Data Processing Agreement of *Brancheorganisaties Zorg*
(Association of Healthcare Sector Organizations)

United in

DATA PROCESSING AGREEMENT

THE PARTIES HERETO:

1. [Name of Controller], having its registered office at [address] in [town] and registered in the Business Register of the Chamber of Commerce under number [KVK number], for the purposes hereof duly represented by [title, name and job title] (hereafter referred to as the "**Controller**"); and

2. [Name of Processor], having its registered office at [address] in [town] and registered in the Business Register of the Chamber of Commerce under number [KVK number], for the purposes hereof duly represented by [title, name and job title] (hereafter referred to as the "**Processor**");

hereinafter also referred to collectively as the "Parties" and individually as a "Party";

WHEREAS:

(a) the Processor performs services for the Controller as described in the Main Agreement [title/reference/date] to which this Data Processing Agreement is annexed as Schedule [X];
(b) the services entail the processing of personal data;
(c) the Processor processes the data in question only on the Controller's instructions and not for its own purposes;
(d) this processing of personal data is governed by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as the "GDPR");
(e) in this Data Processing Agreement the Parties wish to set forth their understandings with regard to the processing of personal data in the context of the services;
(f) this Data Processing Agreement supersedes any similar Main Agreements previously entered into between the Parties, where applicable;
(g) the Association of Healthcare Sector Organizations (*Brancheorganisaties Zorg*) has drafted this Data Processing Agreement to provide a standard agreement;

HEREBY AGREE AS FOLLOWS:

Article 1. Definitions

1.1. Capitalized terms used but not defined in this Data Processing Agreement have the meaning given in the GDPR (including the terms Personal Data, Data Subject, Controller and Processor).

1.2. In this Data Processing Agreement, the following capitalized terms have the following meanings:

a)	Breach	i	an investigation into or seizure of Personal Data by government officials, or the likelihood of such an investigation or seizure;
		ii	a Personal Data breach as defined in Article 4(12) of the GDPR;
b)	Staff Member		a natural person employed by or working for one of the Parties who is involved in the implementation of this Data Processing Agreement.
c)	Main Agreement		the Main Agreement/s in respect of the provision of products and/or services to which this Data Processing Agreement is annexed as a Schedule.
d)	Data Subject Request		A complaint about the processing of Personal Data or a request for exercising the rights of the Data Subject set out in Chapter III of the GDPR.

1.3. Any reference in this Data Processing Agreement to specific standards (such as NEN 7510) is to be read as a reference to the most recent version of such standards. To the extent that the standard in question is no longer maintained, it must be deemed superseded by the most recent version of its logical successor.

Article 2. Subject matter of this Data Processing Agreement and description of Schedules

2.1. This Data Processing Agreement governs the processing of Personal Data by the Processor on the instructions of the Controller in the context of the performance of the Main Agreement.

2.2. The following Schedules form part of this Data Processing Agreement:
   a) Schedule 1: Description of the processing operations
   b) Schedule 2: Security of Personal Data
   c) Schedule 3: Contact information in connection with processing/Breaches/Data Subject Requests.

2.3. This Data Processing Agreement forms an integral part of the Main Agreement. In the event that any provisions of the Data Processing Agreement conflict with the provisions of the Main Agreement, the provisions of the Data Processing Agreement prevail.

Article 3. The processing of Personal Data

3.1. The Processor guarantees that it will process Personal Data on behalf of the Controller only if:
   a) this is necessary for the performance of the Main Agreement (within the scope of the description contained in Schedule 1); or
   b) the Controller has given written instructions to do so.

3.2. The Processor will follow all reasonable instructions of the Controller in connection with the processing of Personal Data. The Processor will immediately notify the Controller if, in its opinion, instructions are contrary to applicable legislation on the processing of Personal Data.

3.3. Without prejudice to the provisions of paragraph 1 of this article 3, the Processor is allowed to process Personal Data if the Processor is required to do so by a legal requirement (including court orders or administrative orders based thereon). In such a case the Processor must inform the Controller of the intended processing and that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The Processor will enable the Controller, where possible, to oppose such compulsory processing and otherwise to restrict the compulsory processing to what is strictly necessary.

3.4. The Processor will process Personal Data in a verifiably proper and careful manner and in accordance with the obligations incumbent upon the Processor under the GDPR and other laws and regulations.

3.5. The Processor will not process Personal Data or have third parties process Personal Data in countries outside the European Economic Area ("EEA") without the Controller's express prior permission in writing.

3.6. The Processor ensures that Staff Members sign a non-disclosure agreement or guarantees that Staff Members will maintain confidentiality with regard to the processing of Personal Data.

Article 4. Security of Personal Data and audit (*version: data concerning health*)
[Please delete if not applicable]

4.1. The Processor will verifiably take suitable and effective technical and organizational security measures which, taking into account the state of the art and the costs involved, are appropriate to the nature (specified in 0) of the Personal Data to be processed, in order to protect the Personal Data against loss, unauthorized disclosure, data corruption or any form of unlawful processing, as well as to guarantee the (timely) availability and integrity of the data. These security measures include any measures described in the Main Agreement.

4.2. The Processor holds ISO 27001 or similar certification or verifiably works in accordance with ISO 27001 and has implemented appropriate written data protection policies for the processing of Personal Data, setting out at least the measures referred to in paragraph 1 of this article 4.

4.3. The Processor holds NEN 7510 certification or verifiably works in accordance with NEN 7510 and has implemented appropriate written data protection policies for the processing of Personal Data. Where applicable, the Processor verifiably meets the security requirements for network connections described in NEN 7512 and the logging requirements described in NEN 7513.

4.4. At the Controller's request, the Processor will submit a valid certificate (or a copy of a valid certificate) issued by an independent third party with relevant expertise, as well as a Statement of Applicability, if available to the third party, or a Third Party Memorandum (TPM), showing that the Processor complies with the obligations under this article.

4.5. The Processor itself regularly commissions internal and/or external audits regarding compliance with the above-mentioned standards.

4.6. The Controller has the right to monitor (or cause to be monitored) compliance with the measures mentioned in articles 4.1 to 4.3 if so requested by the Controller in connection with

breaches (or suspected breaches) of information security or privacy. The Processor and the Controller determine by mutual agreement when and by which independent third party the audit is carried out. The Processor will follow any reasonable instructions to amend the data protection policies, given by the Controller further to such an audit, within a reasonable period.

4.7. The Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Processor will therefore periodically evaluate the measures implemented on the basis of this article 4 and will improve these measures where necessary in order to maintain compliance with the obligations under this article 4. The above provisions are without prejudice to the Controller's right to give instructions to take additional measures (or to ensure that additional measures are taken) if necessary.

Article 4. Security of Personal Data and audit (*version: data not concerning health*)
[Please delete if not applicable]

4.1. The Processor will verifiably take suitable and effective technical and organizational security measures which, taking into account the state of the art and the costs involved, are appropriate to the nature (specified in 0) of the Personal Data to be processed, in order to protect the Personal Data against loss, unauthorized disclosure, data corruption or any form of unlawful processing, as well as to guarantee the (timely) availability and integrity of the data. These security measures include any measures described in the Main Agreement.

4.2. The Processor holds ISO 27001 or similar certification or verifiably works in accordance with ISO 27001 and has implemented appropriate written data protection policies for the processing of Personal Data.

4.3. At the Controller's request, the Processor will submit a valid certificate (or a copy of a valid certificate) issued by an independent third party with relevant expertise, if available to the third party, or a Third Party Memorandum (TPM), showing that the Processor complies with the obligations under this article.

4.4. The Processor itself regularly commissions internal and/or external audits regarding compliance with the above-mentioned standards.

4.5. The Controller has the right to monitor (or cause to be monitored) compliance with the measures mentioned in articles 4.1 to 4.3 if so requested by the Controller in connection with breaches (or suspected breaches) of information security or privacy. The Processor and the Controller determine by mutual agreement when and by which independent third party the audit is carried out. The Processor will follow any reasonable instructions to amend the data protection policies, given by the Controller further to such an audit, within a reasonable period.

4.6. The Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Processor will therefore periodically evaluate the measures implemented on the basis of this article 4 and will improve these measures where necessary in order to maintain compliance with the obligations under this article 4. The above provisions are without prejudice to the Controller's right to give instructions to take additional measures (or to ensure that additional measures are taken) if necessary.

Article 5. Monitoring, information obligations and incident management

5.1. The Processor will actively monitor for security breaches and report the monitoring results to the Controller in accordance with this article 5.

5.2. When a Breach occurs or has occurred, the Processor must notify the Controller's contact specified in Schedule 3 accordingly without delay, but no later than 24 hours after becoming aware of it, and provide all relevant information on:

1) the nature of the Breach;
2) the Personal Data (potentially) affected;
3) the observed and likely consequences of the Breach; and
4) the measures taken or proposed to be taken to remedy the Breach or to minimize the consequences/damage.

5.3. Without prejudice to the other obligations under this article, the Processor is obliged to take measures it may reasonably be expected to take in order to remedy the Breach as soon as possible or to minimize the further consequences. The Processor will consult with the Controller as soon as possible, but within 24 hours, in order to make further arrangements in this respect.

5.4. The Processor will cooperate with the Controller at all times, will follow the Controller's instructions and will conduct a proper investigation into the Breach. The Processor will prepare a report on this, including a proper response and appropriate follow-up steps. The Processor will share this report with the Controller as soon as possible to enable the latter to inform the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*, hereinafter "AP") and/or the Data Subject in a timely manner. Only the Controller may report a Breach to the AP and/or Data Subjects.

5.5. Notifications with respect to Breaches and Data Subject Requests are sent to the Controller's contact specified in Schedule 3.

5.6. The Processor is not permitted to disclose information about Breaches to Data Subjects or other third parties, except to the extent that the Processor is under a legal obligation to do so or the Parties have agreed otherwise.

5.7. If and to the extent that the Parties have agreed that the Processor maintains direct contact with authorities other than the AP, or with other third parties, in relation to a Breach, the Processor will keep the Controller informed of such contacts on an ongoing basis.

Article 6. Cooperation obligations

6.1. The GDPR and other legislation confer certain rights upon Data Subjects. The Processor will provide its full and timely cooperation to the Controller in the performance of the Controller's obligations arising out of these rights.

6.2. The Processor must forward a Data Subject Request it has received with respect to the processing of Personal Data to the Controller as soon as possible, but within 24 hours.

6.3. The Processor must furnish the Controller upon request with all relevant information regarding the aspects of its processing of Personal Data so as to enable the Controller to use that information to prove that it complies with applicable data protection and other laws.

6.4. Furthermore, the Processor must give the Controller all necessary assistance, at the Controller's request, in performing the legal obligations incumbent upon the Controller under

applicable data protection legislation, including the conduct of a data protection impact assessment (DPIA).

Article 7. Use of sub-processors

7.1. The Processor may not outsource its activities consisting of or requiring the processing of Personal Data to a sub-processor without informing the Controller thereof three months in advance and without giving the Controller the opportunity to notify the Processor of any objections it may have. If the Controller has any objections, the Processor will make reasonable efforts to resolve those objections or to change the performance of the services mentioned in the Main Agreement – without impairing the provision thereof – to prevent the processing of Personal Data by the proposed (new) sub-processor.

7.2. If the Processor is unable to resolve the Controller's objections or to change the performance of the services to prevent the processing of Personal Data by the proposed sub-processor, the Controller may suspend or terminate all or part of the Main Agreement subject to six months' notice from the end date of the objection period. During a suspension of the Main Agreement because of objections to a (new) sub-processor and from the end date of the Main Agreement, the Controller will not be obliged to pay the Processor any fees under the Main Agreement or otherwise or any compensation for any loss suffered.

7.3. Article 7.1 does not apply to the sub-processors specified in Schedule 1.

7.4. The Processor will impose on such sub-processor at least the same obligations as those arising for the Processor from this Data Processing Agreement and the law. The Processor will set out these agreements in writing and monitor compliance by the sub-processor with those agreements. The Processor must provide the Controller upon request with a copy of the data processing agreement concluded with the sub-processor.

7.5. The Processor remains fully liable to the Controller for the consequences of outsourcing work to a sub-processor. The use of sub-processors outside the EEA requires permission as set out in article 3.5 of this Data Processing Agreement.

Article 8. Costs

8.1. Data processing costs inherent in the normal performance of the Data Processing Agreement and in the exercise of rights of Data Subjects are deemed to be included in the fees already payable under the Main Agreement.

Article 9. Term of agreement and termination

9.1. This Data Processing Agreement takes effect on the date of its signature and the term of this Data Processing Agreement is equal to the term of the Main Agreement, including any extensions thereof.

9.2. Once signed by both Parties, the Data Processing Agreement forms an integral and inseparable part of the Main Agreement. Termination of the Main Agreement, regardless of how it is terminated (by giving notice or by cancellation), automatically results in termination of the Data Processing Agreement in the same manner, except as otherwise agreed between the Parties in individual cases.

9.3. Obligations which by their nature are intended to survive termination of this Data Processing Agreement will continue in force after termination of this Data Processing Agreement. These

obligations include the obligations arising out of the provisions relating to confidentiality and non-disclosure, liability, dispute resolution and governing law.

9.4. Each of the Parties has the right, without prejudice to the relevant provisions of the Main Agreement, to suspend the performance of this Data Processing Agreement and the associated Main Agreement or to terminate this Data Processing Agreement and the associated Main Agreement without court intervention with immediate effect, if:
   a) the other Party is wound up or otherwise ceases to exist;
   b) the other Party is demonstrably in serious breach of its obligations under this Data Processing Agreement and such attributable breach is not remedied within 30 days following a written notice of default to that effect;
   c) either Party is placed into liquidation or applies for court protection from creditors (*surseance van betaling*).

9.5. In view of the Controller's heavy dependence on the Processor and the continuity risk in the event of incidents and crisis situations (such as bankruptcy), the Processor declares in advance that it is willing to make additional agreements with the Controller, at the Controller's request, in order to mitigate such risks.

9.6. The Controller is entitled to cancel (*ontbinden*) this Data Processing Agreement and the Main Agreement with immediate effect if the Processor indicates that it is unable or no longer able to meet the reliability requirements imposed on the processing of Personal Data by legislation and/or case law.

9.7. The Processor must inform the Controller as soon as possible of any proposed acquisition or transfer of ownership. The Controller has the right to terminate the Main Agreement in the event of compelling objections to the change of ownership, without being liable to pay compensation.

9.8. The Processor may not transfer this Data Processing Agreement and the rights and obligations relating to this Data Processing Agreement to a third party without the Controller's express permission in writing.

9.9. The obligations under this Data Processing Agreement continue in force as long as the Processor processes Personal Data of the Controller, even after the Processor has ceased to provide the care, services and/or facilities to be provided under the Main Agreement for the benefit of the Controller.

Article 10. Retention periods, return and destruction of Personal Data

10.1. The Processor may not retain Personal Data for longer than strictly necessary. The statutory retention periods and any retention periods agreed between the Parties as set out in Schedule 1 also qualify as strictly necessary periods. Under no circumstances will the Processor retain Personal Data beyond the end of this Data Processing Agreement. The Controller determines whether data should be retained and, if so, for how long.

10.2. On termination of the Data Processing Agreement or, where applicable, on expiry of the agreed retention periods, or at the Controller's written request, the Processor will, at reasonable cost and at the Controller's option, irreversibly destroy the Personal Data (or cause the Personal Data to be irreversibly destroyed) or return the Personal Data to the Controller. At the Controller's request the Processor must provide proof that the data have been irreversibly destroyed or deleted. In the event that the data are returned, they must be

returned electronically, in a commonly used, structured and documented data format. If it is impossible to return, irreversibly destroy or delete Personal Data, the Processor must notify the Controller of this immediately. In that case the Processor guarantees that it will treat the Personal Data in confidence and will no longer process them.

Article 11. Final provisions

11.1. If one or more of the provisions of this Data Processing Agreement are void or voidable, the remaining provisions remain in full force and effect.

11.2. This Data Processing Agreement is governed by the laws of the Netherlands.

11.3. Disputes about or in connection with this Data Processing Agreement will be submitted to the exclusive jurisdiction of the courts or arbitrator/s specified in the Main Agreement.

<Name of Controller>	<Name of Processor>
<Name of Controller's representative>	<Naam of Processor's representative>
<Title>	<Title>
Town: _____	Town: _____
Date: _____	Date: _____

Schedule 1: Description of the processing operations

Description of activities and/or services, scope and general purpose of the processing (specify the number of Personal Data/Data Subjects):

Specify the Main Agreement: title / reference / start date / Parties: Describe the activities and/or services: Specify the general purpose of the processing: Specify the number of Personal Data/Data Subjects:

Processing	Type of Personal Data	Categories of Data Subjects	Purposes of processing	Basis for processing	Data transfers outside the EEA	Agreements on retention periods	Agreements on deletion procedure
Specify the type of processing (e.g. hosting, transfer, maintenance or name of the application).	Specify the type of Personal Data (e.g. name and address, BSN, health data, etc.)	Specify Data Subjects (patients, staff members, students, etc.)	Specify the purposes of the processing.	Specify the basis for the processing.	If yes, specify the storage/processing outside the EEA, name the country and describe the instrument on the basis of which transfer can take place (Chapter V of the GDPR) and additional measures.	Describe the agreements regarding retention periods.	Describe the deletion procedure.

Sub-processors

Sub-processor	Description of service and Personal Data	Data outside the EEA	Data processing agreement
Name and address (including the country)	Describe	Yes/No (if yes, specify the country and describe the instrument on the basis of which transfer can take place (Chapter V of the GDPR) and additional measures)	Yes/No

Explanation:

Personal Data are data relating to someone (or data that can be traced back to someone). Any information relating to an identified or identifiable natural person constitutes Personal Data. Someone can be identified, for example, on the basis of an identifier such as a name, an identification number, location data, an online identifying variable or other characteristic elements. Examples include physical, physiological, genetic, psychological, economic, cultural and social elements.

Any **processing** must have one or more specified, explicit and legitimate **purposes**. This refers to the purpose or purposes for which the Personal Data have been obtained/collected. Make the **purpose/purposes of processing** as concrete as possible.

Grounds for the processing of Personal Data: Consent given by Data Subject / Necessary for the performance of a contract / Legal obligation / Protection of the Data Subject's vital interests / Task carried out in the public interest or in the exercise of official authority / Legitimate interests pursued by the Controller or by a third party.

Schedule 2: Security of Personal Data

In this Schedule Processor should demonstrate what measures Processor has implemented to process Personal Data securely.

If Processor holds relevant information security **certification** (**ISO 27001** and, in case of care processes, **NEN 7510**), Processor is requested to attach copies of the relevant documentation and provide the **Statement of Applicability (SoA)** (what measures have been/have not been implemented?) and the **Description of Scope** (what is covered by the certification?).

The Processor holds the following certification (copies, SoA and Description of Scope have been attached as appendices to this Data Processing Agreement):

If Processor does not hold relevant certification or if Processor holds a certificate issued by a certifying body without an accreditation statement from the Dutch Accreditation Council (*Raad voor Accreditatie*), Processor may use a Third Party Memorandum (TPM)[1] to demonstrate that Processor operates in accordance with ISO 27001 and, where applicable, NEN 7510. Processor can then attach this TPM to this Schedule.

[1] This is a declaration by an independent third party, for example an accountant.

Schedule 3: Contact information in the event of Breaches/Data Subject Requests

Controller's contact details:

Processor's contact details: