Order Processing Contract

bexio AG

This Order Processing Contract (hereinafter, the "OPC") specifies the data protection obligations that arise from the contractual relationship between bexio AG (hereinafter, the "Provider") and its customers (hereinafter, the "Client"). The contractual relationship between the Parties is based on the General Terms and Conditions (hereinafter, the "GTC") and the Privacy Policy (hereinafter, the "PP") and therefore, these are an integral part of the OPC. The OPC shall apply to all activities arising from the contractual relationship between the Parties in which employees of the Provider or third parties commissioned by the Provider process the Client's personal data (hereinafter, the "Data"). The Client may contact the Provider's Data Protection Officer at datenschutz@bexio.com for any data protection issues that may arise.

1. Subject matter, duration and specification of the order processing

1.1. The subject matter and duration of the order as well as the type and purpose of the processing shall generally be determined by the GTC, unless the following provisions impose additional obligations.

1.2. Annex A to the OPC specifies the subject matter, nature and purpose of the order processing.

2. Scope of application and responsibility

2.1. The Provider processes personal data on behalf of the Client. This includes activities that are specified in the GTC, the Privacy Policy, in Annex A to the OPC and in the current service description on the Provider's website.

2.2. In the context of the contractual relationship, the Client is solely responsible for compliance with the legal provisions of the data protection laws, in particular for the legality of the transfer of data to the Provider as well as for the legality of the data processing.

2.3. By filling out the login screen when registering and by ordering a user account (the "bexio account") on the Provider's website, the Client gives the Provider the corresponding instruction for data processing. The Client may amend, change or withdraw its instructions in its bexio account or by notifying the Provider. Instructions that are not provided for in the GTC shall be treated as a request for a change of service. The Client must immediately follow up on verbal instructions in writing or by making the appropriate entries in the bexio account.

3. Obligations of the Provider

3.1. The Provider processes the data of data subjects only within the context of the contractual relationship in accordance with the GTC, the Privacy Policy and this OPC, unless there is an exceptional case regulated by law.

3.2. The Provider shall design the internal organization within its area of responsibility in such a way that it meets the special data protection requirements. The Provider shall take the appropriate technical and organizational measures to protect the Client's data in accordance with the respective legal requirements. In particular, these measures shall continuously ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with the processing. The Client is aware of these technical and organizational measures and is responsible for ensuring that they provide an adequate level of protection for the risks related to the data to be processed.

3.3. The measures taken by the Provider are specified in Annex B. 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 at any time. In doing so, the security level contractually agreed upon in the GTC must be maintained.

3.4. To the extent agreed, the Provider shall support the Client within the scope of its possibilities in fulfilling the requests and claims of data subjects under data protection law and in complying with the obligations under data protection law. In accordance with the GTC, the Provider is entitled to demand an expense allowance for this support.

3.5. The employees involved in the processing of the Client's data and other third parties working for the Provider shall process the data exclusively within the context of the contractual relationship in accordance with the GTC, the Privacy Policy and this OPC and are obliged to maintain confidentiality.

3.6. If the Provider becomes aware of any violation of the protection of personal data, it shall take reasonable measures to secure the data and to mitigate any possible adverse consequences for the data subjects. In addition, the Provider shall fully comply with the applicable legal provisions regarding the notification of data protection violations.

3.7. The Provider shall fully comply with the applicable data protection provisions and shall regularly review the effectiveness of the technical and organizational measures to ensure the security of the processing.

3.8. The Provider shall process and store personal data for as long as the contractual relationship between the Provider and the Client exists. The Provider shall rectify or erase the contractual data if the Client instructs it to do so and if this is covered by the scope of the instructions. This provision shall not apply to data that is required for further processing due to legal regulations or for compelling internal purposes. The release of the data and the corresponding remuneration is regulated in the GTC.

4. Obligations of the Client

4.1. The Client shall inform the Provider immediately and in full in writing or via the bexio account if it discovers errors or irregularities in the order results with regard to data protection regulations.

4.2. The Client shall give the Provider the name of the contact person for any data protection issues arising within the context of the contractual relationship, if this person is not the same as the designated contact person.

4.3. The Client declares that it is solely responsible for informing the data subjects whose data is being processed regarding the possible storage, use, processing and transfer of their data by the Provider in accordance with the provisions in the GTC, the Privacy Policy and this OPC. If individual data subjects do not agree with the intended data processing, the Client shall be responsible for erasing the respective data in its bexio account.

4.4. By accepting the GTC and the Privacy Policy, the Client **expressly agrees to the transfer of its data to the Provider's parent company and affiliated companies**. The Client releases the Provider from any possible claims. The Client is responsible for obtaining the consent of the data subjects.

5. Inquiries by data subjects

5.1. If a data subject contacts the Provider with a request for rectification, erasure or information, the Provider shall refer the data subject to the Client, provided that an assignment to the Client is possible according to the data subject's information. The Provider shall forward the data subject's request to the Client within a reasonable period of time. The Provider may support the Client in the event of claims of a data subject under data protection law within the scope of its capabilities. In this case, the Provider shall be entitled to demand compensation for expenses. The Provider is not liable if the Client does not respond to the data subject's request or does not respond to it correctly or in a timely manner.

6. Evidence

6.1. The Provider shall furnish evidence to the Client of its compliance with the obligations set forth in this Annex by appropriate means. This shall be done by means of a self-audit and/or ISO certification.

6.2. If, in individual cases, inspections by the Client or an auditor commissioned by the Client are necessary (e.g., due to subordination to GDPR), such inspections will be carried out during normal business hours without disrupting the Provider's operations, after the Client has notified the Provider, taking into account an appropriate lead time. The Provider may make such inspections dependent on prior notification with a reasonable lead time and on the signing of a confidentiality agreement concerning the data of other customers and the established technical and organizational measures. If the auditor appointed by the Client is in a competitive relationship with the Provider, the Provider may reject the auditor and propose a neutral person. The Provider may charge any costs associated with the audit to the Client, especially if no irregularities have been found.

6.3. If a data protection supervisory authority or any other sovereign supervisory authority of the Client carry out an inspection, Section 6.2 shall generally apply accordingly. It shall not be necessary to sign a confidentiality agreement if this supervisory authority is subject to professional or statutory confidentiality where a violation is punishable under the Swiss Criminal Code.

7. Subcontractors (other processors)

7.1. The Provider may engage subcontractors to perform the contractual services. The Provider may commission subcontractors as processors provided that these subcontractors in turn fulfill the requirements of this OPC to the extent of the subcontract. The Provider shall enter into agreements with the subcontractors to the extent necessary to ensure appropriate data protection and information security measures. Subcontractors that do not have access to customer data or do not process personal data as processors are excluded from this section. A list of current subcontractors in the sense of a processor (hereinafter referred to simply as "subcontractors") is available here:
https://www.bexio.com/en-CH/policies/subcontractor

7.2. The Client agrees that the Provider may use the subcontractors listed on the Provider's website. Before using additional subcontractors, the Provider shall inform the Client by updating the Provider's website. The overview on the website must be updated at least 14 days before the subcontractor is called in. The Client shall regularly check the overview. The Client may object to the change within 14 days from the date of notification for good cause. If no objection is made within this period, the change shall be deemed to have been approved. If there is a good cause under data protection law, and if an amicable solution cannot be found between the parties, the Provider shall be granted a right of special termination.

8. Duty to inform

8.1. The Provider shall inform the Client immediately if the Client’s data stored with the Provider is in danger of seizure or attachment, by insolvency or composition proceedings or by other events or measures of third parties. The Provider shall immediately inform all responsible parties in this context that the sovereignty and ownership of the data lies exclusively with the Client.

9. Liability

9.1. Liability is governed by the relevant provisions in the GTC.

10. Miscellaneous provisions

10.1. In all other respects, the provisions in the GTC and the Privacy Policy shall apply. In the event of any contradictions between the OPC and the GTC, the provisions in the GTC shall take precedence. Should individual parts of the OPC be invalid, this shall not affect the validity of the GTC and the remaining provisions of the OPC.

10.2. Annexes A and B are an integral part of the OPC.

Last version: June 2022

bexio AG

Alte Jonastrasse 24
8640 Rapperswil
Switzerland

Annex A	Subject Matter, Nature and Purpose
Annex B	Technical and Organizational Measures (TOM)

Annex A – Subject Matter, Nature and Purpose

Subject matter of the order:	The processing of the Client’s personal data within the context of the Client’s use of the Provider’s services as Software as a Service.
Nature and purpose of the intended data processing:	The Client’s personal data shall be transferred to the Provider for processing within the context of the Software as a Service services. The Provider shall process this data exclusively in accordance with the GTC and the corresponding service description on the Provider’s website (order management, contact management (CRM), accounting, online banking, payroll accounting, warehouse management, project management, etc.).
Types of personal data:	The types of data depend on the data provided by the Client. These are in particular (depending on the Client’s order): ● Personal master data (name, date of birth, address, employer) including contact data (e.g., telephone, email) ● Contract data, including billing and payment data ● History of contract data
Categories of data subjects:	The categories of data subjects depend on the data provided by the Client. These are in particular (depending on the Client’s order): ● Employees (including job applicants and former employees) of the Client ● Customers of the Client ● Interested parties of the Client ● Service providers of the Client ● Contact details of contact persons
Erasure, blocking and rectification of data:	Requests for erasure, blocking and rectification must be directed to the Client; otherwise, the provisions of the GTC, of the Privacy Policy and in this OPC shall apply.

Annex B - Technical and Organizational Measures (TOM)

The following technical and organizational measures (TOM for short) are fundamental to data processing:

I. Access control

- Designation of security areas
- Implementation of effective access protection
- Designation of persons authorized to access the data
- Management and documentation of personal access authorizations over the entire life cycle
- Monitoring of premises after business hours
- Logging of access

II. Access control:

- Access protection (authentication)
- Simple authentication of employees (via user name/password) with a high level of protection
- Blocking in case of failed attempts/inactivity and a process for resetting blocked access IDs
- Designation of authorized persons
- Management and documentation of personal authentication media and access authorizations
- Automatic access blocking
- Manual access blocking
- Secured transfer of authentication secrets (credentials) in the network
- Logging of access

III. Data entry control:

- Creation of an authorization concept
- Implementation of restrictions on entering data
- Assignment of minimum authorizations
- Administration and documentation of personal data entry authorizations
- Logging of data entry

IV. Transport / forwarding control:

- Secure data transfer between server and client
- Securing the transfer in the backend
- Securing transfer to external systems
- Implementation of security gateways at network transfer points
- Hardening of the backend systems
- Description of all interfaces and transmitted personal data fields
- Machine-to-machine authentication
- Data medium management (process)
- Process for collection and disposal
- Data protection-compliant erasure/destruction process

V. Input control:

- Automatic documentation of input authorizations
- Logging of inputs

VI. Order control:

- Documentation of input authorizations
- Logging of inputs

VII. Availability control:

- Backup concept
- Emergency plan
- Storage of backups
- Testing of emergency systems

VIII. Separation requirement:

- Economy in data collection
- Separate processing