



associated in



## PROCESSOR AGREEMENT (May 2018)

### THE PARTIES TO THE AGREEMENT:

1. The healthcare institution or user which/who purchases services from Familienet B.V. (in the following: “**Data controller**”); and
2. Familienet B.V., established on Verlengde Hereweg 174 in Groningen and listed in the register of the Chamber of Commerce under number 04022404, for the present purpose legally represented by Maarten Bloemink Sr., director (subsequently “**Processor**”).

In the following also jointly referred to as: “Parties” and individually as “Party”.

### CONSIDERING THAT:

- (a) Processor carries out services for the benefit of Data controller, as described in the agreements described in Appendix 1.
- (b) The services entail that Personal data are processed, including data regarding health.
- (c) Processor processes the data in question exclusively by order of Data controller and not for own purposes.
- (d) As of 25 May 2018 is applicable the Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 (GDPR or its Netherlands ratification AVG).
- (e) Parties wish to establish the arrangements regarding the processing of Personal data in the context of the services in this Processor agreement.
- (f) This Processor agreement, if applicable, replaces all previous Agreement(s) of equal tenor.

### DECLARE TO HAVE AGREED AS FOLLOWS:

#### Article 1. Definitions

1.1. In this Processor agreement, by the concepts below with a capital letter is intended as follows:

- |    |                                                           |                                                                                                                                                                                                                                                                         |
|----|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| a) | ‘Algemene Verordening Gegevens Bescherming’ (AVG) or GDPR | Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 regarding the protection of natural persons in connection with the processing of personal data and regarding the free traffic of those data, in replacement of Guideline 95/46/EC. |
| b) | Data Subject                                              | An identified or identifiable natural person (article 4 sub 1 AVG/GDPR).                                                                                                                                                                                                |

c)	Third party	A third party as intended in article 4 sub 10 AVG/GDPR.
d)	Data Protection Officer	An official as intended in article 37 ff. AVG/GDPR.
e)	Incident	<p>A complaint or request (for information) of a Data subject regarding the processing of Personal data by Processor;</p> <p>i An investigation or seizure by government officials of the Personal data or a suspicion that this will take place;</p> <p>ii A breach in connection with Personal data as intended in article 4 under 12 AVG/GDPR;</p> <p>iii Any unauthorised access, removal, maiming, loss or any other form of illegitimate processing of the Personal data.</p>
f)	Collaborator	The natural person engaged by Parties for the implementation of this Processor agreement who works at or for one of the Parties.
g)	Agreement(s)	The agreement(s) indicated in Appendix regarding the supply of products and/or services.
h)	Party	Data controller or Processor.
i)	Parties	Data controller and Processor.
j)	Personal data	All information on an identified or identifiable natural person in the sense of article 4 under 1 AVG/GDPR.
k)	Sub-processor	Every non-subordinate third party which is involved by Processor in the processing of Personal data in the context of the Agreement, not being Collaborators.
l)	Processor	The processor as intended in article 4 sub

- |                                                                                               |                                                                                                                   |
|-----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| m) Processor agreement                                                                        | The underlying agreement.                                                                                         |
| n) Data controller                                                                            | The data controller as intended in article 4 sub 7 AVG/GDPR                                                       |
| o) 'Wet bescherming<br>Persoonsgegevens' (Wbp),<br>Netherlands data protection<br>legislation | Law of 6 July 2000, comprising rules regarding the protection of personal data (Wbp), including later amendments. |

- 1.2. The aforementioned and other concepts are interpreted in accordance with AVG/GDPR. Until 25 May 2018, concepts are interpreted in accordance with the comparable provision from Wbp.
- 1.3. Wherever reference is made in this Processor agreement to certain standards (such as NEN7510) always intended is its most recent version. To the extent the relevant standard is no longer maintained, in its stead must be read the most recent version of the logical successor of the standard in case.
- 1.4. Any possible deviations from the text are only effective to the extent they have been specified in appendix 4. What is stipulated in appendix 4 prevails over what is otherwise stipulated in this processor agreement.

## **Article 2. Object of this Processor agreement**

- 2.1. This Processor agreement regards the processing of Personal data by Processor by order of the Data controller in the context of the implementation of the Agreement(s).
- 2.2. Parties conclude the Agreement(s) to use the expertise which Processor has in the matter of the processing and protecting of Personal data, for the purposes resulting from the Agreement(s) which are further described in this Processor agreement. Processor guarantees that he is qualified to that effect.
- 2.3. This Processor agreement is an integral part of the Agreement(s). To the extent what is stipulated in this Processor agreement is in conflict with the provisions in the Agreement(s), what is stipulated in the Processor agreement prevails.

## **Article 3. Implementation processing**

- 3.1. Processor guarantees that he will exclusively process personal data for Data controller to the extent:
  - a.) this is necessary for the implementation of the Agreement (within the context as specified in Appendix 1); or
  - b.) Data controller has given further instructions to that effect;
- 3.2. In the context of what is stipulated in the first section of article 3 under a) Processor will exclusively process the Personal data specified in Appendix 1 in the context of the nature and purposes of the processing described in that appendix.
- 3.3. Processor will follow all reasonable instructions of Data controller in connection with the processing of the Personal data. Processor immediately informs Data controller if in his opinion instructions violate the applicable legislation regarding the processing of Personal data.

- 3.4. Without prejudice to what is stipulated in the first section of this article 3, it is permitted to Processor to process Personal data if a legal requirement (also including court or administrative orders based on it) obliges him to process. In that case, the Processor informs Data controller prior to the processing of the intended processing and the legal requirement, unless that legislation prohibits this notification on weighty grounds of public interest. Processor will enable Data controller, wherever possible, to defend themselves against this mandatory processing and will also otherwise limit the mandatory processing to what is strictly necessary.
- 3.5. Processor will process the Personal data demonstrably in an adequate and diligent manner, and in accordance with the obligations he is subject to as a Processor pursuant to AVG/GDPR, to the extent still applicable Wbp, and other legislation and regulations. In that context, Processor will at least maintain a register of processing as intended in article 30 AVG/GDPR and provide Data controller upon first request with a copy of that register.
- 3.6. If the provision of services by Processor implies the processing of health-related data or other special Personal data, Processor guarantees that he will not act in violation of health-related legislation.
- 3.7. Processor will not, unless he has obtained emphatic prior written permission from Data controller, process Personal data nor have it processed either by himself or by third parties located outside the European Economic Area (“EEA”).
- 3.8. Processor assures that the involved Collaborators have signed a non-disclosure agreement and on request lets Data controller peruse this non-disclosure agreement.

#### **Article 4. Protection Personal data and control**

- 4.1. Processor will demonstrably take appropriate and effective technical and organisational security measures which, in view of the current state of the art and the associated costs, correspond with the nature (as specified in Appendix 1) of the Personal data to be processed, to protect the Personal data against loss, unauthorised cognisance, maiming or any form of illegitimate processing, as well as to guarantee the (temporary) availability of the data. Included in these security measures are such measures as may have been stipulated in the Agreement. The measures comprise in any case:
  - a.) measures to assure that only authorised Collaborators have access to the Personal data for the purposes which have been explained;
  - b.) measures whereby the Processor exclusively grants his Collaborators and Sub-processors access to Personal data by way of accounts made out to name, whereby the usage of those accounts is adequately logged and whereby the relevant accounts only give access to those Personal data the access to which is necessary for the relevant (legal) persons;
  - c.) measures to protect the Personal data against inadvertent or illegitimate destruction, inadvertent loss or modification, unauthorised or illegitimate storage, processing, access or disclosure;
  - d.) measures to identify weak spots regarding the processing of Personal data in the systems which are deployed for the provision of services to Data controller;
  - e.) measures to guarantee the timely availability of the Personal data;
  - f.) measures to assure that Personal data are processed in a logically separate manner from the Personal data which he processes for himself or on behalf of third parties;
  - g.) the other measures which Parties have agreed on as established in Appendix 2.

- 4.2. Processor demonstrably works in accordance with ISO27001 and/or NEN 7510 and has implemented an appropriate, written security policy for the processing of Personal data, in which the measures mentioned in the first section of this article 4 have at least been stipulated.
- 4.3. Processor is demonstrably compliant with the security measures for network connections as described in NEN7512.
- 4.4. Processor is demonstrably compliant with the requirements regarding logging as described in NEN7513.
- 4.5. Processor is demonstrably compliant with the requirements of other NEN-standards, to the extent they have been declared applicable to healthcare.
- 4.6. Upon first request of Data controller, Processor will present a valid certificate issued by an independent third party with expertise in the matter, if he has such at his disposal, which evinces that Processor is compliant with the obligations from this article.
- 4.7. Data controller has the right to (let) monitor compliance with the measures mentioned in the preceding under article 4.1 through 4.4. If Data controller so requests, Processor enables the former at least once a year to (let) control matters at a time to be further established by Parties through mutual agreement, and additionally in the event Data controller sees grounds for doing so in connection with (suspicion of) information or privacy-incidents. Processor will provide all reasonable assistance for such an investigation. Processor will follow any possible instructions issued reasonably by Data controller in connection with such an investigation, regarding the modification of the security policy, within a reasonable term.
- 4.8. Parties acknowledge that security requirements change constantly and that an effective security requires frequent evaluation and regular improvement of obsolete security measures. Processor will therefore evaluate the measures as they have been implemented pursuant to this article 4 periodically and, where necessary, improve the measures to remain compliant with the obligations pursuant to this article 4. The preceding leaves unaffected the instruction authorisation of Data controller to (let) take additional measures wherever necessary.

#### **Article 5. Monitoring, information obligations, and incident management**

- 5.1. Processor will monitor actively for breaches of the security measures and report on the results of the monitoring in accordance with this article 5 to Data controller.
- 5.2. As soon as an Incident occurs, has occurred or may occur, Processor is obligated to immediately inform Data controller accordingly and thereby to provide all relevant information about:
  - 1) the nature of the Incident;
  - 2) the Personal data which are (possibly) affected;
  - 3) the identified and the probable consequences of the Incident; and
  - 4) the measures which have been or will be taken to resolve the Incident or alternatively to limit the consequences/damage as much as possible.
- 5.3. Processor is obligated, without prejudice to the other obligations from this article, to take measures which can reasonably be expected of him to resolve the Incident as soon as possible or otherwise to limit further consequences as much as possible. Without any delay, Processor enters into consultation with Data controller so as to make further arrangements concerning.
- 5.4. Processor will give Data controller assistance at all times and will follow the instructions of Data controller and enables Data controller to conduct an adequate investigation of

- the Incident, formulate a correct response and take appropriate follow-up steps with regard to the Incident, also including informing the monitoring authority 'Autoriteit Persoonsgegevens' (AP) and/or the Data subject, as stipulated in article 5.8.
- 5.5. Processor will have available at all times written procedures which enable him to provide Data controller with an immediate response regarding an Incident, and to effectively cooperate with Data controller to settle the Incident. Processor will provide Data controller with a copy of such procedures if Data controller so requests.
  - 5.6. Reports made pursuant to article 5.2 are immediately directed at Data controller or, if relevant, to Collaborators of Data controller indicated by the latter during the effective time of this Processor agreement in writing. If Data controller has appointed a Data Protection Officer (DPO), the reports are directed at this DPO.
  - 5.7. It is not permitted to Processor to provide information about Incidents to data subjects or other third parties, barring to the extent that Processor is legally obliged to do so or if Parties have established otherwise.
  - 5.8. If and to the extent Parties have established that Processor maintains direct contact with the authorities or other third parties with regard to an Incident, then Processor will constantly keep the Data controller informed.

#### **Article 6. Assistance obligations**

- 6.1. AVG/GDPR and other (privacy) legislation attributes certain rights to the Data Subject. Processor will offer his full and timely assistance to Data controller for compliance with the obligations which Data controller is subject to pursuant to these rights.
- 6.2. A complaint received by Processor or a request of Data subject with regard to the processing of Personal data is forwarded by Processor without delay to Data controller.
- 6.3. Upon the first request to that effect of Data controller, Processor will provide Data controller with all relevant information regarding the aspects of the aspects of the processing of Personal data conducted by him, so that Data controller, also by way of that information, can prove that they are compliant with the applicable (privacy) legislation.
- 6.4. Processor will furthermore, upon first request of Data controller provide all necessary assistance for compliance with the legal obligations to which Data controller is subject pursuant to the applicable privacy legislation (such as the conducting of a privacy impact assessment).

#### **Article 7. Deployment of sub-processors**

- 7.1. Processor will not outsource his activities which consist of the processing of Personal data or the requiring of the processing of Personal data to a Sub-processor without the prior written consent of Data controller. The preceding is not applicable to the Sub-processors indicated in Appendix 1.
- 7.2. To the extent Data controller agrees with the deployment of a Sub-processor, Processor will impose on this Sub-processor the same or stricter obligations than those resulting for him from this Processor agreement and legislation. Processor will record these arrangements in writing and will monitor compliance with it by the Sub-processor. Upon request, Processor will provide Data controller with a copy of the agreement(s) concluded with the Sub-processor.
- 7.3. Despite the permission of Data controller for the deployment of a Sub-processor who (partially) processes data by order of the Processor, Processor remains fully liable towards Data controller for the consequences of the outsourcing of activities to a

Sub-processor. The consent of Data controller for the outsourcing of activities to a Sub-processor does not affect the fact that for the deployment of Sub-processors in a country outside the European Economic Area permission is required in accordance with article 3.7 of this Processor agreement.

#### **Article 8. Liability**

- 8.1. Parties are both responsible and liable for their own actions.
- 8.2. Any limitation of liability in the Agreement, *mutatis mutandis*, is also applicable to this Processor agreement, under the proviso that:
  - a.) Any possible (implicit or explicit) exclusions of liability for loss and/or maiming of Personal data are precluded;
  - b.) Any possible (implicit or explicit) exclusions of liability for fines imposed by AP or another monitoring agency which are directly related to an attributable shortcoming of Processor, or to an action or lack thereof attributable to Processor, are precluded.
- 8.3. Processor safeguards Data controller against and indemnifies the Data controller for all claims, actions, third-party claims, as well as fines from AP, which flow directly from an attributable shortcoming by Processor and/or his sub-contractors/Sub-processors in complying with his obligations under this Processor agreement and/or any violation by Processor and/or his sub-contractors/Sub-processors of the applicable legislation in the field of the processing of Personal data.
- 8.4. To the extent Parties are severally and jointly liable towards third parties, also including the data subject, or if a fine is imposed on them jointly by AP they are obligated towards each other, each for the part of the debt which concerns them in their mutual relationship, in accordance with what is stipulated in Volume 6, Title 1, Department 2 of the Netherlands Civil Code, 'Burgerlijk Wetboek', to contribute to the debt and the costs, unless AVG/GDPR stipulates otherwise, in which case AVG/GDPR prevails.
- 8.5. To the extent no limitation of liability for Data controller is stipulated in the Agreement, the limitation included in section 2 for Processor also applies to the Data controller.
- 8.6. Any limitation of liability furthermore comes to lapse for the relevant Party in case of intent or gross negligence on the part of the relevant Party.
- 8.7. Parties take care of sufficient coverage for the liability.

#### **Article 9. Costs**

- 9.1. The costs for the processing of data which are inherent to the normal implementation of the Agreement are supposed to be comprised in the remunerations already owed pursuant to the Agreement.
- 9.2. Any support or any other additional services which Processor must provide on grounds of this Processor agreement, or which is requested by Data controller, including all requests for additional information, will be charged to Data controller in accordance with the rates specified in Appendix 3.
- 9.3. The preceding provision is not applicable if the activities are related to a shortcoming of Processor under this Processor agreement. The activities will in that case be conducted free of charges (without prejudice to the right of Data controller to claim the damage effectively incurred from Processor).

## **Article 10. Duration and termination**

- 10.1. This Processor agreement enters into effect on the date of signing and the duration of this Processor agreement is equal to the duration of the Agreement(s) mentioned in Appendix 1, including any possible extensions thereof.
- 10.2. After its signing by both Parties, the Processor agreement is an integral and inextricable part of the Agreement(s). Termination of the Agreement(s), on whatever grounds (cancellation/rescission), results in the Processor agreement being terminated on the same grounds (and vice versa), unless Parties in such case as may occur establish otherwise.
- 10.3. Obligations which by their nature are intended to continue after termination of this processor agreement as well, remain effective after termination of the Processor agreement. Included in these provisions are, for instance, those which result from the clauses regarding non-disclosure, liability, disputes settlement, and applicable law.
- 10.4. Each of the Parties has the right, without prejudice to what is stipulated regarding in the Agreement, to suspend the implementation of this Processor agreement and the associated Agreement, or to rescind it without judicial intervention with immediate effect, if:
  - a.) the other Party is liquidated or otherwise ceases to exist;
  - b.) the other Party demonstrably falls short (gravely) in the fulfilling of the obligations which flow from this Processor agreement and this attributable shortcoming has not been corrected within 30 days following a written default notice to that effect;
  - c.) a Party has been declared bankrupt or applies for suspension of payment.
- 10.5. Considering the great dependence of Data controller on Processor, as well as the risk of continuity in the event of incidents and calamities (such as bankruptcy), Processor presently declares himself willing for such case, upon first request of Data controller, to make additional arrangements with Data controller to reduce aforementioned risks. These additional arrangements may, for example, consist of:
  - a.) the making of arrangements for the supplying periodically back or to a third party of the data processed by Processor; and/or
  - b.) the conclusion with a third party of an agreement which serves for the relevant third party severally and jointly committing itself for or lodging security for compliance with the Agreement; and/or
  - c.) the conclusion with a third party of a (tri-partite) agreement which provides for the relevant third party (constantly) acquiring control over all required information to, in such case as may occur, (start) conduct (a part of) the performances to be implemented pursuant to the Agreement – whether or not on grounds of a new agreement – instead of or parallel to Processor.
- 10.6. Processor has an exit-plan for compliance with all obligations from this Processor agreement, in case the Agreement or the Processor agreement is terminated (prematurely). Upon first request of Data controller, Processor hands over a copy of this plan.
- 10.7. Data controller has the right to rescind this Processor agreement and the Agreement with immediate effect if Processor indicates he cannot (any longer) comply with the reliability requirements which are established for the processing of Personal data pursuant to developments in legislation and/or jurisprudence.
- 10.8. Processor must inform Data controller beforehand and on time about an intended take-over or transfer of property.

10.9. It is not permitted to Processor without the emphatic and written permission of Data controller to transfer this Processor agreement and the rights and obligations which are associated with this Processor agreement to a third party.

**Article 11. Retention periods, returning and destruction of Personal data**

- 11.1. Processor does not retain the Personal data for any longer than is strictly necessary, including the statutory retention periods or any arrangement regarding retention terms as may have been concluded between Parties, as established in Appendix 1. Under no circumstance does Processor keep the Personal data for any longer than until the end of this Processor agreement. Data controller decides whether and if so for how long data must be kept.
- 11.2. Upon termination of the Processor agreement, or if applicable at the end of the established retention periods, or upon written request of Data controller, Processor will, against reasonable costs, at the discretion of Data controller, (let) destroy or return to Data controller the Personal data definitively. Upon request of Data controller, Processor provides evidence for the fact that the data have been definitively destroyed or removed. The returning of data as may occur will be in a generally customary, structured and documented data-format, through electronical channels. If the returning, definitive destruction or removal is not possible, Processor will immediately inform Data controller accordingly. In that case, Processor guarantees that he will handle the Personal data with confidentiality and will no longer process them.

**Article 12. Intellectual property rights**

- 12.1. To the extent the (collection of) Personal data is protected by any intellectual property right, Data controller grants permission to Processor to use the Personal data in the context of the implementation of this Processor agreement.

**Article 13. Final provisions**

- 13.1. The considerations are a part of this Processor agreement.
- 13.2. In case of the nullity and/or annullability of one or more provisions from this Processor agreement, the other provisions remain fully effective.
- 13.3. In all cases for which this Processor agreement does not provide, Parties decide through mutual agreement.
- 13.4. To this Processor agreement, Netherlands legislation is applicable.
- 13.5. Parties will exert themselves to resolve conflicts through mutual agreement. Included here is the possibility to terminate the dispute through mediation or arbitration established through mutual agreement.
- 13.6. Disputes about or in connection with this Processor agreement are exclusively submitted to the court or arbiter(s) indicated for this purpose in the Agreement.

## **Appendix 1 : Agreements, description Personal data, nature processing, etc.**

This Processor agreement is an appendix to the subsequent Agreements and regards the following types of processing of Personal data.

<b>Effective date contract</b>	<i>See Agreement</i>
<b>Reference/number/title contract</b>	<i>See Agreement</i>
<b>Short description services</b>	<i>Delivery of the on-line platform 'Familienet' for communications with and about clients.</i>
<b>Nature of the processing</b>	<i>All clients of the healthcare institution have a secure personal page. Here, Collaborators and family share message, pictures, videos, an agenda, and the book of life. In this way, everyone is well-informed and cooperation improves.</i>
<b>Type of Personal data</b>	<i>Names, pictures, videos, text, documents, and other messages of and about data subjects, but in principle no health-related information.</i>
<b>Categories of data subjects</b>	<i>Clients, family-members, collaborators.</i>
<b>Purposes of the processing</b>	<i>The enabling of communication between healthcare institution, client, and family.</i>
<b>Approved sub-processors</b>	<i>See appendix 4.</i>
<b>Arrangements retention periods</b>	<i>For as long as the Agreement is effective, plus a term of a maximum of 30 days after, in connection with the back-up-systems of Processor.</i>

## **Appendix 2 : Description further security measures**

More specifically, Processor also applies the following security measures:

- The use of encrypted connections (also including the HTTPS-connection of the website of the Processor);
- control of the OWASP top-10 security threats ([www.owasp.org](http://www.owasp.org)) during the Assignment and upon the development of new services;
- access to personal data by staff of Processor only if required for the execution of their tasks and under contractual non-disclosure obligation;
- the use of authorisation systems for access to the service and the Personal data;
- the adoption of appropriate processor agreements with suppliers;
- the application of alarm systems, also with a connection to security services or the police;
- the application of user-profiles with the attribution of user rights;
- the use of authorisation and authentication systems;
- the use of secured SSL/TLS-connections for transmissions;
- the application of anti-virus software;
- a strict selection of hosting providers which are compliant with NEN 7510 and ISO 27001, with which appropriate (sub-)processor agreements are concluded.

**Appendix 3 : Specific rates**

Not applicable. See Agreement.

#### Appendix 4 : Modifications to standard text

Parties emphatically establish the following deviations from the standard text of the processor agreement:

Art.	Text lapsing	Substitute text	Reason
4.2 through 4.7	The entire article sections.	Processor only deploys hosting providers which have demonstrably implemented an appropriate, written security policy, in conformity with ISO27001 and/or NEN 7510, for the processing of Personal data deriving from Processor.	Processor will in principle not process medical or health-related data with their general communication platform.
7.1	Processor will not outsource activities consisting of the processing of Personal data to nor demand that Personal data will be processed by a Sub-processor without the prior written consent of Data controller. The preceding is not applicable to the Sub-processors indicated in Appendix 1.	Processor will only outsource his activities consisting of the processing of Personal data to or require that Personal data will be processed by, a Sub-processor if the latter is established within the European Union and the latter has not signed an appropriate processor agreement with Processor.	New editors provide sufficient assurances and prevents that parties in case of changes to, for example, communication and hosting services, must first arrange for a written contract.
10.6	The entire article section.	None.	The service of Processor enables Data controller to download their own data. This renders superfluous an exit-plan.
11.2	On request of Data controller, Processor provides proof of the fact that the data have been definitively destroyed or removed. The possible returning of data will take place in a generally current, structured and documented data-format, through electronic channels.	None.	Proof of destruction (demonstrating that something is <i>not</i> present) is impossible to provide. In addition, the service of Processor enables Data controller to download the data themselves in a current format.

13.6	None.	<i>In addition:</i> If no competent court has been selected, the court of law in the district of Processor will be exclusively competent.	Solely additional clarity regarding the competent court of law.
------	-------	-------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------