Model
Processing Agreement

for the benefit of contract partners, organisations or institutions which have concluded a licence agreement with Parantion Groep B.V. for the use of the products

Version: 4.0
Date: 29/04/2022
Contact person: Bas Aalpoel
Status of the proposal: Public

Parantion Groep B.V.
PO Box 2109 | 7420 AC | Deventer
Keulenstraat 12 | 7418 ET | Deventer
+31 (0)570 – 23 45 67
www.parantion.nl

WHEREAS:

- In order to perform the Agreement/Licence, the Processor processes Personal Data on behalf of the Controller;
- In the context of the performance of the Agreement, **Parantion** is to be regarded as a Processor within the meaning of the GDPR and «NAAM_INSTELLING» as a Controller within the meaning of the GDPR;
- The Parties wish to handle the Personal Data that are or will be processed for the performance of the Agreement with care and in accordance with the GDPR and other Applicable Laws and Regulations regarding the Processing of Personal Data;
- The Parties wish to lay down in Writing in this Processing Agreement their rights and obligations regarding the Processing of Personal Data of Data Subjects in accordance with the GDPR and other Applicable Laws and Regulations regarding the Processing of Personal Data.

AND AGREE AS FOLLOWS:

ARTICLE 1. DEFINITIONS

In this Processing Agreement, capitalised terms shall have the meanings set out in this article. Wherever in this article a definition is given in the singular, it shall include the plural and vice versa, unless expressly stated otherwise or unless the context otherwise requires.

1.1 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 (General Data Protection Regulation).

1.2 Data Subject: the identified or identifiable natural person to whom the Personal Data relates, as referred to in Article 4(1) of the GDPR.

1.3 Annex: an Annex to this Processing Agreement that forms an integral part of this Processing Agreement.

1.4 Special categories of Personal Data: Personal Data revealing racial or ethnic origin, political opinions, religious or ideological beliefs or trade union membership, and genetic data, biometric data as the unique identifier of an individual, or data concerning health or data concerning a person's sexual behaviour or orientation, as referred to in Article 9 of the GDPR.

1.5 Third Party: a natural or legal person, public authority, agency or other body, other than the Data Subject, nor the Controller, nor the Processor, nor any persons who are authorised under the direct authority of the Controller or the Processor to process Personal Data, as referred to in Article 4(10) of the GDPR.

1.6 Service: the service or services to be provided by the Processor to the Controller under the Agreement.

1.7 Personal Data Breach: a breach or a suspicion of a breach of security that accidentally or illegally results in the destruction, loss, change or unlawful provision of or unlawful access to the Personal Data sent, stored or otherwise processed, as meant in Article 4(12) of the GDPR.

1.8 Employee: the employees and other persons who work under the responsibility of the Processor and who are engaged by the Processor in the performance of the Agreement.

1.9 Recipient: a natural or legal person, public authority, agency or other body, whether a Third Party or not, to whom the Personal Data are disclosed, as referred to in Article 4(9) of the GDPR.

1.10 Agreement: the agreement concluded between the Controller and the Processor pursuant to which the Processor processes Personal Data on behalf of the Controller in the performance of this agreement.

1.11 Personal Data: any information relating to a Data Subject; an identifiable person is a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical,

physiological, genetic, mental, economic, cultural or social identity of that natural person, as referred to in Article 4(1) of the GDPR.

1.12 PIA: the data protection impact assessment carried out prior to the Processing with regard to the effect of the intended processing activities on the protection of Personal Data, as referred to in Article 35 of the GDPR.

1.13 Written/in Writing: written down or by electronic means as referred to in Section 6:227a of the Dutch Civil Code.

1.14 Sub-processor: another processor, including but not limited to group companies, affiliates, subsidiaries and auxiliary suppliers, engaged by the Processor to perform specific processing activities on behalf of the Processor.

1.15 Applicable Laws and Regulations regarding the Processing of Personal Data: the applicable laws and regulations and/or treaties or further treaties, regulations, directives, decisions, policy rules, instructions and/or recommendations of a competent governmental authority regarding the Processing of Personal Data, also including any future amendment and/or supplementation thereof, including national laws implementing the GDPR and the Telecommunications Act.

1.16 Supervisory Authority: one or more independent public authorities responsible for monitoring the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to the Processing of their Personal Data and to facilitate the free flow of Personal Data within the European Union, as referred to in Article 4(21) and Article 51 of the GDPR. In the Netherlands, this is the Personal Data Authority.

1.17 Processing Agreement: the present agreement including Annexes, as referred to in Article 28(3) of the GDPR.

1.18 Processing: an operation or a set of operations relating to Personal Data or a set of Personal Data, executed in automated procedures or otherwise, such as the collection, recording, ordering, structuring, storage, adjustment or amendment, retrieval, consultation, use, provision by means of transmission, dissemination or otherwise making available, aligning, or combining, shielding, deletion or destruction of data as meant in Article 4(2) of the GDPR.

ARTICLE 2. SUBJECT OF THE PROCESSING AGREEMENT

2.1 The Processing Agreement supplements the Agreement and replaces any agreements made previously between the Parties concerning the Processing of Personal Data. In the event of a conflict between the provisions regarding the Processing of Personal Data in the Processing Agreement and the Agreement, the provisions of the Processing Agreement shall prevail.

2.2 The provisions of the Processing Agreement shall apply to all Processing that takes place in the performance of the Agreement. The Processor will inform the Controller within five working days if the Processor has reason to believe that the Processor can no longer comply with the Processing Agreement. The Parties shall then enter into consultation with a view to finding a solution to the situation that has arisen.

2.3 The Controller shall instruct the Processor to process the Personal Data on behalf of the Controller. The instructions of the Controller are further described in the Processing Agreement and the Agreement. The Controller may reasonably give additional or different instructions in Writing. If, in the opinion of the Processor, the additional or different instructions have consequences for the service to be provided, the Processor may terminate the Agreement without being liable for compensation to the Controller.

2.4 The Processor shall process the Personal Data only on the instructions of the Controller and under the responsibility of Controller. The Processor shall only process the Personal Data to the extent that the Processing is necessary for the performance of the Agreement; never for its own benefit, for the benefit of Third Parties and/or for advertising or other purposes, unless a provision of Union or Member State law applicable to Processor obliges the Processor to Process. In this case, the Processor shall inform the Controller in Writing of this provision prior to the Processing, unless that legislation prohibits such notification on important public interest grounds.

2.5 The Processor and the Controller shall comply with the GDPR and other Applicable Laws and Regulations regarding the Processing of Personal Data. The Processor shall notify the Controller as soon as possible, but no later than within 5 working days, if, in the opinion of the Processor, an instruction given by the Controller breaches the GDPR and/or other Applicable Laws and Regulations regarding the Processing of Personal Data.

2.6 The Controller shall provide the Processor with the Personal Data necessary for the performance of its tasks. The Controller warrants that it will provide Processor only with Personal Data that is necessary for the tasks and may be provided by the Controller for that purpose by virtue of express consent. The Controller shall indemnify and hold the Processor harmless against claims from third parties/data subjects on account of unlawful processing or processing in breach of the privacy legislation.

2.7 If the Processor determines the purpose and means of the Processing of Personal Data in violation of the Processing Agreement and/or the GDPR and/or other Applicable Laws and Regulations regarding the Processing of Personal Data, the Processor will be regarded as the Controller for those Processing Operations.

ARTICLE 3. PROCESSING OF PERSONAL DATA

3.1 Prior to entering into the Processing Agreement, the Processor will inform the Controller in Annex A completely and truthfully about the Processing Operations that the Processor carries out in the performance of the Agreement, unless Annex A states that the Processor will include the relevant information in this Annex. The Processor is only authorised to perform the Processing Operations specified in Annex A.

ARTICLE 4. PROVIDING ASSISTANCE AND COOPERATION

4.1 The Processor shall provide all reasonable assistance and cooperation to the Controller in the fulfilment of the Parties' obligations pursuant to the GDPR and other Applicable Laws and Regulations regarding the Processing of Personal Data. The Processor may charge any costs incurred in providing assistance to the Controller. In any event, the Processor shall provide the Controller with assistance in relation to:

(i) The security of Personal Data at the Processor's premises;
(ii) Performing checks and audits;
(iii) Performing PIAs;
(iv) Prior consultation of the Supervisory Authority;
(v) Responding to requests from the Supervisory Authority or any other government body;
(vi) Complying with requests from Data Subjects;
(vii) Reporting Personal Data Breaches.

4.2 Provision of assistance and cooperation in relation to complying with requests from Data Subjects includes at least the following obligations for the Processor:

4.2.1 The Processor shall take all reasonable steps to ensure that the Data Subject can exercise his rights.

4.2.2 If a Data Subject contacts the Processor directly regarding the exercise of his rights, the Processor will not respond (in detail) to this - unless explicitly instructed otherwise by the Controller - but will notify the Controller as soon as possible, but no later than within 5 working days, with a request for further instructions.

4.2.3 If the Processor offers the Service directly to the Data Subject, the Processor is obliged to inform the Data Subject on behalf of the Controller of the Processing of the Data Subject's Personal Data in a manner that is in accordance with the Data Subject's rights.

4.3 Provision of assistance and cooperation in relation to complying with requests from the Supervisory Authority or another government body includes at least the following obligations for the Processor:

4.3.1 If Processor receives a request or order from a Dutch and/or foreign government body regarding Personal Data, including but not limited to a request from the Supervisory Authority, the Processor shall inform the Controller as soon as possible but no later than within five working days insofar as this is permitted by law. When handling the request or order, the Processor shall comply with all reasonable instructions of the Controller and shall provide the Controller with all reasonably necessary

cooperation. The Controller will indemnify and hold the Processor harmless against any claims, demands and penalties that the Processor is faced with as a result of the instructions given by the Controller.

4.3.2 If the Processor is legally prohibited from fulfilling its obligations under Article 4.3.1, the Processor shall represent the reasonable interests of the Controller. These will include in any case:

4.3.2.1 If this is necessary in the opinion of the Processor, the Processor shall legally review the extent to which: (i) the Processor is legally obliged to comply with the request or order; and (ii) the Processor is effectively prohibited from fulfilling its obligations to the Controller under Article 4.3.1.

4.3.2.2 The Processor will only comply with the request or order if the Processor is legally obliged to do so and, where possible, the Processor will object (in court) to the request or order or the prohibition to inform the Controller about it or to follow the Controller's instructions.

4.3.2.3 The Processor shall not provide more Personal Data than strictly necessary to comply with the request or order.

4.3.2.4 If there is a transfer within the meaning of Article 9, the Processor shall investigate the possibilities of complying with Articles 44 up to and including 46 of the GDPR.

4.4 If it is desirable for the purpose of ascertaining the cause of or resolving a Personal Data Breach or a reasonable suspicion of a Personal Data Breach, to obtain knowledge from the Controller, the latter shall also provide all cooperation and assistance to the Processor.

ARTICLE 5. ACCESS TO PERSONAL DATA

5.1 The Processor shall limit access to Personal Data to Employees, Sub-processors, Third Parties and other Recipients of Personal Data to a necessary minimum.

5.2 The Processor shall provide access to Personal Data only to those Employees who need such access for the performance of the Agreement. The categories of Employees are specified in Annex A.

5.3 The Processor shall not give Sub-processors access to Personal Data without the prior general or specific Written consent of the Controller. General Written consent to the engagement of Sub-processors is only given if this is explicitly included in Annex A. Specific authorisation to engage Sub-processors is only granted to Sub-processors specified in Annex A.

5.4 In the case of general Written consent to the use of Sub-processors, the Processor shall inform the Controller in Writing no later than three (3) months prior to any intended changes regarding the addition, replacement or change of a Sub-processor or Sub-processors, giving the Controller the opportunity to object to these changes. The Parties will enter into negotiations about this.

5.5. The general or specific consent of the Controller to engage Sub-processors shall not affect the obligations of the Processor arising from the Processing Agreement, including but not limited to Article 9. The Controller may withdraw its general or specific Written consent to the engagement of Sub-processors if the Processor does not comply or no longer complies with the obligations of the Processing Agreement, the GDPR and/or other Applicable Laws and Regulations regarding the Processing of Personal Data. When the Processor is no longer able to provide its services due to the withdrawal of consent, this constitutes a ground for the Processor to terminate the Agreement. The Processor shall not be liable for compensation in such a case. However, the Controller is obliged to fulfil the payment obligations until the end of the Agreement.

5.6 Should the Controller so demand, the Processor shall provide the Controller with an overview of the Sub-processors engaged by the Processor.

5.7 The Processor shall impose the obligations set out in the Processing Agreement on the persons or legal persons engaged by the Processor, including but not limited to Employees and/or Sub-processors. The Processor shall ensure that the persons or legal persons engaged by the Processor including, but not limited to Employees and/or Sub-processors, comply with the obligations set out in the Processor Agreement by means of a Written agreement.

5.8 The Processor shall inform the Controller without delay if the Processor and/or any persons or legal persons engaged by the Processor, including but not limited to Employees and/or Sub-processors, act in breach of the Processing Agreement and/or the Written agreement concluded with the Processor as referred to in Article 5.7.

5.9 The Processor remains fully responsible and fully liable to the Controller for the fulfilment of the obligations by the Sub-processors engaged by the Processor arising from the Agreement and the Processing Agreement.

ARTICLE 6. SECURITY

6.1 The Processor shall take appropriate technical and organisational measures to ensure a risk-appropriate security level, so that the Processing fulfils the requirements of the GDPR and other Applicable Laws and Regulations concerning the Processing of Personal Data and the protection of the rights of Data Subjects is guaranteed. To this end, the Processor shall at least implement the technical and organisational measures set out in Annex B. The Controller is familiar with the security policy and processing policy of the Processor and is of the opinion that this policy is in accordance with the privacy legislation.

6.2 When assessing the appropriate level of security, the Processor shall take into account the state of the art, the costs of implementation, as well as the nature, scope, context and purposes of the processing, and the risks to the rights and freedoms of persons that vary in terms of probability and seriousness, in particular due to the destruction, loss, alteration or unauthorised disclosure of or access to data transmitted, stored or otherwise processed, whether accidental or unlawful.

6.3 The Processor shall record its security policy in Writing. At the Controller's request, the Processor will allow it to inspect the Processor's security policy at the Processor's offices.

6.4 Adherence to an approved code of conduct as referred to in Article 40 of the GDPR or to an approved certification mechanism as referred to in Article 42 of the GDPR may be used as an element to demonstrate compliance with the requirements referred to in this Article.

ARTICLE 7. AUDIT

7.1 The Controller is entitled to have audits carried out by an independent third party bound by confidentiality to verify compliance with all the points in this Agreement. The audit shall in principle take place no more than once a year. The Controller shall inform the Processor in writing of this intention 14 days before the audit is to be carried out.

7.2 The Processor shall cooperate with the audit and shall make all reasonably relevant information, including supporting data such as system logs, and employees available at the earliest opportunity and within a reasonable time, unless an urgent interest opposes this.

7.3 The findings of the audit will be assessed by the Parties in mutual consultation and, as a result, may or may not be implemented by one or both Parties jointly.

7.4 The Processor is entitled to engage an independent, external expert to conduct an audit of the Processor's organisation in order to demonstrate that the Processor complies with the provisions of the Agreement, the Processing Agreement, the GDPR and other Applicable Laws and Regulations concerning the Processing of Personal Data.

7.5 At the request of the Controller, the Processor shall provide the findings of the independent, external expert referred to in Article 7.4 in the form of a statement in which the expert expresses an opinion on the quality of the technical and organisational security measures taken by the Processor in relation to the Processing Activities carried out by the Processor for the Controller. Required documents are available for inspection at the offices of Processor.

7.6 The costs of the audit as referred to in Article 7.1 shall be borne by the Controller. The costs of the Processor's personnel supervising the audit are excluded from this and shall be borne by the Processor.

7.7 If it is established during an audit that the Processor does not comply with the provisions in the Agreement and/or the Processing Agreement and/or the GDPR and/or other Applicable Laws and Regulations regarding the Processing of Personal Data, the Processor shall immediately take all measures reasonably necessary to ensure that the Processor complies therewith. The cost involved will be for the Processor's account.

ARTICLE 8. PERSONAL DATA BREACH

8.1 The Processor shall inform the Controller without unreasonable delay and no later than within 72 hours of becoming aware of a Personal Data Breach or a reasonable suspicion of a Personal Data Breach. The Processor will inform the Controller via the contact person and contact details of the Controller as set out in Annex A and at least regarding what is set out in Annex C. The Processor shall make every effort to ensure that the information provided is complete, correct and accurate.

8.2 If and to the extent that it is not possible for the Processor to provide all the information in Annex C simultaneously, the information may be provided to the Controller in stages without unreasonable delay.

8.3 The Processor has implemented adequate policies and procedures to detect Personal Data Breaches at the earliest possible stage, inform the Controller thereof within no more than 72 hours, respond to them adequately and promptly, prevent or limit (further) unauthorised access, modification, and disclosure or otherwise unlawful Processing, and prevent any recurrence of a Breach. At the request of the Controller, the Processor shall provide information about this policy and these procedures implemented by the Processor and allow for its inspection.

8.4 The Processor shall keep a Written register of all Personal Data Breaches relating to or in connection with the Agreement or the performance of the Agreement, including the facts concerning the Personal Data Breach, its consequences and the corrective measures taken. At the request of the Controller, the Processor shall provide a copy of this register to the Controller.

ARTICLE 9. TRANSFER OF PERSONAL DATA

9.1 Personal Data may only be transferred to third countries or international organisations if there is an appropriate level of protection and the Controller has granted specific Written consent to this. This specific Written consent is only granted if included in Annex A. The Processor shall only be authorised to make such transfers to third countries or international organisations as are specified in Annex A, unless a provision in Union or national law applicable to the Processor obliges the Processor to process. In this case, the Processor shall inform the Controller in Writing of this provision prior to the Processing, unless that legislation prohibits such notification on important public interest grounds.

9.2 The Controller may attach further conditions to the Written consent referred to in Article 9.1 including, but not limited to demonstrating that the requirements set out in Article 9.3 have been met. When the Processor is no longer able to provide its services due to the conditions set, this constitutes a ground for the Processor to terminate the Agreement. The Processor shall not be liable for compensation in such a case. However, the Controller is obliged to fulfil the payment obligations until the end of the Agreement.

9.3 The Controller may only permit the Processor to transfer Personal Data to third countries or international organisations if:

(i) An adequacy decision in accordance with Article 45(3) GDPR has been taken in respect of the third country or international organisation concerned; or

(ii) Appropriate safeguards in accordance with Article 46 of the GDPR, including binding rules as referred to in Article 47 of the GDPR, have been put in place in respect of the third country or international organisation concerned; or

(iii) One of the specific conditions of Article 49(1) of the GDPR is met in respect of the third country or international organisation concerned.

ARTICLE 10. CONFIDENTIALITY OF PERSONAL DATA

10.1 All Personal Data shall be classified as confidential data and shall be treated as such.

10.2 The Parties shall keep all Personal Data confidential and shall not disclose them in any way whatsoever, either internally or externally, except insofar as:

(i) Disclosure of the Personal Data is necessary in the context of performing the Agreement or Processor Agreement;

(ii) Any mandatory statutory provision or court order obliges the Parties to disclose such Personal Data, in which case the Parties will first notify the other Party of this;

(iii) Disclosure of such Personal Data requires the prior Written consent of the other Party.

10.3 A breach of Articles 10.1 and/or 10.2 will be considered a Personal Data Breach.

ARTICLE 11. LIABILITY AND INDEMNITY

11.1 The Processor shall only be liable to the Controller for direct damage arising from or related to an imputable failure of the Processor to fulfil its obligation under this Agreement. Direct damage exclusively means:
a) The reasonable costs incurred by the Controller to have Processor's performance fulfil the agreement. However, this damage will not be compensated if the Controller has terminated the agreement. Such costs do not include upgrading the Controller's hardware or software.
c) Reasonable costs for establishing the cause and extent of the damage, insofar as that finding relates to direct damage within the meaning of this Agreement.
d) Reasonable costs incurred to prevent or limit damage, to the extent that the Controller demonstrates that these costs have resulted in limitation of the direct damage within the meaning of this Agreement.
Direct damage explicitly does not include the penalty or incremental penalty payment imposed by the Authority. The liability is capped at the amount paid out by the Processor's insurance. If no payment is made despite the Processor's best efforts, liability is capped at EUR 15,000.

11.2 In the event that the Controller is itself the perpetrator of a breach of the abovementioned law or regulation, all costs and damage shall be recovered from the Controller.

11.3 The Processor shall ensure adequate liability coverage by means of a liability insurance. At the Processor's request, the Processor will allow the Controller to inspect this liability insurance policy of the Processor.

ARTICLE 12. CHANGES

12.1 The Processor is obliged to inform the Controller immediately of any intended changes to the Service, the performance of the Agreement and the performance of the Processing Agreement that relate to the Processing of Personal Data. These will include in any case:

(i) Changes that affect or may affect the Personal Data or the categories of Personal Data to be processed;

(ii) Changes to the means by which the Personal Data is processed;

(iii) Engaging other Sub-processors;

(iv) Changes in the transfer of Personal Data to third countries and/or international organisations.

12.2 If a change relating to the Processing of Personal Data or an audit gives cause to do so, the Parties will immediately consult on amending the Processing Agreement at the Controller’s request. If the Processor is no longer able to provide its services due to the change, this constitutes a ground for the Processor to terminate the Agreement. The Processor shall not be liable for compensation in such a case. However, the Controller is obliged to fulfil the payment obligations until the end of the Agreement.

12.3 The Processor is authorised to implement a change in the Service, a change in the performance of the Agreement, a change in the performance of the Processing Agreement and/or a change that results in the amendment of Annex A only if the Controller has given its prior Written consent to this change or these changes. If the Processor is no longer able to provide its services due to the withholding of consent, this constitutes a ground for the Processor to terminate the Agreement. The Processor shall not be liable for compensation in such a case. However, the Controller is obliged to fulfil the payment obligations until the end of the Agreement.

12.4 Changes relating to the Processing of Personal Data may never result in the Controller being unable to comply with the GDPR and/or other Applicable Laws and Regulations relating to the Processing of Personal Data.

12.5 In the event of nullity or voidability of one or more provisions of the Processing Agreement, the other provisions will remain in full force.

ARTICLE 13. DURATION AND TERMINATION

13.1 The duration of the Processing Agreement is identical to the duration of the Agreement. The Processing Agreement cannot be terminated separately from the Agreement. Upon termination of the Agreement, the Processing Agreement will end by operation of law and vice versa.

13.2 The Controller is entitled to terminate the Processing Agreement if the Processor does not or can no longer comply with the Processing Agreement and/or the GDPR and/or other Applicable Laws and Regulations regarding the Processing of Personal Data, without Processor being entitled to any compensation. When giving notice of termination, the Controller will observe a reasonable six-month notice period, unless the circumstances justify immediate termination. In any event, the Controller will be obliged at all times to first give the Processor notice of default and allow a reasonable period of time to remedy any defects.

13.3 Within one year of the termination of the Agreement, the Processor shall destroy and/or return all Personal Data and/or transfer them to the Controller and/or another party designated by the Controller at the Controller's discretion. All existing (other) copies of Personal Data, whether or not held by any persons or legal persons engaged by the Processor including, but not limited to Employees and/or Sub-processors, are hereby demonstrably permanently deleted, unless storage of the Personal Data is required by Union or Member State law.

13.4 At the request of the Controller the Processor shall confirm in Writing that the Processor has fulfilled all obligations set out in Article 13.3.

13.5 The Processor shall bear the costs of destruction, return and/or transfer of the Personal Data. The Controller may set further requirements for the manner of destruction, return and/or transfer of the Personal Data, including requirements for the file format. Any costs will be reasonably charged on to the Controller if specific requirements are set in addition to the standard solution provided by the Processor.

13.6 Obligations from the Processing Agreement that by their nature are intended to continue after termination of the Processing Agreement will remain in force after termination.

ARTICLE 14. APPLICABLE LAW AND DISPUTE RESOLUTION

14.1 The Processing Agreement and its performance are governed by Dutch law.

14.2 All disputes that arise between the Parties in connection with the Processing Agreement shall be brought before the competent court in the city where the Processor has its registered office.

Annex A: Specification of the Processing of Personal Data

Version number 01, Date of last update: 2/5/2018

Description of the Processing
Processing of data for the purpose of development of employees, students, users pupils and other natural persons using the system Personal data for the purpose of proper administration in the system Collecting data for research purposes and quality improvement

Purposes of the Processing
Improving quality and providing insight into development

Categories of Data Subjects (*to be completed by the Controller*)
Employees, students, teachers, quality assurance staff, specialists, respondents. People who use the system within the organisation

(Categories of) Personal Data (*to be completed by the Controller*)
- Personal data, such as name and address, email address, etc. - Administrative data, such as login times, logout times, etc. - Data related to the use and purpose of the system, such as content fields necessary for the development and research of and about students, users, pupils and other natural persons. The controller itself is able to create data fields and items in which it determines which data is to be entered. This is outside the control of the processor. The Controller is therefore fully responsible for the input of this data and guarantees the Processor that it only processes Personal Data to which it is entitled under the agreement.

Retention period of the Personal Data or the criteria for determining it (*complete only if applicable)* (*to be completed by the Controller*)
The Processor shall delete the personal data after termination of the contract as a matter of course. After two months, the data is also removed from the backup.

Categories of Employees

Categories of Processor's Employees (job roles/job categories) who Process Personal Data	(Category of) Personal Data processed by Employees	Type of Processing	Country of Processing
- Support staff: have access to personal data and process it at the request of the controller	Name and address and depending on the content that the Controller has entered in the tool	CRUD	NL
- Sales staff: have access to the personal data of specific customers	Name and address and depending on the content that the Controller has entered in the tool	CRUD	NL
- Development staff: have access to personal data but will not process it, they have access to the personal data for the purposes of developing the software	Name and address and depending on the content that the Controller has entered in the tool	CRUD	NL
Parantion can grant specific rights to individual employees regarding inspection and processing of personal data			

Sub-processors

□ General consent given to the engagement of Sub-processors.

■ Specific consent to the use of the following Sub-processors (*to be completed by the Controller*):

Sub-processor engaged by Processor to Process Personal Data	(Category of) Personal Data processed by Sub-processor	Type of Processing	Country of Processing	Country of establishment of Sub-processor
Fundaments	Same data as Parantion	Management of private cloud environment	NL	NL
Previder	Same data as Parantion	Data centre	NL	NL

Transfers

The Controller has given the Processor specific consent to the transfers to third countries or international organisations listed below (*to be completed by Controller*).

Description of transfer	Entity transmitting the Personal Data + country	Entity receiving the Personal Data + country	Transfer mechanism
n/a			

Contact details

General contact details	Name	Position	Email address	Phone number
Processor	Parantion	Product manager	sales@parantion.nl	0570234567

Contact details Personal Data Breach	Name	Position	Email address	Phone number
Processor	Bas Aalpoel	Director	security@parantion.nl	0570234567

Annex B: Security measures

Version number 01, Date of last update: 02/05/2018

Effects of security measures taken by Processor:

In accordance with ISO:27001 and NEN:751 standards

Certificates held by Processor:

Certificates	Organisational unit/service to which certificate relates	Certification validity period	Statement of Applicability
ISO27001	Entire organisation	6 October 2022	Yes
NEN7510	Entire organisation	6 October 2020	Yes

Qualifications met by Processor:

n/a

Annex C: Information to be provided in the event of a Personal Data Breach

Version number XX, Date of last update: XX-XX-XX

Contact details of reporter

Name, position, email address, telephone number.

Data relating to the Personal Data Breach (hereinafter: 'Breach')

- Give an outline of the incident in which the Personal Data breach occurred.
- How many individuals' Personal Data are involved in the Breach?
  (Please fill in the numbers)

  a) At least: (complete)

  At most: (complete)
- Describe the group of people whose Personal Data are affected (Categories of Data Subjects) by the Breach.
- When did the breach take place?
  (Choose one of the following options and complete as necessary)

  a) On (date)

  b) Between (start date of period) and (end date of period)

  c) Not yet known
- What is the nature of the Breach?
  (You can tick more than one option)

  a) Reading (confidentiality)

  b) Copying

  c) Changing (integrity)

  d) Deletion or destruction (availability)

  e) Theft

  f) Not yet known
- What type of Personal Data is involved?
  (You can tick more than one option)

  a) Name and address

  b) Phone numbers

  c) Email addresses or other addresses for electronic communication

  d) Access or identification data (e.g. login name/password or customer number)

  e) Financial data (e.g. account number, credit card number)

  f) BSN or tax and social insurance number

  g) Passport copies or copies of other identification documents

  h) Gender, date of birth and/or age

  i) Special categories of Personal Data revealing racial or ethnic origin, political opinions, religious or ideological beliefs or trade union membership, and genetic data, biometric data

as the unique identifier of an individual, or data concerning health or data concerning a person's sexual behaviour or orientation

j) Other information, i.e. (please complete)

- What consequences may the Breach have for the privacy of the Data Subjects?
  (You can tick more than one option)

  a) Stigmatisation or exclusion

  b) Damage to health

  c) Exposure to (identity) fraud

  d) Exposure to spam or phishing

  e) Other, i.e. (please complete)

Follow-up actions to the Personal Data Breach

- What technical and organisational measures has your organisation taken to address the breach and prevent further breaches?

Technical protection measures

- Is the Personal Data encrypted, hashed or otherwise made unintelligible or inaccessible to unauthorised persons?
  (Choose one of the following options and complete as necessary)

  a) Yes

  b) No

  c) Partly, namely: (complete)

- If the Personal Data has been made wholly or partly unintelligible or inaccessible, how was this done?
  (Answer this question if you chose option a or option c at the previous question. If you have used encryption, please also explain the method of encryption.)

International aspects

- Does the Breach concern persons in other EU countries?
  (Choose one of the following options)

  a) Yes

  b) No

  c) Not yet known