embloom

Processing Agreement

Version 1.3 - 01-09-2019

APPLICABILITY

This Processing Agreement applies to all forms of processing of Personal Data that Embloom B.V. (hereinafter: Processor) undertakes for the other party to which it provides services (hereinafter: Controller). By activating and logging into the (test) account that has been made available and thus make use of the services of the Processor, the Controller agrees to this agreement and its provisions. The General Conditions of the Processor apply to and form an inextricable part of this Processing Agreement.

WHEREAS:

(a) The Controller wishes to make use of the services of the Processor with regard to the development and provision of Application(s), which contain various instruments for measuring, monitoring and treating clients/patients within the health care sector;

(b) the Services entail the processing of Personal Data, including data relating to health;

(c) the Processor processes the data only by order of the Controller and not for own purposes.

(d) With effect from 25 May 2018, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) will apply.

(e) The Parties wish to record their agreements with regard to the processing of Personal Data within the framework of the services in this Processing Agreement.

(f) Where applicable, this Processing Agreement replaces any previous agreement(s) of a similar nature between the Parties.

DECLARE TO HAVE AGREED AS FOLLOWS:

Artikel 1. Definitions

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

a) General Data Protection Regulation or GDPR — Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

b) Data Subject — an identified or identifiable natural person (article 4(1) GDPR.

c) Third Party — a third party as referred to in article 4(10) GDPR.

d) Data Protection Officer — an officer as referred to in article 37 et seq. GDPR.

e) Incident —

i a complaint or (information) request from a Data Subject with regard to the processing of Personal Data by the Processor;

ii an investigation or seizure of Personal Data by government officials or a suspicion that this will take place;

iii a breach with regard to Personal Data as referred to in article 4(12) GDPR;

iv any unauthorised access, deletion, mutilation or loss or any other form of unlawful processing of Personal Data.

f) Employee — the natural person engaged by the Parties for the performance of this Processing Agreement, who is employed by or works for one of the Parties.

g) Agreement(s) — the agreement(s) listed in appendix 1 for the provision of products and/or services.

h) Party — the Controller or the Processor.

i) Parties — the Controller and the Processor.

j) Personal Data — all information on an identified or identifiable natural person within the meaning of article 4(1) GDPR.

k) Subprocessor — each non-subordinate third party that is engaged by the Processor for the Processing of Personal Data within the framework of the Agreement, not being Employees

l) Processor — the Processor as referred to in article 4(8) GDPR

m) Processing Agreement — the present agreement.

n) Controller — the controller as referred to in article 4(7) GDPR

o) Dutch Personal Data Protection Act (*Wet bescherming persoonsgegevens, Wbp*) — Act of 6 July 2000, containing rules on the protection of personal data (Data Protection Act), as amended.

1.2. The aforementioned and other terms shall be interpreted in accordance with the GDPR. Until 25 May 2018, terms shall be interpreted in accordance with the similar provision of the Wbp.

1.3. Where this Processing Agreement refers to certain standards (such as NEN7510), it always refers to the most current version thereof. In so far as the relevant standard is no longer being maintained, one shall read instead the most current version of the logical successor of that standard.

1.4. Any derogations from the text are only valid in so far as they are specified in appendix 4. The provisions of appendix 4 prevail over any other provisions of this processing agreement.

Artikel 2. Subject of this Processing Agreement

2.1. This Processing Agreement relates to the processing of Personal Data by the Processor by order of the Controller within the framework of the performance of the Agreement(s).

2.2. The parties conclude the Agreement(s) in order to use the expertise that the Processor has with regard to the processing and protection of Personal Data for the purposes arising from the Agreement(s) and described in more detail in this Processing Agreement. The Processor guarantees that it is qualified for this.

2.3. This Processing Agreement forms an inextricable part of the Agreement(s). In so far as the provisions of the Processing Agreement conflict with the provisions of the Agreement(s), the provisions of the Processing Agreement prevail.

Artikel 3. Implementation of the processing

3.1. The Processor guarantees that it will only process Personal Data for the Controller in so far as:

a) this is necessary for the performance of the Agreement (within the frameworks as specified in appendix 1); or

b) the Controller has given further written instructions thereto.

3.2. Within the framework of the provisions of the first paragraph of article 3(a), the Processor will only process the Personal Data specified in appendix 1 within the framework of the nature and purposes of the processing described in that appendix.

3.3. The Processor will follow all reasonable instructions of the Controller with regard to the processing of the Personal Data. The Processor will immediately notify the Controller if it believes that instructions conflict with the legislation applicable to the processing of Personal Data.

3.4. Without prejudice to the provisions of the first paragraph of this article 3, the Processor is allowed to process Personal Data if a statutory provision (including judicial or administrative orders based thereon) oblige it to such processing. The Processor shall in that case first notify the Controller of the intended processing and the statutory provision, unless the relevant legislation forbids such a notification for important reasons of public interest. Where possible, the Processor will enable the Controller to defend itself against such obligatory processing and also otherwise limit the obligatory processing to what is strictly necessary.

3.5. The Processor will demonstrably process the Personal Data in a proper and careful manner and in accordance with the obligations resting on it as Processor under the GDPR, the Wbp - in so far as still applicable -, and other laws and regulations. In this context the Processor will in any case keep a register of processing operations as referred to in article 30 GDPR and provide the Controller with a copy of this register on demand.

3.6. If the provision of services by the Processor implies the processing of health data or other sensitive Personal Data, the Processor guarantees that it will not act in conflict with health legislation.

3.7. Unless with the express prior written permission of the Controller, the Processor will neither itself nor have third parties process Personal Data in countries outside the European Economic Area ("EEA").

3.8. The Processor guarantees that Employees involved have signed a confidentiality agreement and allow the Controller inspection of this confidentiality agreement on request.

Artikel 4. Security of Personal Data and checks

4.1. The Processor shall demonstrably take appropriate and effective technical and organizational security measures, which in the light of the current state of the art and the costs associated with it correspond to the nature of the Personal Data to be processed, as specified in appendix 1, in order to protect the Personal Data against loss, unauthorised access, mutilation or any form of unlawful processing, as well as to guarantee the (timely) availability of the data. These security measures include any measures already stipulated in the Agreement. The measures include in any case:

a) measures to guarantee that only authorised Employees have access to the Personal Data for the stated purposes;

b) measures to the effect that the Processor only gives access to the Personal Data to Employees and Subprocessors via accounts registered in their names, while the use of those accounts is adequately logged and the relevant accounts only give access to those Personal Data to which the relevant (legal) person must necessarily have access;

c) measures to protect the Personal Data against accidental or unlawful destruction, accidental loss or alteration, unauthorised or unlawful storage, processing, access or disclosure;

d) measures to identify weak spots with regard to the processing of Personal Data in the systems that are used to provide services to the Controller;

e) measures to guarantee the timely availability of the Personal Data;

f) measures to guarantee that the Personal Data are processed logically separated from any personal data it processes for itself or on behalf of third parties;

g) the other measures that the Parties have agreed, as recorded in appendix 2.

4.2. The Processor will demonstrably work in accordance with ISO27001 and/or NEN7510 and has implemented an appropriate, written security policy for the processing of Personal Data, in which in any case the measures referred to in the first paragraph of this article 4 are set out.

4.3. The Processor will demonstrably comply with the safety requirements on network connections as described in NEN7512.

4.4. The Processor will demonstrably meet the requirements on logging as described in NEN7513.

4.5. The Processor will demonstrably comply with the requirements of other NEN standards in so far as they have been declared applicable to the health care sector.

4.6. On demand of the Controller, the Processor will submit a valid certificate issued by an independent external expert, if it has one, evidencing that the Processor complies with the obligations set out in this article.

4.7. The Controller has the right to monitor or have monitored the compliance with the measures referred to under articles 4.1 up to and including 4.4. If the Controller so requests, the Processor will give the Controller at least once a year the opportunity to check this or have this checked, at a time specified by the Parties in consultation with each other and furthermore if the Controller sees reason thereto in response to (suspected) information or privacy incidents. The Processor will reasonably cooperate in such an investigation. The Processor will follow any instructions regarding adaptation of the security policy reasonably given by the Controller in response to such an investigation, within a reasonable period.

4.8. The Parties recognize that security requirements change constantly and that effective security requires frequent evaluation and regular improvement of outdated security measures. The Processor will therefore periodically evaluate the measures as implemented under this article 4 and, where necessary, improve the measures in order to remain compliant with the obligations under this article 4. The preceding provisions do not affect the Controller's authority to instruct the taking or having taken of additional measures, if necessary.

Artikel 5. Monitoring, information duties and incident management

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

5.2. Once an Incident occurs, has occurred or could occur, the Processor is obliged to notify the Controller immediately and provide all relevant information on:

1) the nature of the Incident;
2) the (possibly) affected Personal Data;
3) the observed and the probable consequences of the Incident; and
4) the measures that have been taken or will be taken to resolve the Incident or limit the consequences/damage as much as possible.

5.3. Without prejudice to the other obligations arising from this article, the Processor is obliged to take the measures that can reasonably be expected of it in order to remedy the Incident as quickly as possible or limit the further consequences as much as possible. The Processor will forthwith enter into consultations with the Controller to make further agreements on this.

5.4. The Processor will at all times cooperate with the Controller and follow the Controller's instructions and enable the Controller to carry out a proper investigation into the Incident, formulate a correct response and take appropriate follow-up steps with regard to the Incident, including the provision of information to the Dutch Data Protection Authority (AP) and/or the Data Subject as provided in article 5.8.

5.5. The Processor will at all times have written procedures in place that enable it to provide the Controller with an immediate response to an Incident and effectively cooperate with the Controller in handling the Incident. The Processor will provide the Controller with a copy of such procedures if the Controller so requests.

5.6. Reports that are made under article 5.2 will immediately be sent to the Controller or, where relevant, to Employees of the Controller made known by the Controller in writing during the term of this Processing Agreement. If the Controller has appointed a Data Protection Officer (DPO), the reports will be sent to this DPO.

5.7. The Processor is not allowed to provide information on Incidents to Data Subjects or other third parties, except in so far as the Processor is under a legal obligation to do so or the Parties have agreed otherwise.

5.8. If and in so far as the parties have agreed that the Processor maintains direct contact with authorities or other third parties in relation to an Incident, the Processor will keep the Controller constantly informed thereof.

Artikel 6. Cooperation obligations

6.1. The GDPR and other (privacy) legislation grant specific rights to the Data Subject. The Processor will give its full and timely cooperation to the Controller in complying with the obligations resting on the Controller pursuant to these rights.

6.2. A complaint or request from a Data Subject regarding the processing of Personal Data that is received by the Processor, will immediately be forwarded by the Processor to the Controller.

6.3. On demand of the Controller, the Processor will provide all relevant information on aspects of the processing of Personal Data carried out by it to the Controller, so that the Controller can demonstrate, partially on the basis of that information, that it complies with the applicable (privacy) legislation.

6.4. On demand of the Controller, the Processor will furthermore give all necessary assistance in complying with the statutory obligations resting on the Controller pursuant to the applicable privacy legislation (such as making a privacy impact assessment).

Artikel 7. Engagement of subprocessors

7.1. The Processor will not outsource its activities, in so far as consisting of or requiring the processing of Personal Data, to a Subprocessor without the prior written permission of the Controller. The foregoing does not apply to the Subprocessors listed in appendix 1.

7.2. In so far as the Controller consents to the engagement of a Subprocessor, the Processor will impose on this Subprocessor the same or stricter obligations as arise for itself from this Processing Agreement and the law. The Processor will record these agreements in writing and monitor compliance with them by the Subprocessor. On request, the Processor will provide the Controller with a copy of the agreement(s) concluded with the Subprocessor.

7.3. Notwithstanding the Controller's permission for engaging a Subprocessor to (partially) process data on behalf of the Processor, the Processor will remain fully liable to the Controller for the consequences of outsourcing work to a Subprocessor. The Controller's permission for outsourcing work to a Subprocessor does not alter the fact that the engagement of Subprocessors in a country outside the European Economic Area requires permission in accordance with article 3.7 of this Processing Agreement.

Artikel 8. Liability

8.1. Either Party is responsible and liable for its own actions.

8.2. Any limitation of liability in the Agreement applies *mutatis mutandis* to this Processing Agreement, provided that:

a) any (implicit or explicit) exclusions of liability for loss and/or mutilation of Personal Data are excluded;

b) any (implicit or explicit) exclusions of liability for fines imposed by the Dutch Data Protection Authority or another supervisory authority that are directly related to an attributable failure of the Processor or an action or omission attributable to the Processor, are excluded.

8.3. The Processor shall indemnify the Controller and hold the Controller harmless for any claims or actions of third parties, as well as for fines imposed by the Dutch Data Protection Authority that directly arise from an attributable failure of the Processor and/or its subcontractors/Subprocessors in complying with its or their obligations under this Processing Agreement and/or any violation by the Processor and/or its subcontractors/Subprocessors of the legislation applicable in the field of the processing of Personal Data.

8.4. In so far as the Parties are jointly and severally liable to third parties, including the Data Subject, or jointly have a fine imposed by the Dutch Data Protection Authority, they are obliged to each other, each for the portion of the debt accruing to it in their mutual relationship, to contribute to the debt and costs in accordance with the provisions of Book 6, Title 1, Section 2 of the Dutch Civil Code, unless the GDPR provides otherwise, in which case the GDPR prevails.

8.5. In so far as the Agreement does not contain a limitation of liability for the Controller, the limitation contained in paragraph 2 for the Processor also applies to the Controller.

8.6. Any limitation of liability will furthermore expire for a Party in the event of intent or gross negligence on the part of that Party.

8.7. The Parties will arrange for adequate cover of their liability.

Artikel 9. Costs

9.1. The costs of the processing of data that are inherent to the normal performance of the Agreement are deemed included in the fees already payable under the Agreement.

9.2. Any supporting services or other additional services that the Processor shall provide under this Processing Agreement or that are requested by the Controller, including any requests for additional information, will be charged to the Controller on the basis of the rates specified in appendix 3.

9.3. The foregoing provision does not apply if the work relates to a failure of the Processor under this Processing Agreement. The work will in that case be carried out free of charge (without prejudice to the Controller's right to recover the damage actually suffered from the Processor).

Artikel 10. Duration and termination

10.1. This Processing Agreement takes effect on the date of signing and the duration of this Processing Agreement is equal to the duration of the Agreement(s) referred to in appendix 1, including any extensions thereof.

10.2. Once it has been signed by both Parties, this Processing Agreement forms an integral and inextricable part of the Agreement(s). Termination of the Agreement(s), for whatever reason (termination/dissolution), has the effect that the Processing Agreement is terminated for the same reason (and vice versa), unless the Parties agree otherwise in a specific situation.

10.3. Obligations that by their nature are intended to remain in effect after termination of this Processing Agreement, will continue to apply after termination of this Processing Agreement. These provisions include, for example, those arising from the provisions regarding confidentiality, liability, settlement of disputes and applicable law.

10.4. Either Party is entitled, without prejudice to what is provided thereon in the Agreement, to suspend the performance of this Processing Agreement and the related Agreement or terminate it with immediate effect, without judicial intervention being required, if:

a) the other Party is dissolved or otherwise ceases to exist;

b) the other Party demonstrably fails [seriously] in complying with the obligations arising from this Processing Agreement, and fails to remedy such an attributable failure within 30 days after a written notice of default to that effect;

c) a Party is declared bankrupt or applies for a suspension of payments.

10.5. In view of the Controller's high dependency on the Processor and the continuity risk in the event of incidents and disasters (such as a bankruptcy), the Processor declares now for then to be prepared, on demand of the Controller, to make supplemental agreements with the Controller to reduce the aforementioned risks. Such supplementary agreements can include:

a) agreements on periodically returning or providing to a third party the data processed by the Processor; and/or

b) an agreement with a third party to the effect that the third party undertakes joint and several liability for or guarantees performance of the Agreement; and/or

c) a (tripartite) agreement with a third party to the effect that the third party will (constantly) have all data at its disposal that are necessary to be able to, where appropriate, deliver or start delivering (a part of) the performances under the Agreement - under a new agreement or otherwise -, instead of or parallel to the Processor.

10.6. The Processor has an exit plan for compliance with all the obligations under this Processing Agreement in the event that the Agreement or this Processing Agreement is terminated (before the end of its term). The Processor will provide a copy of this plan on demand of the Controller.

10.7. The Controller is entitled to terminate this Processing Agreement and the Agreement with immediate effect, if the Processor informs it that it cannot, or no longer, meet the reliability requirements that are set on the processing of the Personal Data in the light of developments in the legislation and/or the case law.

10.8. The Processor shall inform the Controller well in advance of an intended acquisition or transfer of ownership.

10.9. Without the express written permission of the Controller, the Processor is not allowed to transfer this Processing Agreement and the rights and obligations associated with this Processing Agreement to a third party.

Artikel 11. Retention periods, return and destruction of Personal Data

11.1. The Processor will retain the Personal Data no longer than strictly necessary, including the statutory retention periods or any agreement made between the Parties on retention periods, as recorded in appendix 1. Under no circumstances will the Processor retain the Personal Data longer than until the end of this Processing Agreement. The Controller decides if and how long data must be retained.

11.2. On termination of the Processing Agreement or, if applicable, on expiry of the agreed retention periods or at the written request of the Controller, the Processor will, for a reasonable fee, at the discretion of the Processor, definitively destroy or have destroyed the Personal Data or return them to the Controller. At the request of the Controller, the Processor will provide proof of the fact that the data have been definitively destroyed or deleted. If data are returned, this will be done in a generally accepted, structured and documented data format and by electronic means. If return, definitive destruction or deletion are not possible, the Processor will immediately notify the Controller. The Processor guarantees in that event that it will treat the Personal Data confidentially and no longer process them.

Artikel 12. Intellectual property rights

12.1. In so far as the (collection of) Personal Data is protected by any intellectual property right, the Controller gives the Processor permission to use the Personal Data within the framework of the performance of this Processing Agreement.

Artikel 13. Final provisions

13.1. The recitals form part of this Processing Agreement.

13.2. In the event of nullity or voidability of one or more of the provisions of this Processing Agreement, the remaining provisions will remain in full effect.

13.3. In all situations not provided for by this Processing Agreement, the Parties will decide in consultation with each other.

13.4. This Processing Agreement is governed by Dutch law.

13.5. The Parties will endeavour to resolve any conflicts in consultation with each other. This includes the possibility to agree that the dispute shall be resolved by means of mediation or arbitration.

13.6. Disputes over or in connection with this Processing Agreement will be submitted exclusively to the court or arbitrator(s) designated for this purpose in the Agreement.

Bijlage 1: Description of Personal Data, nature of processing, etc.

This Processing Agreement is an appendix to the following Agreements and relates to the following processing of Personal Data.

Agreements	Offer Embloom (the agreement is concluded by signing the offer) or trial account.
Brief description of services	Providing an e-health platform for diagnostics, impact measurement and treatment of psychological and physical problems.
Nature of the processing	Processing patient data and customer data
Type of Personal Data	*Controller*: • Personal details and contact information; • Communications data and correspondence (digital and written); • Contract data (contractual relationship, products and services, financial data, etc.); • Usage data (data, information, data files or materials that user sends/has sent to the Applications during the use of the Services). *Data Subject:* • Personal details and contact information; • Medical data (diagnosis, test results, etc.); • Communications data and correspondence (digital and written); • Usage data (data, information, data files or materials that user sends/has sent to the Applications during the use of the Services).
Categories of data subjects	Care providers, employees, patients, family members, friends and other relations and persons on whom the patient or care provider enters information during the use of the application.
Purposes of the processing	Diagnostics, impact measurement and treatment of psychological and/or physical problems.
Approved subprocessors	• True: Hosting provider (www.true.nl) • Stepco: Backups office environment, including e-mails (www.stepco.nl) • KPN: Zorg Messenger – Secure communications and data exchange (www.kpn.nl/zakelijk) • VANAD Enovation: ZorgMail – Secure communications and data exchange (www.zorgmail.nl) • Zivver: Secure communications and data exchange (www.zivver.nl) • Spryng: SMS authentication (www.spryng.nl) • AFAS: Invoicing customers (www.afas.nl) • FreshMail: Newsletter customers (www.freshmail.com) • Teamleader: Relationship management / CRM (www.teamleader.nl)
Agreements on retention periods	Data of Data Subjects will be retained during the term of the agreement, unless the Controller orders deletion of data. After termination of the agreement, the data of Data Subjects will be deleted from the database of the Processor, and will be deleted automatically from the backups of the Processor within three months. Data of the Controller will be retained in accordance with statutory requirements.

Bijlage 2: Description of further security measures

Buildings

Technical and organizational measures to prevent physical access by unauthorised persons to buildings where the data processing takes place:

- door security (electric door opener with access registration and logged key allocation);
- video surveillance with motion sensor and recording function;
- burglar alarm system with follow-up by the security service.

Network and computers

Technical and organizational measures to prevent access by unauthorised persons to the network and the computers of the Processor:

- disk encryption is applied to all workstations;
- each workstation is provided with anti-virus software that is automatically updated;
- computers are automatically updated when security updates become available;
- authentication with user name and password;
- password allocation and policy (including requirements on length and complexity);
- passwords may only be stored in a digital (offline) password safe;
- computers are automatically locked after a period of inactivity;
- use of differentiated authorisations;
- only administrators can install/uninstall software;
- number of administrators is reduced to the "most necessary";
- logging of access and actions of all users;
- the use of data carriers or e-mail for sensitive data is only allowed if necessary, at the request of the Controller and adequately encrypted (AES-256 or stronger);
- the networks are protected by a firewall;
- the corporate network is separated from the guest network.

Application

Technical and organizational measures to prevent access by unauthorised persons to the application that processes Personal Data:

- all communications with the application are encrypted;
- authentication with user name and password;
- password allocation and policy (including requirements on length and complexity);
- options for two-step authentication;
- options for IP restrictions;
- use of differentiated authorisations (based on customer, roles and permissions);
- number of administrators is reduced to the "most necessary";
- logging of access and actions of all users;
- automatic log off after a period of inactivity;
- automatic blockade after too many failed login attempts;
- server access is blocked on the basis of IP address;
- Processor has protocols for (further) development and management of the application;
- the security of the application is periodically tested in practice by independent parties.

Application development

Technical and organizational measures that the Processor follows during the (further) development of the application;

- security requirements are set when the specifications are drawn up;
- security requirements are included and tested in test scripts;
- regression tests are included and performed in test scripts;
- all communications from/to the application are encrypted;
- authentication and authorisation are tested at all times;
- input of data is always validated;
- output of data is always validated and cleaned up to prevent invalid or harmful output;
- permissions are set as defensively as possible;
- code is developed as defensively as possible;
- logging can be extended if necessary;
- review procedure for the implementation of third-party codes;
- developed code is reviewed by another person than the developer(s) of the code;
- developed code is tested by two different persons who have not developed the code;
- if rejected code is adjusted, a new review and test are performed;
- there are separate environments for development, testing, acceptance and production;
- personal data of production are not used for development, testing and acceptance.

Employees

Measures that employees of the Processor must comply with:

- employees receive training in the field of privacy and information security;
- employees have signed a confidentiality statement;
- employees shall submit a certificate of good conduct (VOG) when they enter the employment;
- employees are bound to rules of conduct regarding responsible use of the application, buildings, computers, printers, e-mail and internet of the Processor;
- employees shall report (potential) security incidents to the security officer.

Availability

Technical and organizational measures to guarantee the availability of the systems and applications of the Processor:

- systems bearing the application of the Processor are placed with an ISO27001 and NEN7510 certified provider;
- systems bearing the application of the Processor are scalable;
- systems bearing the application of the Processor are designed redundantly;
- systems bearing the application of the Processor are provided with an emergency power supply;
- systems bearing the application of the Processor are only accessible for administrators of the provider;
- the provider has climate control in server rooms;
- the provider has fire and smoke detection systems in server rooms;
- the provider applies (pro)active monitoring to the systems of the Processor;
- the provider makes daily snapshots of the entire application environment of the Processor;

- the provider makes daily data backups of the application environment of the Processor;
- the Processor makes a daily off-site data backup of the application environment;
- data backups are kept for three months;
- the Processor retains data of the Controller for an indefinite period of time and only destroys them when the agreement of the Controller with the Processor is terminated;
- the Processor periodically tests the ability to recover the data backup;
- the Processor applies (pro)active monitoring to its applications;
- the Processor has a Business Continuity Plan in place.

Bijlage 3: Specification rates

The hourly rate is € 110,- excluding VAT.

Bijlage 4: Adjustments to the standard text

Art.	Text that is deleted	Replacement text	Reason
1.1. g	the agreement(s) listed in appendix 1 for the provision of products and/or services.	each agreement, including the trial account, for the provision of services by the Processor to the Controller that involves the processing of Personal Data by the Processor for the Controller.	The Controller can make use of the services of the Processor under an agreement that is concluded by signing the offer or requesting a trial account.
7.1	The Processor will not outsource its activities, in so far as consisting of or requiring the processing of Personal Data, to a Subprocessor without the prior written permission of the Controller. The foregoing does not apply to the Subprocessors listed in appendix 1.	The Controller gives the Processor permission to (partially) outsource activities that consist of or require the processing of personal data to others than the Subprocessors listed in appendix 1, provided that the Processor notifies the Controller before the engagement starts. The Controller may object to the engagement of a Subprocessor, after which the Parties will consult on a suitable solution. If no suitable solution is found, the Controller will be allowed to terminate the Agreement with the Processor with immediate effect.	The prevention of an (unnecessary) administrative burden if new Subprocessors are engaged. The Controller remains entitled to oppose the engagement of a new Subprocessor, but need not give its written approval. In addition to the aforementioned reason, there are more reasons why the old article 7.1 leads to an unworkable situation. For example, the situation could arise that the implementation of new functionalities is delayed in expectation of the written approval of all Controllers.
7.2	In so far as the Controller consents to the engagement of a Subprocessor, the Processor will impose on this Subprocessor the same or stricter obligations as arise for itself from this Processing Agreement and the law. The Processor will record these agreements in writing and monitor compliance with them by the Subprocessor. On	The Processor will impose on this Subprocessor the same or stricter obligations as arise for itself from this Processing Agreement and the law. The Processor will record these agreements in writing and monitor compliance with them by the Subprocessor. On request, the Processor will provide the Controller with a copy of the agreement(s) concluded with the Subprocessor.	Textual adjustments resulting from the change in 7.1.

	request, the Processor will provide the Controller with a copy of the agreement(s) concluded with the Subprocessor.		
7.3	Notwithstanding the Controller's permission for engaging a Subprocessor to (partially) process data on behalf of the Processor, the Processor will remain fully liable to the Controller for the consequences of outsourcing work to a Subprocessor. The Controller's permission for outsourcing work to a Subprocessor does not alter the fact that the engagement of Subprocessors in a country outside the European Economic Area requires permission in accordance with article 3.7 of this Processing Agreement.	The Processor remains fully liable to the Controller for the consequences of outsourcing work to a Subprocessor. The Controller's permission for outsourcing work to a Subprocessor does not alter the fact that the engagement of Subprocessors in a country outside the European Economic Area requires permission in accordance with article 3.7 of this Processing Agreement.	Textual adjustments resulting from the change in 7.1.
10.1	This Processing Agreement takes effect on the date of signing and the duration of this Processing Agreement is equal to the duration of the Agreement(s) referred to in appendix 1, including any extensions thereof.	This Processing Agreement enters into effect at the moment when the Controller makes use of the services of the Processor for the first time and remains in effect as long as the Processor provides services to the Controller that involve the processing of Personal Data by the Processor for the Controller.	Textual adjustments resulting from the change in 1.1 under g.
10.2	Once it has been signed by both Parties, this Processing Agreement forms an integral and inextricable part of the Agreement(s). Termination of the Agreement(s), for whatever reason (termination/dissolution), has the effect that the Processing	The Processing Agreement forms an integral and inextricable part of the Agreement. Termination of the Agreement or cooperation, for whatever reason (termination/dissolution), has the effect that the Processing Agreement is terminated for the same reason	This Processing Agreement will not be signed. The Processor shall accept the Processing Agreement and the General Conditions digitally.

	Agreement is terminated for the same reason (and vice versa), unless the Parties agree otherwise in a specific situation.	(and vice versa), unless the Parties agree otherwise in a specific situation.	