dutch DPA and/or the data subjects.

8.4 The Processor is never liable for correct and/or timely performance of the obligation to notify to which the Controller is subject as referred to in Articles 33 and 34 of the GDPR.

Article 9 Assistance to the Controller

9.1 The Processor will, as far as is reasonably possible, assist the Controller in performing its obligation under the GDPR to answer requests to exercise the rights of a data subject, in particular the right to inspection (Article 15 of the GDPR), rectification (Article 16 of the GDPR), deletion (Article 17 of the GDPR), restriction (Article 18 of the GDPR), portability (Article 20 of the GDPR) and the right to object (Articles 21 and 22 of the GDPR). The Processor will forward a complaint or request from a data subject relating to the Processing of Personal Data as soon as possible to the Controller, who will be responsible for handling the request. The Processor is entitled to charge the Controller for any costs involved in the cooperation.

9.2. The Processor will, as far as reasonably possible, assist the Controller in performing its obligation under the GDPR to carry out a data protection impact assessment (Articles 35 and 36 of the GDPR). In that case, the Parties will make further (written) arrangements.

9.3. The Processor will provide the Controller with all of the information which is reasonably required to show that the Controller has complied with its obligations under the GDPR.

9.4. The Processor will enable the Controller (i) at most once per calendar year, or (ii) if there is justified reason to do so on the basis of a specific situation, both subject to a reasonable period of notice and with the consent of the Processor, to check compliance with the Processing Agreement and in particular the security measures taken by the Processor. Such an audit will at all times be conducted in a manner that will have the least possible effect on the normal operations of the Processor and will be at the expense of the Controller. The Processor is entitled to charge the Controller for any costs incurred in complying with the provisions of this Article. If the Processor is of the opinion that an instruction relating to the provisions of this paragraph constitutes a breach of the GDPR or of any other privacy law applicable to it, the Processor will immediately inform the Controller.

9.5. The audit in Article 9.4 only takes place after the Controller has requested and assessed the similar audit reports present at the Processor and has brought forth reasonable arguments that justify an audit initiated by the Controller. Such an audit is justified if the similar audit reports present at the Processor do not or do not sufficiently give a definitive answer regarding compliance with the provisions in the Processing Agreement.

Article 10 Termination & Miscellaneous

10.1. Without prejudice to the specific provisions of the Agreement, the Processor will offer the Controller the choice of deleting the processed Personal Data or returning them to the Controller, and removing existing copies, unless the Processor is legally obliged to continue storing the Personal Data (or parts thereof).

10.2. The Controller will properly inform Processor about statutory and other retention periods that apply to the Processing of Personal Data for the Processor.

10.3. The obligations of this Processing Agreement which by their nature are intended to survive termination will also survive termination of this Processing Agreement.

ANNEX 1 OVERVIEW OF PERSONAL DATA

TYPE OF PERSONAL DATA:

- First name;
- Last name;
- Gender;
- Date of birth;
- E-mail address;
- Telephone number;
- Address;
- IP-address;;
- Timezone
- Special personal data: medical history;
- Other special personal data: different per type of research. Participants agree to the collection of this information via the informed consent procedure.

CATEGORIES OF DATA SUBJECTS:

- Subjects: persons who show interest in participating in the study and have accepted the privacy statement for this;
- Participants: people who participate in a study and have also given informed consent for this.
- Staff: persons preparing and conducting research or using Your Research software.

For more information regarding data retention and (on request):

- 02.13 POL Data Classification & retention periods

PURPOSES OF PROCESSING:

- Determine whether a participant is eligible to join a study.
- Collection of data in the context of the research.
- Being able to assign a personal unique account.
- Possibility to invite people for research.
- Support of participants and staff

ANNEX 2 SPECIFICATION OF THE SECURITY MEASURES

1. the management of powers and authorizations of employees, to prevent unauthorized access to information;
2. measures in case the confidentiality of the Personal Data is damaged;
3. measures in case of calamities;
4. measures to prevent viruses, threats, and technical vulnerabilities;
5. taking the necessary measures to prevent security breaches as referred to in the applicable privacy regulations;
6. the use of servers that are only accessible via secure connections;
7. the ability to repair the availability of and access to the Personal Data in a timely manner in the event of a physical or technical incident; and
8. a procedure for testing, assessing, and evaluating the effectiveness of the technical and organizational measures to ensure the security at regular intervals.

For more information regarding security measures (on request):

- 02.16 POL Data Protection Compliance Statement
- 02.14 POL Application Security
- ISO-27001 certificate

ANNEX 3 OVERVIEW OF SUB PROCESSORS

Microsoft Azure for hosting
Amazon Web Services for email
Twilio for SMS notification

.

Your Research

+31(0)85 0043 969 • info@yourresearch.com

www.yourresearch.com