# Data Processing Addendum

Contents



## 1. General Regulations

### 1.1 Introduction, Scope, Definitions

1.1.1 These terms govern the rights and obligations of the customer ("**Controller**") and Personio ("**Processor**") in the context of the processing of personal data on behalf of the Controller in relation to the Software and Services provided by the Processor ("**DPA**"). This DPA is designed to comply with the provisions of the EU General Data Protection Regulation ("**GDPR**"). Where there is any conflict between the terms of this DPA and the Agreement, then the terms of this DPA shall take precedence.

1.1.2 Unless otherwise defined in this DPA, all capitalised terms shall have the meaning given to them in the Agreement or in the GDPR, as applicable.

1.1.3 The Controller agrees to the terms of this DPA on behalf of itself and any affiliate(s) who may be involved in the Processing of Personal Data under this DPA.

### 1.2 Scope of Processing, Categories of Data, Data Subjects

1.2.1 Details regarding the potential processing information is set out in sections 1.2.2 and 1.2.3. The Controller acknowledges the scope of the processing information is at the Controller's discretion and shall vary depending on the nature of the use of the Software and Services.

1.2.2 Data types / categories may include:

- Personnel master data (e.g. name, address, date of birth, telephone number)
- Contract master data (e.g. information on professional qualifications and school education, information on continuing vocational training, other documents, employment contracts and certificates concluded or issued between the Controller and his employees)
- Accounting and service data (e.g. bank details, absences, vacation plans, sick leave, working hours, employee evaluations)
- Payroll data
- Contract billing and payment data

1.2.3 Categories of data subjects may include in relation to the Controller (or affiliated company of the Controller):

- Employees - Freelancers, salaried employees or volunteers
- Former employees - freelancers, salaried employees or volunteers
- Future employees, volunteers or applicants

1.2.4 The provision of the contractually agreed data processing takes place exclusively in a member state of the European Union, another state party to the Agreement on the European Economic Area or a state with an adequate level of data protection in accordance with Art. 45 GDPR, as determined by the European Commission.

1.2.5 The Processor shall only carry out an international transfer of personal data to a country outside of the European Economic Area in compliance with the GDPR and shall implement appropriate safeguards to the extent necessary under the GDPR.

1.2.6 The Processor shall Process Personal Data for the duration of the provision of the relevant Software or Services, unless otherwise agreed upon in writing.

## 2. Confidentiality

The Processor shall ensure that confidentiality is maintained in accordance with Art. 28 para. 3 S. 2 point (b), 29 and 32 para. 4 GDPR. The Processor shall ensure that any person that it authorises to Process Personal Data shall be subject to confidentiality provisions (whether a contractual or a statutory duty).

## 3. Obligations of the Controller

3.1 The Controller shall be responsible for its own compliance with the GDPR in relation to the use of the Software and Services (as applicable).

3.2 The Controller must inform the Processor immediately and in full if they detect errors or irregularities in light of processing with regard to data protection regulations.

3.3 If necessary, the Controller shall provide the Processor with the contact person for any data protection issues arising within the scope of this DPA.

## 4. Instructions

4.1 The Processor shall not Process any Personal Data on behalf of the Controller other than on the documented instructions of the Controller (provided that such instructions are within the scope of the Software/Services) or as necessary to comply with the GDPR. The Processor shall notify the Controller as soon as reasonably practicable if it determines, acting reasonably, an instruction may infringe the GDPR. The Processor shall not be required to comply with such infringing instruction unless and until the matter has been resolved by agreement of the parties.

4.2 The Controller designates the persons exclusively authorised to issue instructions within the Software. In the event that no person authorised to issue instructions is appointed, only natural persons authorised to legally represent the Controller are entitled to issue instructions. The Processor may suspend the execution of instructions until the Controller has provided proof of the authority to legally represent the Controller to the Processor.

## 5. Obligations of the Processor

### 5.1 General Obligations of the Processor

5.1.1 The Processor shall appoint a data protection officer. Contact details (as updated from time to time) of the data protection officer shall be made available on the Processor's website.

5.1.2 The Processor shall provide reasonable assistance to the Controller in relation to any data protection impact assessment and prior consultations with the Supervisory Authority, in each case solely in relation to the Processing of the Controller's Personal Data by, taking into account the nature of the processing and information available to the Processor. The Processor may charge the Controller for any assistance to the extent it is not commercially reasonable for the Processor to provide such assistance without charge (considering volume, complexity and timescale). The Processor shall provide the Controller with details of any estimated applicable fees in advance.

5.1.3 The Processor shall immediately inform the Controller of any control actions and measures taken by the Supervisory Authority in so far as they relate to this DPA. This shall also apply if a competent authority determines that Personal Data from this Processing has been processed by the Processor and is connected to administrative or criminal proceedings, unless the Processor is obliged by law or by the authorities to refrain from making such notification.

**5.2 Audit**

5.2.1 The Controller is entitled to inspect compliance with the obligations arising from the DPA, the technical and organisational measures ("**TOM**") and GDPR upon agreement with the Processor during its usual business hours, taking into account a minimum of 14 days' notice or to have them checked by auditors to be appointed in individual cases. To this end, the Controller may, among other things, inspect the relevant buildings and facilities of the Processor, obtain information or inspect their own data with due regard to the legitimate interests of the Processor. For audits that become necessary due to a security incident or a more than insignificant violation of the provisions for the protection of personal data or provisions of this DPA ("**Event-related On-site Audit**"), the notification period from sentence 1 shall be reduced to an appropriate period. Furthermore, Event-related On-site Audits are not subject to the restrictions of sections 5.2.3-5.2.4 of this DPA.

5.2.2 The Processor may make the consent to the audit dependent on the auditor submitting to an appropriate confidentiality agreement. If the auditor commissioned by the Controller is in a competitive relationship with the Processor or if another justified case exists, the Processor has the right to object to the Controller's choice.

5.2.3 Within the scope of this clause, the Processor is only obliged to tolerate and cooperate in one **non**-event-related on-site audit (without cause) per calendar year. The effort of an **non**-event-related on-site audit (without cause) is generally limited to one day per calendar year for the Processor.

5.2.4 If and as long as the Processor provides sufficient evidence of the fulfilment of its obligations, in particular the implementation of the TOM and its effectiveness, by means of appropriate evidence, they reserve the right to refuse the **non**-event-related on-site audit from this section. Appropriate evidence may in particular include approved rules of conduct within the meaning of Art. 40 GDPR or an approved certification procedure within the meaning of Art. 42 GDPR. Both parties agree that the submission of certificates or reports by independent bodies, a conclusive company data security concept or a suitable

certification by an IT security and data protection audit are also recognised as suitable evidence.

## 6. Technical and Organisational Measures

6.1 Taking into account 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, the Processor shall implement and maintain TOM to ensure an appropriate level of security of the Controller's Personal Data. The latest version of TOM can be accessed within the Software (currently in "Settings" > "Support" > "Subscription & Billing" > "Data Processing Information").

6.2 The TOM are subject to technical progress and further development and the Processor may update or modify the security measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Software and Services.

## 7. Sub-processors

7.1 Subcontracting relationships within the meaning of this DPA are only those services that are directly related to the provision of the main service as specified in section 1.2.1. Current sub-processors used by the Processor can be accessed via the Software (currently in "Settings" > "Support" > "Subscription & Billing" > "Data Processing Information"). Ancillary services, such as transport, maintenance and cleaning, the use of telecommunications services, user service or customer relationship management as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems, are not included. The Processor's obligation to ensure compliance with data protection and data security in accordance with the relevant legal provisions shall remain unaffected in these cases as well.

7.2 The assignment of sub-processors for the Processing or use of Personal Data is in principle only permitted with the approval of the Controller. For the sub-processors listed within the Software at the time the Agreement is concluded, this approval is granted upon conclusion of the Agreement.

7.3 The Processor may remove or add new sub-processors. The Processor shall inform the Controller in text by active notification (email) if they intend to remove or engage a new sub-processor. If the Controller raises no reasonable objection on data protection grounds in text form (including email) within 14 days of receipt of the notice, then it shall be taken as

an approval of the change. In the event of an objection, if the parties are not able to achieve a resolution, the Processor may terminate the Agreement with immediate effect.

7.4 The Processor shall enter into an agreement with any sub-processor imposing appropriate contractual obligations on the sub-processor as set out in this DPA and meet the requirements of Art 28 (3) of the GDPR. The Processor shall remain responsible for any act or omission of its sub-processors.

## 8. Rights of the Data Subjects

8.1 If a data subject addresses the Processor with a claim under Chapter III of the GDPR with regard to the rights of the data subjects, the Processor will refer the data subject to the Controller, provided that an assignment to the Controller is possible after indication of the data subject.

8.2 The Controller acknowledges that the Software enables comprehensive self-administration of its personal data to assist it in connection with its obligations under GDPR (including its obligations to responding to data subject requests). To the extent the Controller is unable to independently address a request then the Processor shall provide reasonable assistance.

8.3 The Processor is not liable if the Controller does not respond to the request of a data subject, does not respond correctly or does not respond in due time and this is solely the fault of the Controller.

## 9. Information and Notification Obligations

The Processor shall notify the Controller without undue delay upon becoming aware of a Personal Data Breach affecting the Controller's personal data. Any notification shall be in accordance with Article 33 of the GDPR.

## 10. Disclosure and Deletion of Data

10.1 Upon completion of the data processing, the Processor shall disclose the Personal Data provided in accordance with the following paragraphs. As a rule, the data processing is terminated at the end of the term of the Service Agreement.

10.2 The Processor is obliged to keep the Personal Data provided for a period of 30 days after the end of the Agreement. The Controller is entitled at any time until the expiry of this period to demand in text form the disclosure of personal data in a machine-readable format or deletion of the stored personal data or, if possible, to download the data directly from the Software. The Controller is solely responsible for the timely export of their data.

10.3 If the Controller issues the Processor with binding instructions for deletion in text form, the Processor shall be entitled to carry out the deletion of data even before the expiry of the retention period pursuant to section 10.2. The only exception to this is the data in respect of which the Processor is legally obliged to store.

10.4 If the Controller has neither requested the data to be disclosed nor requested the deletion of such data by the end of the period pursuant to section 10.2., the Processor shall be obliged to delete such data.

## 11. Liability

11.1 Both parties shall be liable in accordance with Article 82 of the GDPR in relation to any loss caused by a breach of this DPA or the GDPR.

11.2 Where, in accordance with Article 82 (para 4) GDPR, both parties are responsible for any claims by the data subject or third parties, then the Controller shall be solely liable for any loss, except to the extent any proportion of the total loss can be attributed to the Processor. The Controller bears the burden of proof that damage is not the result of circumstances under its responsibility.

11.3 Any exclusions of liability in this DPA shall not apply in the event of intent or gross negligence or in the event of damage resulting from death or personal injury.

11.4 In all other respects, liability shall be governed by the Service Agreement.

## 12. Final Provisions

12.1 Both parties are obliged to confidentially treat all knowledge of business secrets and data security measures of the other party that were acquired within the scope of the contractual relationship, even beyond the termination of the Agreement. This also applies in particular to the contents of this DPA, as well as all documents, evidence etc. made available within the framework of the data protection audit. If there are any doubts as to whether information is subject to confidentiality, it shall be treated as confidential until it is released in writing by the other party.

12.2 Amendments and supplements to this DPA and all its components - including any assurances given by the Processor - shall be made in text form (including email) in accordance with the GDPR, which may also be in an electronic format, and require an express indication that these terms and conditions have been amended or supplemented. This also applies to the waiver of this formal requirement. The parties agree that

adjustments to this DPA shall be concluded in an electronic format in accordance with Article 28 para. 9 GDPR.

12.3 Should the data of the Controller be endangered by seizure or confiscation, by insolvency or composition proceedings or by other events or measures of third parties, the Processor shall inform the Controller immediately. The Processor shall immediately inform all parties involved in this connection that the sovereignty and ownership of the data lies exclusively with the Controller as the "responsible party" in the sense of the GDPR.

12.4 The law of the Federal Republic of Germany shall apply. The UN Convention on Contracts for the International Sale of Goods (CISG) is not applicable. Exclusive place of jurisdiction for all disputes in connection with this DPA is, if permissible, Munich.

12.5 This DPA replaces all previous or concomitant warranties, arrangements, agreements, contracts or notifications among the Controller and the Processor, whether written or oral, with respect to the subject matter of this DPA unless the parties have concluded a DPA before August 08, 2023.

12.6 Should individual parts of this DPA be invalid, this shall not affect the validity of the remaining parts of this DPA.

Version 08-2023