Data Processing Policy

Last updated: 13-11-2024

PLEASE READ THIS DATA PROCESSING POLICY CAREFULLY

The following contains the Data Processing Policy (DPP) of Scriptix B.V. (Processor) for the Scriptix Content Accessibility Platform, having its place of business at Kon. Wilhelminahaven ZZ 20, 3134KG, Vlaardingen Netherlands, registered at the Chamber of Commerce under number 75668475 (hereafter: “Scriptix”) for Scriptix Speech Recognition (hereafter: “the Services”). Partner under this DPP acts as Controller.

- the Controller has access to personal data of various data subjects,
- the Controller intends to have the Processor perform certain processing operations, for which the Controller determines purpose and means,
- the Processor is willing to do so, and further is willing to adhere to the obligations regarding security and other aspects of data processing legislation to the best of its abilities,
- the Parties, considering the requirement from data processing legislation for a written instrument to record their rights and obligations,
- the Processor will take the mandatory security measures, and other measures, imposed by the General Data Protection Regulation (hereinafter: GDPR).
- the Parties, in consideration of the requirements of Article 28(3) GDPR, wish to lay down their rights and obligations in writing.

Article 1. Purposes of processing

1.1. Processor hereby agrees under the terms of this Data Processing Policy to process personal data on behalf of the Controller. Processing shall be done solely for the purpose of storing data in the 'cloud' for the benefit of Controller, and associated online services, and all purposes compatible therewith or as determined jointly.

1.2. The personal data to be processed by Processor for the purposes as set out in the previous clause and the categories of data subjects involved are set out in Appendix 1 to this Data Processing Policy. Processor shall not process the personal data for any other purpose unless with Controller's consent. Controller shall inform Processor of any processing purposes to the extent not already mentioned in this Data Processing Policy.

1.3. All personal data processed on behalf of Controller shall remain the property of Controller and/or the data subjects in question.

Article 2. Processor obligations

2.1. Regarding the processing operations referred to in the previous clause, Processor shall comply with all applicable legislation, including at least all data processing legislation such as the GDPR.

2.2. Upon first request Processor shall inform Controller about any

measures taken to comply with its obligations under this Data Processing Policy.

2.3. All obligations for Processor under this Data Processing Policy shall apply equally to any persons processing personal data under the supervision of Processor, including but not limited to employees in the broadest sense of the term.

2.4. Processor shall inform Controller without delay if in its opinion an instruction of Controller would violate the legislation referred to in the first clause of this article.

2.5. Processor shall provide reasonable assistance to Controller in the context of any data protection impact assessments to be made by Controller.

2.6. Processor shall, in accordance with Article 30 GDPR, keep a register of all categories of processing activities which it carries out on behalf of the Controller under this Data Processing Policy. At Controller's request, Processor shall provide Controller access to this register.

Article 3. Transfer of personal data

3.1. Processor may process the personal data in any country within the European Union.

3.2. Transfer to countries outside the European Union is not permitted.

3.3. Processor lists sub-processors, their country of incorporation and countries where processing will take place in Appendix 2.

Article 4. Allocation of responsibilities

4.1. The authorized processing operations shall be performed by employees of Processor within an automated environment.

4.2. Processor is solely responsible for the processing of personal data under this Data Processing Policy in accordance with the instructions of Controller and under the explicit supervision of Controller. For any other processing of personal data, including but not limited to any collection of personal data by Controller, processing for purposes not reported to Processor, processing by third parties and/or for other purposes, the Processor does not accept any responsibility.

4.3. Controller represents and warrants that the content, usage, and instructions to process the personal data as meant in this Data Processing Policy are lawful and do not violate any right of any third party.

Article 5. Involvement of sub-processors

5.1. Processor involves sub-processors as listed under Appendix 2. Processor shall not involve any third parties in the processing under this Data Processing Policy without the prior written permission of Controller, which permission may be made conditional.

5.2. In any event, Processor shall ensure that any third parties are

bound to at least the same obligations as agreed between Controller and Processor.

5.3. Processor shall ensure that these third parties shall comply with the obligations under this Data Processing Policy and is liable for any damages caused by violations by these third parties as if it committed the violation itself.

Article 6. Security

6.1. Processor shall use reasonable efforts to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk for the processing operations involved, against loss or unlawful processing (in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed).

6.2. Processor shall implement at least the following specific security measures:

- Logical access control, using: strong passwords, 2FA
- Physical access control measures
- Encryption of digital data containing personal data
- Organizational measures for access control
- Transport Layer Security (TLS) technology for securing network communication
- A secure internal network
- Checks on granted authorizations

6.3. Processor does not warrant that the security is effective under all circumstances. If any security measure explicitly agreed in this Data Processing Policy is missing, then Processor shall use best efforts to ensure a level of security appropriate to the risk considering the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Article 7. Notification and communication of data breaches

7.1. Controller is always responsible for notification of any security breaches and/or personal data breaches (which are understood as: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed as described in Article 4 (12) of the GDPR) to the competent supervisory authority, and for communication of the same to data subjects. To enable Controller to comply with this legal requirement, Processor shall notify Controller without undue delay an actual or threatened security or personal data breach.

7.2. A notification under the previous clause shall be made within 48 hours of discovery.

7.3. The notification shall include at least the fact that a breach has occurred. In addition, the notification shall:

- describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- describe the likely consequences of the personal data breach;
- include the name and contact details of the Data Protection Officer (if appointed) or a contact person regarding privacy subjects;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Article 8. Processing requests from data subjects

8.1. In the event a data subject makes a request to exercise his or her legal rights under the GDPR (Articles 15-22) to Processor, the parties shall jointly consult on how to handle the request. Controller shall however retain final responsibility on the request.

Article 9. Confidentiality obligations

9.1. All personal data that Processor receives from Controller and/or collects itself is subject to strict obligations of confidentiality towards third parties. Processor shall not use this information for any goals other than for which it was obtained, not even if the information has been converted into a form that is no longer related to an identified or identifiable natural person.

9.2. The confidentiality obligation shall not apply to the extent Controller has granted explicit permission to provide the information to third parties, the provision to third parties is reasonably necessary considering the nature of the assignment to Controller or the provision is legally required.

Article 10. Audit

10.1. Controller has the right to have audits performed on Processor by an independent third party bound by confidentiality obligations to verify compliance with the security requirements, and all issues reasonably connected thereto.

10.2. Processor shall give its full cooperation to the audit and shall make available employees and all reasonably relevant information, including supporting data such as system logs.

10.3. The audit findings shall be assessed by Processor and implemented if and to the extent deemed reasonable by Processor.

10.4. The costs of the audit shall be borne by Controller, unless its findings result in revealing shortcomings under this agreement on the part of Processor. In that case costs for the audit shall be borne by Processor.

Article 11. Liability

11.1. Parties explicitly agree that any liability is as provided by law.

Article 12. Term and termination

12.1. This Data Processing Policy enters into force upon signature by the parties and on the date of the last signature.

12.2. This Data Processing Policy is entered into for the duration of the cooperation between the parties.

12.3. Upon termination of the Data Processing Policy, regardless of reason or manner, Processor shall - at the choice of Controller - return in original format or destroy all personal data available to it.

12.4. Parties may change this Data Processing Policy only with mutual consent.

Article 13. Applicable law and competent venue

13.1. This Data Processing Policy and its execution are subject to Dutch law.

13.2. Any disputes that may arise between the parties in connection with this Data Processing Policy shall be brought to the competent court for the place of business of Processor.

Appendix 1: Stipulation of personal data and data subjects

Data subjects and personal data of different purposes
Processor shall process the below (personal) data of the categories data subjects from different purposes (with retention period if specified) under the supervision of Controller, as specified in article 1 of the Data Processing Policy:

- First and last name of Controller's personnel appointed to work with Processor's platform.
- Email address of Controller's personnel appointed to work with Processor's platform.
- Company details of Controller.
- Company/organization details of Controller's end customers.
- Audio-visual material processed (uploaded) on Processor's platform.
- Translations from STT results.

Controller represents and warrants that the description of personal data and categories of data subjects in this Appendix 1 is complete and accurate and shall indemnify and hold harmless Process for all faults and claims that may arise from a violation of this representation and warranty.

Appendix 2: List of sub-processors

Processor shall process the (personal) data from Appendix 1 under the supervision of Controller, as specified in article 1 of the Data Processing Policy with the following sub-processors:

Company Name	**Country of Incorporation**	**Place of Processing**
Microsoft Azure	U.S.	West-Europe
DeepL GmbH	Germany	Finland