

Appendix 2 - Agreement for data processing according to Art. 28 (3) GDPR

between

The customer

- hereinafter referred to as "Client" -

and

Timly Software AG, Talstrasse 58, 8001 Zurich, Switzerland

- hereinafter referred to as "Provider" -

together also called the "Parties".

1. Subject of the order

- 1.1. Within the scope of the Service Agreement, it is necessary for the Provider to handle personal data for which the Client acts as a controller within the meaning of Art. 4 No. 7 GDPR (hereinafter referred to as "Client Data"). This contract contains the provisions, in particular the rights and obligations of the parties under data protection law, regarding the handling of Client Data by the Provider for the performance of the Service Agreement. The order includes the services described in the service agreement.
- 1.2. The Provider shall process the Personal Data exclusively in a Member State of the European Union or in a state party to the Agreement on the European Economic Area, without prejudice to paragraph 3.
- 1.3. If the Provider processes Personal Data in a third country (i.e. outside the European Union/a state party to the Agreement on the European Economic Area), it shall require the prior written consent of the Client and shall only do so if and to the extent that the specific requirements of Art. 44 et seq. of the GDPR are met.

2. Information on the content of the order

- 2.1. The Provider shall process the Client Data exclusively on behalf of the Client (Section 1 (1) of this Agreement) and in accordance with the documented instructions of the Client within the meaning of Article 28 (3) a of the GDPR.
- 2.2. The Provider shall process the Client Data exclusively in the manner, to the extent and for the purposes that are conclusively necessary for the provision of the Service in accordance with the Service Agreement. The Provider is prohibited from processing the Client Data in any other way or for any other purpose, in particular from using the Client Data for its own purposes.

- 2.3. The Provider also processes the following sensitive data such as communication data (e.g. telephone, e-mail), contract master data (contractual relationship, product or contractual interest), Client history, contract billing and payment data, planning and control data, information data (from third parties, e.g. credit agencies, or from public directories) as well as names, first names and e-mail addresses insofar as these are stored by the Client.
- 2.4. The categories of persons affected by the processing on the part of the client include Clients, interested parties, subscribers, employees, suppliers, sales representatives, contact persons. The Provider shall document the processing of the categories of processing in a directory within the meaning of Article 28 (2) and shall make it available to the client in an appropriate manner upon request.

3. Client's authority to issue instructions, processing subject to instructions

- 3.1. The Client shall issue all instructions and orders in writing or in a documented electronic format. If the Client issues an instruction verbally, this must be confirmed immediately by the Client in writing or in a documented electronic format. The Client shall have a general right to issue instructions to the Provider regarding the type, scope and method of data processing used.
- 3.2. The data may be processed exclusively in accordance with the provisions of this Agreement and the instructions of the Client. The Provider is prohibited from using the data for other purposes and in particular from disclosing the data to third parties. No copies or duplicates may be made without the knowledge of the Client. Excluded from this are backup copies, insofar as these are required to ensure proper data processing, as well as all data required to comply with statutory retention obligations.
- 3.3. All changes to the subject matter and procedure of the processing shall be jointly agreed and documented. The Provider may disclose the personal data processed under this Agreement to third parties or the Data Subject only with the prior written consent of the Client.
- 3.4. If the Provider is of the opinion that an instruction of the Principal violates statutory data protection provisions, it shall notify the Principal thereof without undue delay. He may then suspend the execution of the instruction in question until it has been confirmed or amended by the Principal's representative.

4. Rights and obligations of the client

- 4.1. The client shall be solely responsible externally, in particular vis-à-vis third parties and data subjects, for assessing the permissibility of the processing of personal data pursuant to Article 6 (1) of the GDPR and for safeguarding the rights of data subjects pursuant to Articles 12-22 of the GDPR. The Provider is nevertheless obliged, to the extent permitted by law, to forward all requests by Data Subjects to the Client if they are recognizably directed at the Client. The Provider shall support the Client to a reasonable extent in responding to

requests from data subjects (e.g. correction, deletion and blocking of data) and shall be entitled to charge reasonable compensation for this.

- 4.2. The Client is the owner of the Client Data and, in the relationship between the Parties, the owner of all rights, if any, to the Client Data.
- 4.3. The Client shall be responsible for making the Client Data available to the Provider in a timely manner for the performance of services under the Service Agreement. Furthermore, the Client shall be responsible for the quality and the lawful collection of the Client Data. The Client shall inform the Provider immediately and in full if it discovers errors or irregularities with regard to data protection provisions or its instructions during the examination of the Provider's order results.
- 4.4. In the event that a third party or a data subject asserts a claim directly against the Provider due to violations of the data subject rights and/or related claims, the Client undertakes to indemnify the Provider for all damages, costs/fees, including legal fees, or other expenses or losses, arising from the claim, provided and to the extent that the Provider has informed the Client of the assertion of the claim and such infringement has not arisen as a result of processing operations contrary to the Client's instructions and has given the Client the opportunity to cooperate with the Provider in defending the claim.

5. Obligations of the Provider

- 5.1. The Provider is obliged to process personal data exclusively within the framework of the agreements made and in accordance with the Client's instructions. This shall not apply insofar as the Provider is obliged to process otherwise by the law of the Union or the Member States to which the Provider is subject (e.g. investigations by state authorities, law enforcement agencies). In this case, the Provider shall notify the Client of these legal requirements prior to the processing, unless the relevant law prohibits such notification due to an important public interest (cf. Art. 28 (3) sentence 2 lit. a GDPR).
- 5.2. The Provider shall not use the personal data provided by the Client for processing for any other purposes, in particular not for its own purposes. The Provider may not make any copies or duplicates of the Client Data without the prior written consent of the Client, to the extent that and as long as they are not required to ensure proper data processing, to properly provide the services in accordance with the Service Agreement (including data backup) or to comply with statutory retention obligations.
- 5.3. The Provider may also not disclose Client Data to third parties or other recipients without the prior written consent of the Client. This does not apply to the transfer of data to sub-Providers whose commissioning has been approved by the Client.
- 5.4. The Provider shall provide third parties or authorities with information on personal data from this contractual relationship, to the extent legally permissible, only after prior written or electronically documented instruction or consent by the Client.
- 5.5. If the Client is obliged to provide information about the Client Data or its processing to a government agency, a data subject or another person, the

Provider shall be obliged to support the Client in providing such information upon first request, in particular by immediately providing all information and documents about the contractual processing of Client Data including the technical and organizational measures taken by the Provider, about the technical process of using Client Data, the locations where Client Data are used and about the employees involved in the processing.

- 5.6. The Provider undertakes to cooperate to the necessary extent in the fulfillment of the rights of the data subjects pursuant to Art. 12-22 GDPR, in the preparation of the lists of processing activities, in any required data protection impact assessments of the Client, as well as in the compliance with the obligations of the Client with regard to the security of the processing and to provide the Client with appropriate support to the extent possible (cf. Art. 28 (3) sentence 2 lit. e, f GDPR).
- 5.7. The Provider shall be obliged to correct, delete or restrict the processing of personal data from this contractual relationship if the Client requests this by means of a written or electronically documented instruction and if legitimate interests of the Provider, in particular compliance with statutory provisions, do not conflict with this.
- 5.8. The Client and the Provider shall agree on the implementation of a change to the object of processing or a change to the procedure. The change shall be recorded in writing or in a documented electronic format.
- 5.9. The Provider shall be entitled to charge reasonable compensation for the acts of support under this § 5.
- 5.10. After completion of the contractually agreed work or earlier upon request by the Client - at the latest upon termination of the service agreement - the Contractor shall, at the Client's discretion, hand over to the Client or, after prior consent, destroy in a data-protection-compliant manner all documents, processing and utilization results created, as well as data files related to the contractual relationship that have come into its possession. The same shall apply to test and reject material. The record of the deletion shall be submitted upon request. Documentation which serves as proof of the orderly and proper processing of data shall be retained by the Contractor in accordance with the respective retention periods beyond the end of the contract. The Contractor may hand them over to the Client at the end of the contract in order to discharge the Contractor.

6. Technical and organizational measures

- 6.1. The Provider is obliged to implement and maintain during the term of the contract those technical and organizational measures that are necessary to ensure a level of protection for the specific commissioned processing that is appropriate to the risk to the rights and freedoms of the natural persons concerned by the processing. The protection objectives of Art. 32 (1) GDPR such as confidentiality, integrity and availability of the systems and services as well as their resilience in relation to the type, scope, circumstances and purpose of the processing operations shall be taken into account in order to minimize any risk during the term of the contract.

- 6.2. The data protection concept of the Ordering Party (Technical and Organizational Measures (TOM)) of Timly Software AG presents in detail the selection of measures suitable for the identified risk, taking into account the protection goals according to the state of the art and with special consideration of the IT systems and processing procedures used at the Ordering Party. The Client confirms that the technical and organizational measures provide an appropriate level of protection for the Client Data, taking into account the risks of the processing of the Client Data.
- 6.3. The technical and organizational measures are subject to technical progress and further development. In this respect, the Provider is permitted to implement alternative adequate measures. In doing so, the security level of the specified measures must not be undercut. Significant changes must be documented.

7. Correction, deletion and blocking of data

- 7.1. The Provider may correct, delete or block the data processed on behalf of the Client only in accordance with the Client's instructions.
- 7.2. Insofar as a data subject should contact the Provider directly for the purpose of correction or deletion of his/her personal data, the Provider shall forward this request to the Client.

8. Controls and other obligations of the Provider

The Provider will comply with the following:

- a) To the extent provided for by law, the Provider shall designate in writing a data protection officer who shall perform his or her activities in accordance with the legal requirements. The Data Protection Officer is appointed by the Provider (currently not provided for by law). The Client shall be informed immediately of any change of data protection officer.
- b) The Provider and any person subordinate to the Provider who has access to personal data of the Client may process such data exclusively in accordance with the instructions of the Client pursuant to Clause 9 of this Agreement, including the powers granted in this Agreement, unless they are required to process such data by the law of the European Union or the member states to which the Provider is subject. In such a case, the Provider shall notify the Client of such legal requirements, unless the relevant law prohibits such notification due to an important public interest.
- c) When carrying out the work, the Provider shall only use persons who are bound to confidentiality and who have been familiarized in advance with the data protection provisions relevant to them.

- d) Contracting authorities and Providers shall cooperate with the supervisory authority in the performance of their duties upon request.
- e) The Provider shall inform the Client without undue delay about control actions and measures of the supervisory authority insofar as they relate to this order. This shall also apply insofar as a competent authority is investigating the Provider in the context of administrative or criminal proceedings relating to the processing of personal data in the course of the Order Processing.
- f) The Provider shall support the Client to the extent that the Client is subject to an inspection by the supervisory authority, administrative offense or criminal proceedings, the liability claim of a Data Subject or a third party or any other claim in connection with the Order Processing at the Provider.
- g) The Provider shall regularly monitor its internal processes, as well as the technical and organizational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of applicable data protection law and that the protection of the rights of the Data Subject is guaranteed.
- h) The Provider shall provide evidence of the technical and organizational measures taken to the Client within the scope of its control powers pursuant to Section 7 of this Agreement.

9. Subcontracting relationships

- 9.1. Subcontracting relationships within the meaning of this regulation are those services which relate directly to the provision of the main service. This does not include ancillary services which the Provider makes use of, e.g. in the form of telecommunications services, postal/transport services or the disposal of data carriers. However, the Provider shall be obligated to enter into appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security of the Principal's data also in the case of outsourced ancillary services.
- 9.2. The Provider shall be entitled to use the sub-Providers listed in Annex 3 for the processing of Personal Data in order to perform the Order. The commissioning of further or other sub-Providers for the processing of the Client's personal data shall only be permitted after prior written information of the Client about the identity of the sub-Provider and the subject of the sub-processing, unless the Client objects to this change within a reasonable period of at least 10 working days. In all other respects the following shall apply:
- a) The transfer of personal data of the Client to the sub-Provider and its initial activity shall be permitted only after all the conditions for subcontracting have been met.

- b) If the SubProvider provides the agreed service outside the EU/EEA with the consent of the Principal pursuant to Section 2.1, the Provider shall ensure the admissibility under data protection law in accordance with the data protection regulations applicable to the performance of the contract.
- c) The sub-Provider shall be subject to the same data protection obligations by way of a contract as set forth in this Agreement, in particular providing sufficient guarantees that the appropriate technical and organizational measures will be implemented in such a way that the processing will be carried out in accordance with the legal requirements.

10. Control rights of the client

- 10.1. The Client shall have the right to carry out inspections in consultation with the Provider or to have such inspections carried out by auditors to be named in the individual case who are bound to professional secrecy. It shall have the right to satisfy itself of the Provider's compliance with this Agreement in its business operations by means of spot checks which must be notified in good time. The Provider may demand reasonable compensation for the expenses it incurs (e.g. working hours of the employees deployed).
- 10.2. The Provider shall ensure that the Client can satisfy itself of the Provider's compliance with its legal and contractual obligations. The Provider undertakes to provide the Client with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organizational measures.
- 10.3. Evidence of such measures, which do not only relate to the specific order, can be provided by current test certificates, reports or report extracts from independent bodies (e.g. auditors, auditing, data protection officers, IT security department, data protection auditors, quality auditors), suitable certifications (IT security or data protection audit, e.g. in accordance with "BSI-Grundschutz") or other measures provided for by law.

11. Support of the client, notification in the event of infringements by the Provider.

The Provider shall support the Client in complying with its obligations to protect and secure personal data as provided for by law and shall document this in an appropriate manner. This includes:

- a) ensuring an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing as well as the predicted likelihood and severity of a possible breach of rights due to security vulnerabilities, and allow for immediate detection of relevant breach events,
- b) the obligation to document breaches of the protection of personal data and to report them to the Client without undue delay. The Provider shall, in

agreement with the Client, take appropriate measures to secure the data and minimize any potential adverse effect on the data subjects,

- c) the obligation to support the Client by taking appropriate measures, insofar as the Client is required to notify the competent supervisory authority or the data subject of the personal data breach,
- d) the obligation to support the Client within the scope of its duty to inform the data subject and, in this context, to provide him with all relevant information without delay upon request.

12. Miscellaneous and final provisions

12.1. The term of this agreement corresponds to the term of the service agreement. The provisions on ordinary termination of the service agreement shall apply accordingly. Termination of the Service Agreement shall automatically result in termination of this Agreement. Isolated termination of this Agreement is excluded.

12.2. Should any present or future provision of the agreement be or become invalid or unenforceable in whole or in part, or should there be a loophole in this agreement, this shall not affect the validity of the remaining provisions. In place of the invalid or unenforceable provision, the valid provision shall be deemed agreed which comes closest to the economic sense and purpose of the invalid or unenforceable provision. In the event of a loophole, that provision shall be deemed agreed which corresponds to what would have been agreed in accordance with the economic sense and purpose of this agreement if the parties had considered the loophole from the outset.

12.3. The Parties undertake to amend and/or supplement this Agreement at the request of a Party if this becomes necessary due to a change in the data protection laws applicable to the Parties or because the European Commission and/or the supervisory authorities responsible for the Parties indicate through general statements or publications (e.g. by providing standard contractual clauses pursuant to Art. 28 (7), (8) of the GDPR) or in the form of declarations or orders in individual cases that this Agreement in its existing form does not meet the requirements of the applicable data protection laws.

02/2022, Timly Software AG

datenschutz@timly.ch