Order Processing Contract

bexio AG

This order processing contract specifies the obligations regarding data protection that arise from the contractual relationship between bexio AG (hereinafter the "Provider" or "Order Processor") and its customers (hereinafter the "Client" or "Data Controller"). For all data protection questions, the Client can contact the Provider's Data Protection Officer via datenschutz@bexio.com.

1. Subject matter

1.1. A legal relationship exists between the Parties for the execution of which personal data is transferred from the Data Controller to the Order Processor (the "main contract"). The legal relationship between the Parties is based on the Provider's General Terms and Conditions ("GTCs"). This order processing contract is concluded between the Parties in order to ensure adequate protection for the transfer of personal data.

1.2. Unless otherwise provided in this Agreement, all terms shall have the same meaning as in the Swiss Data Protection Act ("DPA"). Furthermore, this Agreement supports the Parties in complying with the EU General Data Protection Regulation ("GDPR") as far as protected personal data of customers from the EU area is concerned in this respect.

2. Description of the data processing

2.1. The Provider processes personal data on behalf of the Client. The subject matter and duration of the contractual relationship as well as the nature and purpose of the processing result in principle from the General Terms and Conditions and Annex A to the Order Processing Contract. The data processing is also specified in the current service description on the Provider's website and in the data protection declaration ("DSE").

2.2. By filling in the registration form for the registration and ordering of a user account ("bexio account") on the Provider's website, the Client gives the Provider the corresponding instructions for data processing. The Client may add to, change or withdraw their instructions in their bexio account or by notifying the Provider. Instructions that are not provided for in the General Terms and Conditions are treated as a request for a change in service. Oral instructions must be obtained immediately in writing or by corresponding action in the bexio account by the Client.

3. Obligations of the Client

3.1. Within the framework of the contractual relationship, the Client is solely responsible for compliance with the statutory provisions of data protection laws, in particular for the legality of data transfer to the Provider and for the legality of data processing.

3.2. The Client is satisfied that the technical and organisational measures ("TOM") implemented by the Order Processor and described in Annex B are sufficient to ensure adequate data protection for the personal data transferred.

3.3. The Client must inform the Provider immediately and in full in writing or via the bexio account if they detect errors or irregularities in the order results with regard to data protection regulations.

3.4. The Client shall inform the Provider of the contact person for data protection issues arising within the framework of the contractual relationship, if this differs from the contact person named.

3.5. The Client declares that they bear sole responsibility for informing the persons affected by the data processing regarding the possible storage, use, processing and forwarding of data by the Provider in accordance with the provisions in the GTC, the DSE and this order processing contract. If individual data subjects do not agree with the intended data processing, the Client is responsible for deleting the respective data in their bexio account.

3.6. By accepting the General Terms and Conditions and the order processing contract, the Client expressly declares **their consent to the transfer of their 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 subject.

4. Obligations of the Provider

4.1. General information

4.1.1. With regard to the processing of personal data, the Order Processor warrants that they

- will process this personal data in accordance with this order processing contract and exclusively for the purposes pursued by the Data Controller,
- the purposes pursued by the Data Controller result from Annex A, from the bexio account or from the explicit instructions of the Data Controller or are determined by another agreement with the Data Controller,
- will provide the Data Controller with the information necessary to monitor compliance with the obligations set out in this Agreement,
- take into account the principles of data privacy by design and by default in their work tools, products, applications or services,
- will inform the Data Controller if they can no longer or are unlikely to be able to comply with this Agreement, and
- will cooperate with the competent supervisory authorities to the extent permitted by law.

4.1.2. Persons authorised to issue instructions by the Data Controller will be notified to the Order Processor at the beginning of order processing in writing or in the bexio account. In the event of a change or long-term incapacity of the contact person, the Provider must be informed immediately in writing or in the bexio account of the successor or the substitute. Oral instructions are only binding if confirmed directly in writing by the person responsible. Email is sufficient for compliance with the written form.

4.1.3. The Provider must inform the Client immediately if they are of the opinion that an instruction violates legal regulations. The Provider is entitled to suspend the implementation of the relevant instruction until its legality is confirmed by the Data Controller or the instruction is amended.

4.2. Data security

4.2.1. The Provider shall organise the internal organisation within its area of responsibility in such a way that it meets the special requirements of data protection. It shall take technical and organisational measures for the adequate protection of the Client's personal data that meet the respective legal requirements. In doing so, the Order Processor has taken into account the state of the art, the implementation costs and the type, scope and purposes of the processing as well as the probability of occurrence and severity of the risk to the fundamental and personal rights of data subjects. The measures are described in Annex B and are reviewed periodically. Changes to the measures are permissible provided that the previous safety level is not undercut. The Client is aware of these technical and organisational measures and is responsible for ensuring that they offer an adequate level of protection for the risks of the data to be processed.

4.2.2. In carrying out the work, the Provider will only use employees who are obliged to maintain confidentiality and who have previously been familiarised with the data protection provisions relevant to them.

4.2.3. To the extent agreed, the Provider shall support the Client within the scope of their means 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 General Terms and Conditions, the Provider is entitled to demand an expense allowance for this.

4.2.4. If the Provider becomes aware of any breach of the protection of personal data, they shall take reasonable measures to secure the data and to mitigate any possible adverse consequences for the data subjects. Furthermore, the Provider fully complies with the applicable legal provisions regarding the reporting of data protection violations.

5. Subcontractors (other order processors)

5.1. The Provider may engage subcontractors to perform the contractual service. The Processor may only delegate the processing to a third party with the prior consent of the Data Controller. The commissioning of subcontractors as order processors by the Provider is permissible insofar as they in turn fulfil the requirements of this Order Processing Contract to the extent of the subcontract. To the extent necessary, the Provider shall enter into agreements with the subcontractors in order to ensure adequate data protection and information security measures. Subcontractors who do not have access to personal data or do not process personal data as Order Processors are excluded from this section. A list of the current subcontractors in the sense of an Order Processor (hereinafter, for the sake of simplicity, referred to only as "subcontractors") is available here:

https://www.bexio.com/de-CH/richtlinien/subunternehmer

5.2. The Client agrees that the Provider may use the subcontractors named on the Provider's website. Before consulting other subcontractors, the Provider shall inform the Client by updating their website. The overview on the website must be updated at least 14 days before each consultation. The Client shall consult the overview on a regular basis. The Client may object to the change for good cause within 14 days of becoming aware of it. If there is no objection within this period, approval to the change shall be deemed as given. If there is an important reason under data protection law and if a mutually agreeable solution cannot be found between the Parties, then the Provider shall be granted a special right of termination.

5.3. As a rule, ancillary services for the Provider without reference to the data of the Data Controller pursuant to Annex A (e.g., telecommunications services, postal/transport services, maintenance and user services or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software) shall not be deemed subcontracted processing. However, the Provider is obliged to take appropriate control measures to ensure data protection and data security of the Client's data, also in the case of ancillary services.

6. Transborder disclosure

6.1. The processing of the data in accordance with Annex A shall in principle take place in Switzerland or in a Member State of the European Union or in another state that is party to the Agreement on the European Economic Area. Any relocation to another third country may only take place if the relevant legal requirements are met.

6.2. If the Order Processor uses subcontractors in countries that do not have an adequate level of data protection according to the Federal Data Protection and Information Commissioner, the Annex to the VDSG or the EU Commission, then the Order Processor shall ensure that the disclosure is admissible under data protection law by taking appropriate measures commensurate with the respective data transfer.

7. Rights of data subjects

7.1. If a data subject approaches the Provider with requests for correction, deletion or information, the Provider will 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 request of the data subject to the Client within a reasonable period of time. The Provider may support the Client in the event of data protection claims by a data subject within the scope of their means. In this case, the Provider is entitled to demand an expense allowance. The Provider shall not be liable if the Client does not respond to the request of the data subject, does not respond correctly or does not respond in due time.

8. Verification options

8.1. The Provider shall demonstrate to the Client compliance with the obligations set out in this Annex by appropriate means. This is implemented through a self-audit and/or ISO certification.

8.2. If, in individual cases, inspections by the Client or an auditor commissioned by the Client are necessary (e.g., due to subordination to the GDPR), these shall be carried out during normal business hours without disrupting operations after notification and taking into account a reasonable lead time. The Provider may make them subject to prior notification with a reasonable lead time and after the signing of a confidentiality agreement with regard to the data of other customers and the technical and organisational measures set up. If the auditor commissioned by the Client is in a competitive relationship with the Provider, the Provider may reject this and propose a neutral person. The Provider may charge the Client for any costs associated with the audit, in particular if no irregularities could be detected.

8.3. Should a data protection supervisory authority or any other sovereign supervisory authority of the Client carry out an inspection, this chapter shall apply accordingly. A confidentiality agreement shall not be necessary if this supervisory authority is subject to professional or legal secrecy, in which a violation is punishable under the Criminal Code.

9. Information obligations

9.1. Should the Client's data held by the Provider be at risk as a result of seizure or confiscation, bankruptcy or insolvency proceedings or other events or measures taken by third parties, the Provider shall inform the Client of this without delay. The Provider shall inform all persons responsible in this context without delay that the sovereignty and ownership of the data lie exclusively with the Client.

10. Duration and termination

10.1. The Provider processes and stores personal data for as long as the contractual relationship between the Provider and the Client exists. The Provider shall correct or delete the contractual data if the Client instructs this and this is covered by the framework of instructions. This does not apply to data that is required for further processing due to legal regulations or for mandatory internal purposes. The Provider is entitled to suspend the implementation of any abusive instructions until their legality is proven. The disclosure of the data and the corresponding remuneration is regulated in the General Terms and Conditions.

11. Liability

11.1. Liability is based on the corresponding provisions in the General Terms and Conditions.

12. Miscellaneous

12.1. In all other respects, the provisions of the General Terms and Conditions and DSE shall apply. In the event of any contradictions between the Order Processing Agreement and the General Terms and Conditions, the provisions in the General Terms and Conditions shall prevail. Should any part of the order processing contract be invalid, this shall not affect the validity of the General Terms and Conditions and the remaining provisions of the order processing contract.

12.2. Annex A and Annex B are essential components of this order processing contract.

Last version: September 2023

bexio AG

Alte Jonastrasse 24
8640 Rapperswil
Switzerland

Annex A	Subject matter, nature and purpose
Annex B	Technical and organisational measures (TOM)

1. Annex A – Subject matter, nature and purpose

Purpose of the Contract:	Processing of the Client's personal data within the scope of their use of the Provider's services as software as a service.
Nature and purpose of the intended data processing:	The personal data processed by the Client will be transferred to the Provider within the scope of the software-as-a-service services. The Provider processes this data exclusively in accordance with the General Terms and Conditions and the corresponding service description on the Provider's website (order management, contact management (CRM), accounting, e-banking, payroll, warehouse management, project management, etc.).
Type of personal data:	The types of data depend on the data transmitted by the Client. These include, in particular, (depending on the 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 the contract data
Categories of data subjects:	The categories of data subjects depend on the data transmitted by the Client. These include, in particular, (depending on the order): ● Employees (including applicants and former employees) of the Client ● The Client's customers ● Prospective customers of the Client ● The Client's service provider ● Contact details for contact persons
Deletion, blocking and correction of data:	Enquiries for deletion, blocking and correction must be addressed to the Client; in all other respects, the provisions of the General Terms and Conditions, the DSE and the present Order Processing Contract shall apply.

2. Annex B – Technical and organisational measures (TOM)

I. Access control:

Measures to deny unauthorised persons access to data processing systems with which personal data is processed or used:

- Alarm system
- Automated access control
- Photoelectronic sensors / motion detectors
- Key management (key issuance, etc.)
- Chip cards / transponder closure system
- Manual locking system (use that is limited to key persons in the event of errors in access control systems)
- Video surveillance in the entrance area
- Wearing of a visible and mandatory badge
- Definition of security areas
- Determination of authorised persons
- A separate and documented control for access to data centres and server rooms only for specially authorised personnel is implemented. Access by authorised personnel is logged with name and card or token number. There are separate access controls for data centres.

II. Access control:

Measures to prevent the use of data processing systems by unauthorised persons:

- Assignment of user rights
- Password assignment
- Authentication with username / password / MFA
- Automatic suspension of access rights
- Manual suspension of access rights
- Logging of access
- Use of hardware firewalls
- Use of user profiles
- Additional measures: web application firewalls, regular vulnerability scans, regular penetration testing, patch management, minimum requirements for password complexity and forced password changes, use of virus scanners.

- Assignment of user profiles to IT systems
- Use of VPN technology
- Encryption of mobile storage media
- Use of mobile device management (for example: remote locking and wiping of smartphones)
- Hardware encryption for notebooks

III. Access control:

Measures to ensure that those authorised to use a data processing system can only access the data subject to their access authorisation, and that personal data cannot be unauthorised, read, copied, changed or removed during processing, use and after storage:

- Creation of an authorisation concept (identity access management)
- Reduction of the number of administrators to an "absolute minimum"
- Assignment of minimum permissions
- Implementation of access restrictions
- Secure media clean-up before reuse
- Hardware encryption (backup tapes, notebooks)
- Rights management by system administrators
- Password policy with requirements for password length, password change management
- Secure storage of data carriers

IV. Disclosure controls

Measures to ensure that personal data cannot be read, copied, changed or removed without authorisation during electronic transmission or during transport or storage on data media, and that it can be checked and determined to which parties personal data is to be transmitted by data transmission devices:

- Creation of a leased line or a VPN connection
- Encryption (backup for off-site storage)
- TLS encryption for all communications (web client, APIs, mobile apps)
- Securing the transmission in the backend
- Securing the transmission to external systems
- Implementation of security gateways at the network transfer points
- Hardening of the backend systems
- Description of all interfaces and the transmitted personal data fields

- Machine-machine authentication
- Data protection-compliant deletion/destruction procedure

V. Input control

Measures to ensure that it can be subsequently checked whether and by whom personal data can be entered, changed or removed in data processing systems:

- Rights assignment for input, modification and deletion of data based on an authorisation concept
- Automatic documentation of input permissions
- Logging of inputs

VI. Availability controls

Measures to ensure that personal data is protected against accidental destruction or loss:

- Uninterruptible power supply (UPS)
- Devices to monitor temperature and humidity in server rooms
- Fire and smoke detection systems
- Alerting if unauthorised access to server rooms takes place
- Creation of backup & recovery concepts
- Creation of data backups
- Testing of data recovery
- Secure off-site storage of data backups
- Air conditioning systems in server rooms
- Extinguishing systems in server rooms
- Emergency plan
- Storage of backups
- Testing of emergency facilities

VII. Requirement of separation

Measures to ensure that personal data collected for different purposes is processed separately:

- Creation of an authorisation concept
- Approved and documented database rights
- Logical client separation (at software level)
- Separation of productive and test systems

- Economy in data collection