Data Processing Agreement Dutchview

Version 2.3

Processor Agreement

Data Processing Agreement between (to be specified) Data Controller and Dutchview information technology bv.

<Organisation>, with its registered office at <address>, hereinafter to be referred to as the Data Controller, legally represented herein by <Mr or Ms>, <personal name>, <position>,

and

Dutchview information technology bv, with its registered office at Achter de Muren Zandpoort 10, 7411GE, Deventer, the Netherlands, hereinafter to be referred to as the Data Processor, duly represented herein by Mr R.B. Loenen, CEO,

declare to have concluded a Data Processing Agreement as referred to in the General Data Protection Regulation (GDPR) between the Data Controller and the Data Processor. Where this Data Processing Agreement uses terms that correspond to definitions from the GDPR, these terms shall have the meaning of the definitions from the GDPR.

Definitions

Article 1.

1.1 Appendices: appendices to this Data Processing Agreement, which are part of this Data Processing Agreement.

1.2 Supervisory Authority: the Dutch Data Protection Authority (DPA) is the independent administrative body that has been appointed by law in the Netherlands as the Supervisory Authority to supervise the processing of Personal Data.

Duration and Termination

Article 2.

2.1 This Data Processing Agreement shall take effect at the time of signature and shall continue as long as the Data Processor acts as a Data Processor of the Personal Data made available by the Data Controller.

Subject of this Data Processing Agreement

Article 3.

3.1 The Data Processor shall process the Personal Data made available by or via the Data Controller exclusively on the instructions of the Data Controller within the framework of the performance of the contract/offer of …….

The Data Processor shall not process the Personal Data for purposes other

than those for which they were collected, unless legal requirements dictate otherwise.

3.2 The Data Processor undertakes to process the Personal Data made available by or via the Data Controller within the framework of these activities with due care.

Obligations of the Data Processor

Article 4.

4.1 The Data Processor shall process data on behalf of the Data Controller in accordance with the Data Controller's instructions.

4.2 The Data Processor has no control over the Personal Data made available. The Data Processor does not take decisions about the receipt and use of the data, the provision thereof to third parties and the duration of the storage of data. The control over the Personal Data provided under this Data Processing Agreement shall never be vested in the Data Processor.

4.3 When processing Personal Data in the context of the activities referred to in Article 3, the Data Processor shall act in accordance with the applicable laws and regulations regarding the processing of Personal Data. The Data Processor shall follow all reasonable instructions of the contact person, as referred to in Article 12.2, unless legal obligations dictate otherwise.

4.4 The Data Processor shall at all times provide the Personal Data made available by the Data Controller with regard to this Data Processing Agreement at the first request of the contact person, as referred to in Article 12.2.

4.5 The Data Processor shall at all times enable the Data Controller to meet the statutory deadlines for the obligations under the GDPR, in particular the rights of Data Subjects, such as, but not limited to, a request for access, correction, addition, deletion or protection of Personal Data and performing a granted registered objection.

Duty of Confidentiality

Article 5.

5.1 Persons employed by or working on behalf of the Data Processor, as well as the Data Processor itself, are obliged to maintain confidentiality with regard to the Personal Data of which they may take cognisance, except insofar as a regulation given by or pursuant to the law obliges them to provide such data. The employees of the Data Processor shall sign a declaration of confidentiality to this end.

5.2 If the Data Processor is required under a legal obligation to provide data, the Data Processor shall verify the basis of the request and the identity of the party requesting the data and the Data Processor shall immediately, prior to the provision, inform the Data Controller thereof. This does not apply if prohibited by law.

Obligation to Report Data Breaches and Security Incidents

Article 6.

6.1 The Data Processor shall inform the Data Controller as soon as possible - but no later than 24 hours after the first discovery - of all (suspected) breaches of security as well as other incidents that must be reported to the Supervisory Authority or Data Subject pursuant to legislation, without prejudice to the obligation to undo or limit the consequences of such breaches and incidents as quickly as possible. The Data Processor shall also, at the first request of the Data Controller, provide all information the Data Controller considers necessary to assess the incident. When doing so, the Data Processor shall provide the Data Controller at least with the information described in Appendix 1.

6.2 The Data Processor shall have a thorough action plan for the handling and settlement of breaches and shall, upon request, provide the Data Controller with access to the plan. The Data Processor shall inform the Data Controller of any material changes to the action plan.

6.3 The Data Processor will leave the reporting of any breaches to the Supervisory Authority or authorities to the Data Controller.

6.4 The Data Processor shall provide all necessary cooperation to provide additional information to the Supervisory Authority or authorities and/or Data Subject(s) as soon as possible. When doing so, the Data Processor shall provide the Data Controller at least with the information described in Appendix 1.

6.5 The Data Processor will keep a detailed log of all (suspected) breaches of security, as well as the measures taken following such breaches, containing at least the information referred to in Appendix 1, and make it available for inspection at the first request of the Data Controller.

Security Measures and Inspections

Article 7.

7.1 The Data Processor shall implement all appropriate technical and organisational measures to protect and ensure continued protection of Personal Data processed on behalf of the Data Controller against loss or against any form of unlawful processing.

7.2 The Data Controller is at all times entitled to inspect the processing of Personal Data (or have it inspected). The Data Processor is obliged to grant the Data Controller or, if covered under the confidentiality clause, the inspection body on behalf of the Data Controller, access and provide full cooperation to ensure the inspection can actually be performed.

7.3 The inspection by or on behalf of the Data Controller shall only take place after informing the Data Processor thereof in writing.

7.4 The Data Processor undertakes to provide the Data Controller, or the third party engaged by the Data Controller, with the requested information within a period to be determined by the Data Controller. This will allow the Data Controller, or the third party engaged by the Data Controller, to form an opinion about the

Data Processor's compliance with this Data Processing Agreement. The Data Controller, or the third party engaged by the Data Controller, is obliged to treat all information relating to these inspections as confidential.

7.5 The Data Processor is required to implement the recommendations for improvement indicated by the Data Controller or the third party engaged by the Data Controller within a reasonable period of time to be determined by the Data Controller.

7.6 The reasonable costs of the inspection shall be borne by the party incurring the costs, unless the inspection shows that the Data Processor has failed to comply with any point of this Data Processing Agreement. In such a case, the costs of the inspection shall be borne by the Data Processor.

Engagement of Third Parties

Article 8.

8.1 The Data Processor shall only be entitled to outsource all or part of the performance of the work to third parties after prior written permission from the Data Controller.

8.2 The Data Controller may attach conditions to the written permission with regard to confidentiality and compliance with the obligations arising from this Data Processing Agreement.

8.3 In such cases, the Data Processor shall at all times remain the point of contact and responsible for compliance with the provisions of this Data Processing Agreement. The Data Processor guarantees in writing that these third parties will adhere to at least the same obligations as those agreed between the Data Controller and the Data Processor and shall, at the Data Processor's request, allow the Data Processor to inspect the agreements with these third parties which include these obligations.

8.4 Data Processor may only process the Personal Data within the European Union. Transferring data to other countries is permitted only with the prior written consent of the Data Controller and in compliance with applicable laws and regulations.

Amendment and Termination of the Data Processing Agreement

Article 9.

9.1 This Data Processing Agreement can only be amended by means of a written proposal approved by both parties.

9.2 Once the cooperation has ended, the Data Processor shall, at the discretion of the Data Controller, (i) return the Personal Data provided by the Data Controller under this Data Processing Agreement to the Data Controller in whole or the part specified by the Data Controller
(ii) destroy all Personal Data received from the Data Controller in any form at all locations and demonstrate the destruction of these data, unless the parties agree otherwise. If necessary, the Data Controller may impose further requirements on how the data are provided, including requirements on the file format, or the destruction thereof. These activities must be carried out within a reasonable period to be agreed upon and a report will be made of these activities.

9.3 The Data Processor shall at all times guarantee the data portability described in the previous paragraph in such a manner that no loss of functionality or (parts of) the data will occur.

9.4 The Data Controller and the Data Processor shall consult with each other about amending this Data Processing Agreement in the event a change in legislation or a change in the interpretation of legislation gives rise thereto.

9.5 If one party fails to comply with an agreed obligation, the other party may give notice of default, giving the defaulting party a reasonable period of time to comply with the obligation. The negligent party is in default, if it still fails to comply. A notice of default is not necessary if a strict deadline applies to the fulfilment of the obligation, if fulfilment is permanently impossible or if it must be inferred from a notification or the attitude of the other party that it will fail in the fulfilment of its obligation.

9.6 The Data Controller shall be entitled, without prejudice to the provisions to that effect in the Data Processing Agreement and the main agreement related thereto, and without prejudice to the other provisions of the law, to suspend the execution of this Data Processing Agreement by means of a registered letter, or to dissolve the agreement in whole or in part with immediate effect without judicial intervention, after the Data Controller has established that:

a) the Data Processor applies for (provisional) suspension of payments; or
b) the Data Processor files for bankruptcy or is declared bankrupt; or
c) the company of the Data Processor is dissolved, or
d) the Data Processor discontinues its company; or
e) there is a substantial change in control over the activities of the Data Processor's company which means that it cannot reasonably be expected of the Data Controller to maintain the Data Processing Agreement; or
f) a substantial part of the assets of the Data Processor are attached (other than by the Data Controller); or
g) the other party demonstrably fails to fulfil the obligations arising from this Data

Processing Agreement, and this serious attributable failure has not been remedied within 30 days after a written notice of default to that effect, or one of the other situations referred to in Article 9.5 occurs.

9.7 The Data Processor shall immediately inform the Data Controller if there is a threat of bankruptcy or suspension of payments, so the Data Controller can decide in a timely manner to recover the Personal Data before bankruptcy is declared.

9.8 The Data Controller is entitled to terminate this Data Processing Agreement and the main agreement with immediate effect if the Data Processor indicates that it is not or no longer able to meet the reliability requirements imposed on the processing of Personal Data due to developments in law and/or case law.

9.9 In the event of premature termination of the Data Processing Agreement, Articles 9(2) and (3) shall apply mutatis mutandis.

Liability

Article 10.

10.1 If the Data Processor fails to fulfil its obligations under this Data Processing Agreement, the Data Controller may declare the Data Processor in default. However, the Data Processor shall immediately be in default if the fulfilment of the relevant obligation is already permanently impossible within the agreed period for reasons other than force majeure. The notice of default will be made in writing, whereby the Data Processor is given a reasonable period to still fulfil its obligations. This term is a strict deadline. If the obligation is not fulfilled within this period, the Data Processor shall be in default.

10.2 Based on the provisions of the GDPR, the Data Processor bears liability, including for any damage or loss arising from non-compliance with this Data Processing Agreement.

10.3 The Data Processor shall indemnify the Data Controller against damage or loss to the extent that such damage or loss arises as a result of the Data Processor's activities.

Applicable Law

Article 11.

11.1 This Data Processing Agreement and all disputes arising from it or associated therewith are governed by Dutch law.

Thus drawn up and signed in duplicate,

on

On behalf of the Data Controller, <details of the Data Processor's representative, as referred to in the introductory sentence, to be specified>

on

On behalf of the Data Processor, Rutger-Jan Loenen, CEO of Dutchview information technology bv

Appendix 1: Information to assess incidents

The Data Processor shall provide all information the Data Controller considers necessary to assess the incident. When doing so, the Data Processor shall provide the Data Controller at least with the following information:

- the (alleged) cause of the breach;
- the (insofar as known and/or expected) consequences thereof;
- the (proposed) solution;
- contact details for following up on the notification;
- the number of persons whose data are involved in the breach (if the exact number is not known, the minimum and maximum numbers of persons whose data are involved in the breach);
- a description of the category of persons whose data are involved in the breach;
- the type or types of Personal Data involved in the breach;
- the date on which the breach occurred (if no exact date is known: the period within which the breach occurred);
- the date and time on which the breach became known to the Data Processor or to a third party or subcontractor it engages;
- whether the data were encrypted, hashed or otherwise made unintelligible or inaccessible to unauthorised persons;
- the measures already taken to stop the breach and to minimise the consequences of the breach.

Appendix 2: Mail traffic from Dutchview applications

Dutchview uses Mandrill to send automated e-mails. To do this, the relevant e-mail addresses must be listed in Mandrill. In Mandrill these e-mail addresses are stored for a maximum of 90 days because this is necessary for logging and bug tracking purposes. The way in which Mandrill handles this information is described in https://mailchimp.com/help/about-mailchimp-the-eu-swiss-privacy-shield-and-the-dpr/ and https://mailchimp.com/legal/data-processing-addendum/.