Annex “Commissioned Processing” to the General Terms and Conditions

Commissioned Processing Agreement

between

the customer

–Client–

and

bexio AG

Alte Jonastrasse 24

8640 Rapperswil

Switzerland

–Provider–

Preamble

The Annex specifies the data protection obligations of the Contracting Parties resulting from the Contract concluded between the Parties (General Terms and Conditions of the Provider). It applies to all activities in connection with the Contract and the processing of the Client’s personal data (hereinafter referred to as “Data”) by the employees of the Provider or persons commissioned by the Provider.

1 Subject Matter, Duration, and Specification of Commissioned Processing

(1) The details regarding the Provider’s services are regulated in the respective Contract between the Provider and the Client (hereinafter referred to as the “Contract”). The Contract consists of the Provider’s General Terms and Conditions.

(2) The Contract shall specify the subject matter and duration of the commission along with the nature and purpose of the processing unless specified otherwise in Appendix A.

(3) The term of the Annex is based on the term of the Contract provided that the provisions of the Annex do not give rise to obligations in excess hereof.

2 Scope and Responsibility

(1) The Provider shall process the Data specified in Appendix A on behalf of the Client for the purpose and to the extent stated therein. This shall include the activities that are specified in the Contract.

(2) Within the framework of the Contract, the Client shall be solely responsible for compliance with the legal provisions of data protection laws, in particular for the legality of data transmission to the Provider and for the legality of data processing.

(3) The instructions shall be initially defined in the Contract and may further be modified, supplemented, or replaced by the Client in writing or in an electronic format (text form) and shall be sent to the body designated by the Provider on individual instructions (individual instructions). Instructions that are not provided for in the Contract shall be treated as a request for a change in service. The Client shall immediately follow up on verbal instructions in writing or in text form.

3 Obligations of the Provider

(1) The Provider may only process the Data of data subjects within the scope of the commission and on the instructions of the Client unless there is an exceptional case regulated by law. The Provider shall inform the Client immediately if the Provider believes that an instruction violates any applicable laws. The Provider may suspend the implementation of the instruction until it has been confirmed or amended by the Client.

(2) The Provider shall structure the internal organization in its area of responsibility in such a way that it meets the special requirements of data protection. The Provider shall take technical and organizational measures that meet the respective legal requirements so as to adequately protect the Client's Data. The Provider shall take technical and organizational measures to ensure the confidentiality, integrity, availability, and resilience of the systems and services in connection with the processing in the long term. The Client shall be aware of these technical and organizational measures and shall be responsible for ensuring that they offer an appropriate level of protection against any risks for the Data to be processed.

(3) The measures taken by the Provider are described in more detail in Appendix B. The technical and organizational measures shall be subject to technical progress and further development. In this respect, the Provider shall be permitted to implement alternative adequate measures. The security level of the defined measures shall not be undershot. Major amendments shall be documented.

(4) To the extent agreed, the Provider shall support the Client, within the scope of its abilities, in satisfying the requests and claims of data subjects and in complying with the data protection obligations.

(5) The Provider guarantees that the employees involved in the processing of the Client's Data and other persons working for the Provider are prohibited from processing the Data outside the instructions. Furthermore, the Provider guarantees that the persons authorized to process personal Data have undertaken to maintain confidentiality or are subject to an appropriate statutory obligation of confidentiality. The confidentiality/non-disclosure obligation shall continue to apply even after the completion of the commission.

(6) The Provider shall inform the Client immediately if the Provider becomes aware of any breaches of the Client's personal Data protection. The Provider shall take the necessary measures to secure the Data and to mitigate possible adverse consequences for data subjects, and shall consult with the Client without delay.

(7) The Provider shall provide the Client with the following contact person for any data protection issues arising within the framework of the Contract: the data protection officer of bexio AG, datenschutz@bexio.com.

(8) The Provider undertakes to comply with its respective data protection obligations and to implement a procedure for the regular review of the effectiveness of the technical and organizational measures so as to ensure the security of the processing.

The Provider shall correct or delete the contractual Data if this is instructed by the Client and included in the instruction framework. Should the deletion in conformity with data protection or the corresponding restriction of Data processing be impossible, the Provider shall undertake the destruction of data carriers and other materials in conformity with data protection on the basis of a specific assignment by the Client or shall return these data carriers to the Client unless already agreed in the Contract.

In special cases to be determined by the Client, these shall be retained or handed over. The compensation and protective measures for these purposes shall be agreed separately unless already agreed in the Contract.

(9) Data, data carriers, and all other materials shall either be surrendered or deleted at the request of the Client following the completion of the commission. Any additional costs arising due to deviating specifications in the surrender or deletion of Data shall be borne by the Client.

(10) Should a claim be raised by a data subject against the Client in connection with the commissioned processing, the Provider undertakes to support the Client in defending the claim within the scope of its abilities.

(11) The Provider shall be compensated for services provided pursuant to Section 3, 5, 6(2) and 6(3) (e.g. surrendering the data carriers, contacting data subjects, or carrying out the reviews) according to its current hourly rates or external expenses.

4 Obligations of the Client

(1) The Client shall inform the Provider immediately and to the full extent of any errors or irregularities with regard to data protection regulations detected in the results of commissioned processing.

(2) The Client shall provide the Provider with the contact person for any data protection issues arising within the scope of the Contract if the contact person is different from the contact person already named by the Client.

5 Requests of Data Subjects

Should a data subject contact the Provider with requests for correction, deletion, or information, the Provider shall refer the data subject to the Client provided that the assignment to the Client is possible according to the information provided by the data subject. The Provider shall immediately forward the request of the data subject to the Client. The Provider shall support the Client within the scope of its abilities and on instruction, to the extent agreed. The Provider shall not be liable if the request of the data subject is not addressed by the Client or if it is not addressed properly or in due time.

6 Capabilities to Provide Evidence

(1) The Provider shall provide the Client with appropriate evidence of compliance with the obligations laid down in the Annex. This takes place through a self-audit and/or certification according to ISO 27001.

(2) Should inspections be necessary in individual cases as requested by the Client or an auditor commissioned by the Client, they shall be carried out during normal business hours without disrupting operations, following notification and taking into account reasonable lead time. The Provider may make this contingent upon prior notification with reasonable lead time and upon the signing of a confidentiality agreement with regard to the Data of other customers and the established technical and organizational measures. Should the auditor commissioned by the Client be in a competitive relationship with the Provider, the Provider shall have the right of objection against the auditor.

(3) Should an inspection be carried out by a data protection supervisory authority or another sovereign supervisory authority of the Client, Paragraph 2 shall apply accordingly. The signing of a confidentiality agreement is not requited if the supervisory authority is subject to professional or statutory secrecy where a violation is punishable under the Criminal Code.

7 Subcontractors (Additional Commissioned Processors)

(1) The commissioning of subcontractors by the Provider is permissible as long as they meet the requirements hereof within the scope of the subcontract. A list of the current subcontractors can be found here:
https://www.bexio.com/de-CH/richtlinien/subunternehmer

(2) The Client agrees that the Provider may engage subcontractors. The Provider shall inform the Client before engaging or replacing the subcontractors. The Provider is obliged to inform the Client of the assignment of a subcontractor by updating the above list. The list shall be updated at least 14 days in advance. The Client shall review the list on a regular basis. The Client may object to the change – within 14 days – for an important reason with the Provider. Should there be no objection within the specified time period, the consent to the change shall be deemed given. If there is an important reason under data protection law and if an amicable solution cannot be found between the Parties, the Provider shall be granted a special right of termination.

(3) A subcontractor relationship requiring approval shall exist if the Provider commissions further providers to render all or part of the service agreed in the Annex. The Provider shall enter into agreements with these third parties 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 customer Data shall be excluded from this Chapter and shall therefore not be included in the said list.

(4) Should the Provider place orders with subcontractors, the Provider shall be responsible for transferring its data protection obligations from the Annex to the subcontractor.

8 Obligations to Provide Information

The Provider shall inform the Client immediately should the Client's Data be at risk with the Provider through seizure or attachment, through insolvency or composition proceedings, or

through other events or measures of third parties. The Provider shall immediately inform all Responsible Persons in this context that the sovereign rights to and ownership of Data lies exclusively with the Client as the "Responsible Person" within the meaning of the General Data Protection Regulation.

9 Liability

The liability shall be governed by the Contract.

10 Miscellaneous

(1) In all other respects, the provisions of the Contract shall apply. In the event of any contradictions between the provisions of the Annex and the provisions of the Contract, the Annex shall take precedence. Should any part of the Annex be invalid, this shall not affect the validity of the Contract and the remaining provisions hereof.

(2) Appendix A and Appendix B shall be integral part hereof.

Appendix A to the Commissioned Processing Agreement

Subject matter of the commission:	Processing of the Client's personal Data within the scope of its use of the Provider's services as Software as a Service.
Type and purpose of the intended Data processing:	Personal data processed by the Client shall be transmitted to the Provider within the scope of the Software as a Service services. The Provider shall process the Data only according to the agreement made (commission management, customer relationship management (CRM), accounting, e-banking, payroll accounting, warehouse management, and project management).
Type of personal Data:	Data types depend on the Data transmitted by the Client. These are (depending on the commission): • Personal master Data (name, date of birth, address, employer), including contact Data (e.g. phone number, email address) • Contract Data, including billing and payment Data • History of contract Data
Categories of data subjects:	The categories of data subjects depend on the Data transmitted by the Client. These are (depending on the commission): • Client's employees (including applicants and former employees) • Client's customers • Client's prospective customers • Client's service providers • Contact details for contact persons
Deletion, blocking, and	Requests for deletion, blocking, and correction shall be addressed to the

correction of Data:	Client; otherwise the provisions of the Contract shall apply.

Appendix B

To the Commissioned Data Processing Agreement

Technical and organizational measures (TOM)

1 Technical and Organizational Measures

The following technical and organizational measures (TOM for short) are fundamental for Data processing

(1) Physical access control:

The following measures are in place for physical access control:

1) Definition of security areas
2) Realization of effective physical access protection
3) Definition of persons with physical access rights
4) Management and documentation of personal access authorizations over the entire life cycle
5) Accompaniment of visitors and external personnel
6) Monitoring of rooms outside of closing times
7) Logging of physical access

(2) System access control:

1) System access protection (authentication)
2) Easy authentication of employees (by username/password) with a high level of protection
3) Blocking in case of unsuccessful attempts/inactivity, and a process for resetting blocked access codes
4) Prohibition of the saving function for passwords and/or form entries
5) Definition of authorized persons
6) Administration and documentation of personal authentication media and access authorizations
7) Automatic system access blocking
8) Manual system access blocking
9) Secure transmission of authentication credentials in the network
10) Logging of system access

(3) Data access control:

The following measures are in place for Data access control:

1) Creation of an authorization concept
2) Implementation of Data access restrictions
3) Awarding of minimal authorizations
4) Administration and documentation of personal Data access authorizations
5) Logging of Data access

(4) Transport/transmission control:

The following measures are in place for transmission control:

1) Secure data transmission between server and client

2) Securing the transmission in the back end
3) Securing the transmission to external systems
4) Implementation of security gateways at network transmission points
5) Hardening of the back-end systems
6) Description of all interfaces and the transmitted personal Data fields
7) Machine-to-machine authentication
8) Data carrier management (procedure)
9) Process for collection and disposal
10) Privacy-oriented deletion/destruction procedure

(5) Input control:

The following measures are in place for input control:

1) Documentation of input authorizations
2) Logging of entries

(6) Commission control:

The following measures are in place for input control:

3) Documentation of input authorizations
4) Logging of entries

(7) Availability control:

The following measures are in place for availability control:

1) Backup concept
2) Emergency plan
3) Storage of backups
4) Inspection of emergency infrastructure

(8) Separation rule:

The following measures are in place for intended use control:

1) Efficient data collection
2) Separate processing