

DATA PROCESSING ADDENDUM

Last modified: June 2, 2023

Introduction

This Data Processing Addendum and its Annexes (**DPA**) reflects the parties' agreement with respect to the Processing of Personal Data by us on behalf of you, in connection with the Autoscriber Terms of Use (available at: [Terms of Use](#)) entered into between you and us (the **Agreement**).

This DPA is supplemental to, and forms an integral part of, the Agreement and is effective after you accepted the Terms of Use, during the sign-up process. Please contact us if you do not agree with the content of our DPA, in which case we will conclude a tailored data DPA.

We update this DPA from time to time. If you have an active Autoscriber subscription, we will let you know when we do via email or via in-app notification. The term of this DPA will follow the term of the Agreement. Terms not otherwise defined in this DPA will have the meaning as set forth in the Agreement. For the purpose of this DPA, Autoscriber and the customer are each a **Party** and together the **Parties**.

Signed version?

This Autoscriber DPA is made available at [Data Processing Addendum](#) and is incorporated into the Autoscriber Terms of Use. For customers that would like to receive a signed copy of the Autoscriber DPA, we have made this copy available to you. This copy includes signatures on the DPA version last modified June 2, 2023. No changes made to this copy are agreed to by Autoscriber. Please note that we update this DPA as we describe in the 'Introduction' section below. If you have any questions, please contact your Autoscriber representative.

1. Definitions

| Definition | Meaning |
|-------------------------------|--|
| Applicable Legislation | The GDPR and all other relevant legislation and regulations in the field of protection of Personal Data, like the Dutch Telecommunications Act (<i>Telecommunicatiewet</i>) regarding the use of cookies. |
| Controller | You, who as a customer makes use of Autoscriber's Service to Process Personal Data and determines the purpose and means of the processing. |
| Data Breach | (suspicion of) a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. |
| DPIA | Data protection impact assessment. |
| Data Subject | Any person of which personal data is collected on the basis of this DPA; data subjects within the meaning of what is specified in the GDPR. |
| EEA | European Economic Area: the Member States of the European Union (EU) and Iceland, Liechtenstein and Norway. |
| Employee | The employees and other persons engaged by the Processor for the performance of the Agreement. |
| GDPR | General Data Protection Regulation. |
| Personal Data | Data which can be used either directly or indirectly to identify a natural person, as intended in the GDPR. |
| Processing | Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means. Examples are: collection, storage, alteration or use. |
| Processor | The party which Processes Personal Data on behalf of the Controller. |
| DPA | The underlying Data Processing Addendum, applicable between Parties. |
| Recipient | A natural or legal person, public authority, agency or another body to whom/which the Personal Data are disclosed. |
| Services | the service(s) to be provided by the Processor to the Controller based on the Agreement. |
| Sub-Processor | Third parties engaged by the Processor for the performance of the Agreement. |
| Supervisory Authority | An independent public authority which is established by an EU Member State pursuant to the GDPR. In the Netherlands, this is the Dutch Data Protection Authority (<i>Autoriteit Persoonsgegevens</i>). |

| | |
|--------------------|---|
| Third Party | A third party other than the Data Subject, the Controller or the Processor, or the person who, under the direct authority of the Controller or Processor, is authorised to process Personal Data. |
|--------------------|---|

2. Scope

- 2.1. The DPA applies to all Processing in the performance of the Agreement.
- 2.2. The DPA is part of the Agreement and replaces all previous arrangements between the Parties regarding the Processing of Personal Data. In the event of any conflict, the provisions of the DPA prevail.

3. Parties' Roles

- 3.1. Within the context of the performance of the Agreement, Autoscriber processes Personal Data on your behalf and is deemed a Processor within the meaning of the GDPR. You are deemed a Controller within the meaning of the GDPR.
- 3.2. If the Processor determines the purpose and means of the Processing instead of the Controller, the Processor is deemed as the controller for that Processing.

4. Processing of Personal Data

- 4.1. The Processor shall only Process Personal Data:
 - a) As described in **Annex A** (*Description of Processing Activities*);
 - b) In accordance with the Agreement and to comply with other reasonable instructions provided by the Controller that are consistent with the terms of the Agreement (the **Purpose**).
- 4.2. Autoscriber shall act on behalf of and on the instructions of the Controller in carrying out the Purpose.
- 4.3. The Controller may amend its instructions or issue additional instructions at the Controller's sole discretion.
- 4.4. The Processor shall never process the Personal Data for its own benefit, the use of Third Parties and/or other purposes, unless Applicable Legislation oblige the Processor to perform Processing. The Processor shall notify the Controller of this provision prior to the Processing to the extent permitted by law.
- 4.5. The Parties shall comply with the GDPR and other Applicable Legislation concerning the Processing of Personal Data. If the Processor suspects that an instruction from the Controller breaches the GDPR or Applicable Legislation, the Processor shall immediately notify the Controller.

5. Assistance & Cooperation

- 5.1. The Processor shall provide the Controller with all necessary assistance and cooperation in complying with the obligations of the GDPR and Applicable Legislation, including:

- a) The security of Personal Data;
- b) The performance of checks and audits;
- c) The performance of DPIA's;
- d) The prior consultation with the Supervisory Authority;
- e) Compliance with requests from the Supervisory Authority or another public body;
- f) Compliance with requests from Data Subjects;
- g) Reporting Data Breaches.

Requests from Data Subjects

- 5.2. With regard to requests from Data Subjects, the Processor shall take all reasonable measures to ensure that the Data Subject can exercise its rights.
- 5.3. If a Data Subject contacts the Processor directly, the Processor shall immediately report this to the Controller, with a request for further instructions. Pending instructions, the Processor shall adequately assist and inform the Data Subject about the next steps.
- 5.4. If the Processor offers the Services directly to the Data Subject, the Processor is obliged to inform the Data Subject on behalf of the Controller about the Processing of the Data Subject's Personal Data in a manner that is in accordance with the Data Subject's rights.

Requests from Supervisory Authority

- 5.5. With regard to requests from the Supervisory Authority or a Dutch and/or foreign public body, the Processor shall immediately notify the Controller in so far as this is permitted by law. When handling the request or order, the Processor shall observe all of the Controller's instructions and provide to the Controller all reasonably required cooperation.
- 5.6. If the Processor is prohibited by law from complying with its obligations on the basis of Article 5.5, the Processor shall promote the Controller's reasonable interests in the following way:
 - a) The Processor shall procure a legal assessment of the extent to which (i) the Processor is required by law to comply with the request or order; and (ii) the Processor is in fact prohibited from complying with its obligations to the Controller based on Article 5.5;
 - b) The Processor shall only cooperate with the request or order if the Processor is required by law to do so, and the Processor shall object where possible (by legal action) to the request or order or the injunction against informing the Controller in this respect or against following the Controller's instructions;
 - c) The Processor shall not provide any more Personal Data than strictly necessary to comply with the request or order;
 - d) In the case of a transfer as specified in Article 10, the Processor shall investigate the possibilities for complying with the rules of the GDPR regarding transfers.

Data Protection Impact Assessment

- 5.7. The Controller shall investigate the necessity under the GDPR to carry out a DPIA and to consult the relevant Supervisory Authority in advance, for the engagement of the Processor.
- 5.8. The Processor shall provide reasonable assistance to the Controller with any DPA and with any prior consultations to any Supervisory Authority which are required under the GDPR.

6. Access to Personal Data

- 6.1. The Processor shall limit access to Personal Data by Employees, Sub-Processors, Third Parties and other Recipients of Personal Data to a necessary minimum.
- 6.2. The Processor shall restrict the access to the Personal Data to authorised Employees on a need-to-know basis.
- 6.3. The Controller authorises the engagement of the Sub-Processor(s) by the Processor listed in **Annex C** (*Sub-Processors*).
- 6.4. Controller provides Processor with a general authorisation to engage Sub-Processors in connection with the provision of the Services.
- 6.5. The Controller's consent to outsourcing work to a Sub-Processor does not affect the fact that for the deployment of Sub-Processors in a country outside the EEA requires consent in accordance with Article 10 of this DPA.
- 6.6. Processor will impose the same material data protection obligations on the Sub-Processors as set out in this DPA, in particular in relation to the implementation of appropriate technical and organisational measures.
- 6.7. Processor shall notify Controller of any intended changes concerning the engagement or replacement of a Sub-Processor and Controller shall be given thirty (30) days to object, duly motivated and in writing, after receiving such notification.
- 6.8. If the Processor fails to address such an objection, the Controller's sole and exclusive remedy is to terminate the Agreement and this DPA immediately by providing written notice to the Processor.
- 6.9. In the event the Processor uses Sub-Processors, Processor shall remain fully liable to the Controller for the fulfilment of its obligations under this DPA, the Agreement, the GDPR and the Applicable Legislation.

7. Security Measures

- 7.1. The Processor implements all appropriate technical and organisational measures to safeguard a level of security appropriate to the risk, so that the Processing complies with the requirements under the GDPR and Applicable Legislation.
- 7.2. The Processor shall take at least the security measures included in **Annex B** (*Security Measures*).

8. Audit

- 8.1. At the Controller's request and with a maximum of 1 (one) time per calendar year, the Controller has the right to have an audit performed by an independent (legal) person authorised by the Controller in respect of the Processor's organisation, in order to demonstrate that the Processor complies with the provisions of the DPA, the GDPR and other Applicable Legislation and Regulations.
- 8.2. The costs of any audit are at the Controller's expense, unless the audit reveals any material non-compliance by Processor (or Sub Processor) under this DPA, in which case the reasonable costs of the audit shall be borne by Processor.
- 8.3. The Processor shall immediately take all measures that are reasonably necessary according to an audit, to ensure the compliance of the Processor. The associated costs are borne by the Processor.

9. Data Breach

- 9.1. The Processor shall notify the Controller of a Data Breach without unreasonable delay and within 36 (thirty-six) hours at the latest. This report includes if possible (at least) all information from the most recent "Data Breaches form" of the Dutch Supervisory Authority.
- 9.2. If the Processor is unable to simultaneously provide all of the information from the Data Breach, the information may be provided to the Controller step-by-step without unreasonable delay and no later than within 36 (thirty-six) hours after the discovery.
- 9.3. At the Controller's request, the Processor will provide the Controller with reasonable assistance as necessary to enable the Controller to notify the Data Breaches to the competent Supervisory Authority and/or affected Data Subjects.
- 9.4. The Processor has organised adequate policy and adequate procedures to comply with its obligations regarding Data Breaches, including a Data Breach Register. At the Controller's request, the Processor shall provide information about and allow inspection of this policy and procedures.

10. Transfers of Personal Data

- 10.1. The Processor may only transfer Personal Data to countries outside the EEA or to international organisations if:
 - a) there is an adequate level of protection and a transfer mechanism of the GDPR can be invoked; and
 - b) the Controller has given express prior written consent for the transfer.
- 10.2. The Processor consents to the transfer of Personal Data as described in **Annex D** (*Data Transfers*).

- 10.3. The Processor shall immediately notify the Controller in writing of any (planned) permanent or temporary transfers of Personal Data to a country outside the EEA and shall only give effect to such planned transfers after obtaining the Controller's written consent. The Controller shall at all times have the right to attach additional conditions to its consent to such processing.
- 10.4. The provisions in this Article 10 do not apply in case a provision under Union law or under Member State law requires the Processor to perform Processing. In that event, the Processor shall notify the Controller of this provision in writing prior to the Processing to the extent permitted by law.
- 10.5. At the Controller's request, the Processor shall demonstrate that the requirements laid down in Article 10.1 have been met.

11. Confidentiality and Non-Disclosure

- 11.1. All Personal Data are qualified as confidential and must be treated as such.
- 11.2. The Parties shall keep all Personal Data confidential and shall not disclose them in any way (internally or externally) unless:
 - a) disclosure and/or provision of the Personal Data is necessary in the context of the performance of the Agreement or the DPA;
 - b) any mandatory statutory provision or court decision requires the Parties to disclose and/or provide the Personal Data, in which case the Parties shall first notify the other Party;
 - c) disclosure and/or provision of the Personal Data takes place with prior written consent from the other Party.

12. Liability & Indemnification

- 12.1. The Processor is not liable for any loss or damage caused by a breach by the Controller of the GDPR or Applicable Legislation. The Controller indemnifies the Processor against claims of Sub-processors, other Third Parties, Data Subjects or other persons regarding such loss and damage, and against any legal and other expenses incurred by the Processor in that context and any fines imposed on the Processor.
- 12.2. The Processor's limitation of liability agreed on in the Agreement and the applicable terms and conditions, apply to this DPA. One or more claims for compensation under this DPA and/or the Agreement jointly can in no event result in exceeding that limitation.
- 12.3. If no limitation of liability is provided for in the Agreement, the Processor's liability under this DPA is in any event limited to:
 - a) the amount of the fee for the assignment under the Agreement; or
 - b) in any event the part of the assignment to which the liability relates.

13. Term & Termination

- 13.1. The DPA constitutes an integral part of the Agreement and shall automatically terminate upon termination of the Agreement.
- 13.2. The Controller may terminate the DPA if the Processor does not or can no longer comply with the DPA, the GDPR and/or the Applicable Legislation, without the Processor being entitled to any damages. The Controller shall observe a reasonable notice period, unless the circumstances justify immediate termination.
- 13.3. Within 1 (one) month after termination of the Agreement, the Processor shall:
 - a) destroy and/or return all Personal Data, including all existing copies held by (legal) persons engaged by the Processor;
 - b) transfer the Personal Data to the Controller and/or another party to be designated by the Controller, at the Controller's discretion.
- 13.4. At the Controller's request, the Processor shall confirm in writing that the Processor has satisfied all obligations under Article 13.3.
- 13.5. The Processor shall bear the reasonable costs for the destruction, return and/or transfer of the Personal Data. The Controller may impose additional requirements on the manner of destruction, return and/or transfer of the Personal Data, including requirements on the file format.

14. Legal Effect

- 14.1. This DPA shall only become legally binding between the Parties when the Controller has agreed to the Terms of Use, as specified in the Section "Introduction".

15. Miscellaneous

- 15.1. Only written amendments to this DPA shall be valid.
- 15.2. Obligations under the DPA that are intended by their nature to continue after termination of this DPA will continue to apply after termination of the DPA.
- 15.3. This DPA replaces all prior agreements between Parties regarding the processing of Personal Data.

ANNEX A – Description of Processing Activities

| SPECIFICATION OF PROCESSING | |
|----------------------------------|--|
| Data Subjects Categories | <p>The categories of Data Subjects whose Personal Data is Processed include:</p> <ol style="list-style-type: none"> a. Medical Practitioner: a person using the Autoscriber Flow on behalf of the Controller (such as: doctors, surgeons, nurses, medical interns) b. Patient: a patient of the Medical Practitioner using Autoscriber Flow; c. Companion: a companion of the Patient who is present during an interview between the Medical Practitioner and the Patient. |
| Personal Data Categories | <p>Autoscriber Processes the following (special) categories of Personal Data on behalf of the Controller:</p> <ol style="list-style-type: none"> a. The recordings of the conversation between the Medical Practitioner and the Patient (the Recordings); b. any other (special categories of) Personal Data entered into Autoscriber’s platform by the Medical Practitioner in relation to the Patient (Other Data). <p>These Recordings and Other Data may contain (sensitive) personal data, such as: name, date of birth, address, contact information, complaints, diagnoses, medication use, allergies, height, weight, medical history, blood group.</p> |
| Description of Processing | <p>Autoscriber offers access to Autoscriber Flow: an AI-application that turns the conversation between a doctor and a patient into a structured summary, as more particularly described in the Agreement. Personal Data will be processed in accordance with the Agreement (including this DPA) and may be subject to the following processing activities:</p> <ol style="list-style-type: none"> a. Storage and other Processing necessary to provide, maintain and improve the Service provided to Controller pursuant to the Agreement; b. Disclosures in accordance with the Agreement and/or as compelled by applicable law. c. To provide customer and technical support to Customer |
| Frequency of Processing | Continuously and as determined by the Controller. |
| Retention Period | Subject to the Section “ Term & Termination ” of this DPA, we will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing. |

ANNEX B – Security Measures

| SECURITY MEASURES TAKEN BY AUTOSCRIBER | |
|--|---|
| Access Control | The access to the Personal Data is restricted to the authorised employees on a <i>need-to-know</i> basis. |
| Encryption | The Personal Data is secured by means of JSON Web Encryption (JWE). |
| Multifactor Authentication | The access to the Personal Data is secured with two-factor authentication (2FA). |
| Transmission Control | <i>Standalone version</i> Data in-transit: Secure network connections with Transport Layer Security (TLS) technology or a non-deprecated technology that is similar to TLS. |
| Non-disclosure | Non-Disclosure Agreements (NDA's) are concluded in the event that confidential information is exchanged. |

ANNEX C – Sub-Processors

| Sub-Processor | Purpose of Processing | Entity Location | Compliance Info | Remarks |
|------------------------|--|-----------------|--|---|
| Google LLC | Cloud service provider; External communication with users and customers; deploying models. | USA | Cloud Data Processing Addendum | Data residency: data is hosted in Europe. |
| Slack | Internal communication tool (HIPAA-compliant). | USA | Data Processing Addenda | Data residency: data is hosted in Europe. |
| Confluence | Internal workspace tool. | USA | Data Processing Addendum | |
| HubSpot | CRM-tool for external communication with users and customers. | USA | Data Processing Agreement | Data residency: data is hosted in Europe. |
| Microsoft Azure | Hosting and infrastructure; deploying models, storing and transferring data. | USA | Data Protection Addendum | Data residency: data is hosted in Europe. |
| Okta (Auth0) | User authentication tool. | USA | Data Processing Addendum | |

ANNEX D – Data Transfers

The Controller has given the Processor consent for the transfers to third parties or international organisations included below.

| Description of Transfer | Entity transferring the Personal Data + Country | Entity receiving Personal Data + Country | Transfer Mechanism |
|--------------------------------|--|---|---------------------------|
| | | | |

SIGNED

On behalf of Controller

Autoscriber B.V.

A handwritten signature in black ink, appearing to be 'Jacqueline Kazmaier', written over a horizontal line.

By: _____

By: Jacqueline Kazmaier

Title: _____

Title: Director

Date: _____

Date: 10.07.2023