Xentral ERP Software GmbH
Data Processing Agreement

Introduction, Scope, Definition

(1) These terms govern the rights and obligations of the customer ("Controller") and Xentral ERP Software GmbH ("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").

(2) The Processor collects, processes and uses personal data of the Controller in the course of providing SaaS services ("Data Processing"). For this purpose, the Parties have concluded an Agreement (in accordance with the Xentral General Terms and Conditions for Software-as-a-Service Services, hereinafter the "SaaS GTC").

(3) 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 Subject Matter and Duration of Data Processing

(1) Subject Matter of Data Processing

(a) Material Scope

The subject matter of this DPA is the provision of the Software-as-a-Service (SaaS) described in the offer for the Controller.

This DPA applies to all activities in which employees and/or – insofar as permitted pursuant to § 6 below – subcontractors of the Processor collect, process or use personal data of the Controller.

(b) Territorial Scope

Pursuant to this DPA, data processing is permitted worldwide, i.e. within the territory of the European Union and the European Economic Area (EEA), secure third countries (Article 45 GDPR) and other countries pursuant to Article 46 GDPR.

(2) Duration of Data Processing

This DPA shall enter into force upon acceptance of the offer that refers to this DPA. The term of this DPA corresponds to the term or validity of the main contract (SaaS GTC) between the Parties. The right to extraordinary termination for good cause remains unaffected.

§ 2 Scope, Nature and Purpose of Data Processing and Data Subjects

(1) Scope and Purpose of Data Processing

Within the framework of the Controller's order, the scope and purpose of data processing comprise:

- SaaS operation in accordance with the offer and the SaaS GTC
- Operation of a ticket system and support channels, insofar as contractually agreed.

(2) Types of Data Processed

The Controller acknowledges that the scope of the processing information is at the Controller's discretion and may vary depending on the use of the Software, the booked plan and apps (if applicable) and Services. Data types / categories may include:

- Personal master data
- Communication data (e.g. telephone, email)
- Contract master data (contractual relationship, product or contract interest)
- Customer history
- Contract billing and payment data
- Planning and control data
- Information data (from third parties, e.g. credit agencies, or from public directories)
- Further/deviating categories of data pursuant to Annex 2 (if any; to be subsequently provided by the Controller and confirmed by Xentral)

(3) Categories of Data Subjects

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

- Customers
- Prospective customers
- Employees
- Suppliers
- Further/deviating data subjects pursuant to Annex 3 (if any; to be subsequently provided by the Controller and confirmed by Xentral)

§ 3 Responsibility, Including Instructions

3.1 Responsibility of the Controller

(1) With regard to data processing, the Controller is responsible for compliance with all applicable data protection regulations, in particular the GDPR and the German Federal Data Protection Act ("BDSG" as amended with effect from 25 May 2018), unless tasks are explicitly assigned to the Processor therein (cf. Article 28 GDPR).

In particular, the Controller is responsible for ensuring that:

- the lawfulness of the processing pursuant to Article 6 (1) GDPR is assessed, in particular that any required consents and/or works agreements necessary for the collection, processing or use of personal data have been obtained and that the statutory legal bases exist;
- the rights of data subjects (Articles 12–23 GDPR) are granted;
- the Processor comes into contact with as little personal data as possible when performing maintenance services under this DPA, in accordance with Article 25 GDPR;
- appropriate precautions are taken in the event that Xentral does not operate properly in whole or in part (e.g. through daily data backups, fault diagnosis, regular review of data processing results);
- the Processor is informed in good time prior to any remote access to data to what extent the Controller's data are not protected against data loss. In the absence of such notification, the Processor may assume that all data of the Controller to which the Processor has access are protected against data loss.

(2) The Controller is the "controller" and "master of the data" within the meaning of Article 4 (7) GDPR. The Processor processes the data exclusively for performance in accordance with the Controller's instructions pursuant to this DPA. In addition, the following applies:

- All instructions of the Controller at the time of conclusion of this DPA are conclusively set out in the provisions of this DPA and its annexes. Further instructions shall be issued by the Controller only insofar as they are necessary for the performance of data processing. Instructions shall be issued only in written or text form and in a documented manner.
- The Controller shall designate persons authorized to issue instructions and their representatives vis-à-vis the Processor at least in text form. In the absence of such designation, only the persons authorized for support (Section 9.2 Customer Care GTC) shall be deemed authorized to issue instructions within the meaning of this DPA.

(3) The Controller shall inform the Processor if and insofar as the technical and organizational measures (Annex 1) and/or the other provisions of this DPA no longer comply with the applicable data protection regulations applying to the Controller (including statutory amendments). The Controller is aware in particular that the Processor generally offers only unencrypted email communication and that unencrypted email communication does not ensure sufficient confidentiality vis-à-vis third parties. If the Controller wishes encrypted email communication, it shall use the ticket system (pursuant to Section 2.5 Customer Care GTC) and/or coordinate accordingly with the Processor.

(4) The Controller shall inform the Processor of any current communication with data protection authorities insofar as such communication concerns or may concern data processing under this DPA.

3.2 Responsibility of the Processor

(1) The Processor shall process personal data that it processes on behalf of the Controller under this DPA exclusively for the performance of this DPA, unless it is obliged to process such data otherwise by EU law or the law of a Member State (e.g. investigations by law enforcement authorities); in such a case, the Processor shall inform the Controller of such legal requirements prior to processing, unless the applicable law prohibits such notification for reasons of important public interest (Article 28 (3) sentence 2 lit. a GDPR).

(2) If and insofar as the Processor considers that compliance with instructions of the Controller within the meaning of the preceding paragraph would result in a violation of data protection provisions, the Processor shall immediately inform the Controller thereof (Article 28 (3) sentence 3 GDPR). In this case, the Processor is entitled to suspend execution of the relevant instruction until it has been confirmed or amended by the Controller's contact person.

(3) The Processor undertakes to inform the Controller immediately if and insofar as it or

persons employed by it have violated data protection provisions or the provisions of this DPA.

(4) The Processor shall, where required, appropriately support the Controller in fulfilling its obligations pursuant to Articles 30 and 32–36 GDPR (Article 28 (3) sentence 2 lit. f GDPR). The Processor shall immediately notify the Controller of disruptions, violations by the Processor or persons employed by it, violations of data protection regulations or the determinations made in the order, as well as any suspicion of data breaches or irregularities in the processing of personal data. Notifications pursuant to Articles 33 or 34 GDPR for the Controller may only be made by the Processor upon prior instruction.

(5) The Processor shall support the Controller in fulfilling the rights of data subjects (Articles 12–23 GDPR), provided that the Controller has issued a documented request (in writing or text form) to the Processor.

§ 4 Audits

(1) The Processor shall obligate its employees authorized to process data to confidentiality and shall monitor compliance therewith. Upon request, the Processor shall provide the Controller with evidence of this obligation to data secrecy.

(2) The Processor is entitled to provide evidence of compliance with data protection and data security, in particular pursuant to Article 28 (3) lit. h GDPR, at its own premises and/or at subcontractors by submitting audit certificates. On-site audits shall be omitted in such case, unless extraordinary circumstances exist (§ 4 (3) sentence 2). The certificates shall be updated by the Processor at most once per year.

(3) If the Processor cannot provide current certificates pursuant to § 4 (2), the Controller may audit the measures to ensure data protection and data security at the Processor during its usual business hours once per year on a random basis, provided there are no indications of a violation by the Processor of the Controller's instructions or of this DPA.

(4) Otherwise, the Controller may carry out the aforementioned audits at any time if there are specific indications of a violation by the Processor of the Controller's instructions or of a violation of this DPA.

(5) Audits pursuant to § 4 (2) and (3) of this DPA shall be announced by the Controller at least 21 days in advance, unless indications require an earlier audit, and shall be coordinated with the Processor regarding subject matter and scope.

(6) For the execution of audits pursuant to § 4 (3), the Processor shall in particular grant the Controller access to the data processing systems intended for data processing under this DPA.

(7) Audits pursuant to § 4 (3) conducted by the Controller may be carried out, where available, by the Controller's data protection officer or by neutral IT experts appointed by the Controller, provided that they declare under penalty of law to safeguard the legitimate confidentiality and data protection interests of the Processor and its other customers.

(8) The Processor is obliged to grant the competent data protection authority access to its business premises and records of data processing for the Controller to the extent required by law. If official audits are initiated by the Controller, the Controller shall reimburse the Processor for the effort incurred as a result of such audits.

§ 5 Principles of Technical and Organizational Measures

(1) The technical and organizational measures pursuant to Article 32 GDPR shall be implemented in coordination with the Controller (Annex 1).

(2) These measures (Annex 1) are subject to technical progress and may be replaced by other adequate measures by the Processor, provided that the original level of security is not undercut. The Processor shall document such replacements and make them available to the Controller upon written request.

(3) The Processor's data protection officer is listed in Annex 1. The Processor may change the data protection officer unilaterally. If the contact details of the data protection officer change as a result, the Processor shall inform the Controller accordingly.

§ 6 Engagement of Subprocessors

(1) General Authorization

Without prejudice to § 6 (2) (b), the Processor is generally entitled, at its discretion, to engage subprocessors for the performance of this

DPA, provided that such subprocessors have appropriate technical and organizational measures and meet the requirements of Article 28 (4) sentence 1 and Article 28 (3) GDPR.

(2) Requirements for Engaging Subprocessors

If and insofar as the Processor engages subprocessors pursuant to § 6 (1), the contractual arrangements with such subprocessors shall be designed to meet the requirements of data protection and data security applicable between the Parties.

(a) In particular, the Processor shall ensure that the provisions of this DPA also apply in relation to subprocessors, unless the Controller has consented to the engagement of specific subprocessors in individual cases. Such consent shall be deemed granted if (i) the subprocessors listed in Annex 4 are engaged or (ii) the Processor has notified the Controller of the engagement of a subprocessor under deviating arrangements and the Controller has not objected thereto in at least text form within four weeks. In any case, the Processor shall provide the Controller, upon request, with information about the relevant contractual arrangements with the subprocessor and shall submit the corresponding contractual documents upon request.

(b) The Processor shall inform the Controller in good time in advance of any intended changes concerning the engagement of new or replacement of existing subprocessors. Thereafter, the Controller shall have the opportunity to object to the announced change within the meaning of Article 28 (2) sentence 2 GDPR.

(c) The Controller agrees that in cases where the Processor engages a subprocessor for the performance of specific processing activities (on behalf of the Controller) and such processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the Processor and the subprocessor may ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission pursuant to Article 46 (2) GDPR, provided that the conditions for the application of such standard contractual clauses are met.

(3) Audit Rights of the Controller

In its contractual arrangements with subprocessors, the Processor shall ensure that on-site audits may be conducted at the subprocessors or by third parties commissioned by the Processor. The Processor shall ensure that the Controller is granted the audit rights pursuant to Article 28 (3) lit. h GDPR.

§ 7 Rectification, Erasure and Blocking of Data

(1) Data collected, processed and used on behalf of the Controller shall be rectified, erased or blocked by the Processor only in accordance with the Controller's instructions, unless legitimate interests of the Processor prevent this. If a data subject contacts the Processor directly for this purpose, the Processor shall forward such request to the Controller without delay.

(2) The Controller's contact person shall immediately review the request pursuant to § 7 (1) sentence 2 and shall inform the Processor in writing whether it is justified and instruct the Processor to carry out rectification, erasure or blocking.

(3) After completion of the contractual services, the Processor shall hand over to the Controller or delete, as described in Annex 1, all data, documents and generated processing or usage results in its possession or in the possession of subcontractors that are related to the contractual relationship. The Controller shall notify its decision in this regard in text form no later than upon termination – or, in the case of fixed-term contracts, at least six weeks prior to the end of the term.

§ 8 Other Provisions

(1) In the event of contradictions between this DPA and its annexes, the provisions of this DPA shall prevail.

(2) The exclusive place of jurisdiction and place of performance for this DPA is Augsburg.

(3) Should individual provisions of this DPA be invalid or incomplete, the remaining provisions shall remain effective. If several statutory provisions could alternatively apply to fill gaps or replace invalid provisions, the statutory provision that most closely reflects the economic intent of the Parties shall apply.

Annexes:

1 – Technical and Organisational Measures
2 – List of Subprocessors

Annex 1 – Technical and Organisational Measures (TOMs)

Data Protection Officer of the Processor:

DataCo GmbH
Sandstraße 33
80335 München
Deutschland
www.dataguard.de

A. Pseudonymization and Encryption Measures

See Section:

- B.2 item 3
- B.4. item 3 and 4
- B.7. item 3

B. Measures to Ensure Confidentiality, Integrity, Availability and Resilience of Systems and Services in Connection with Processing on a Permanent Basis

1. **Physical Access Control**: Unauthorized persons are prevented from accessing data processing facilities:
    - The Processor's business premises are locked outside business hours.
    - A logged key allocation exists for keys to the Customer's business premises.
2. **System Access Control**, which prevents data processing systems from being used by unauthorized persons:
    - The Processor maintains written policies for the use of data carriers and notebooks of its employees.
    - The Processor reviews the written policies for the use of data carriers and notebooks of its employees.
    - Xentral's file systems are encrypted with FileVault macOS.

3. **Data Access Control**, which ensures that those authorized to use a data processing system access only the data subject to their access authorization, and that personal data cannot be read, copied or modified without authorization during processing, use and after storage:
    - Access to the processed data in Xentral is carried out on the basis of the need-to-know principle.
    - The Processor logs the data processing in Xentral.
    - The Processor regularly reviews the implementation of the authorization concept.

4. **Transfer Control**, which ensures that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or during their transport or their storage on data carriers, and that it can be checked and determined at which points the transmission of personal data by means of data transmission facilities is intended:
    - Data exchange within the scope of Xentral is encrypted with FileVault macOS.
    - Data exchange via Xentral is logged on the Processor's web server.
    - Data on physical data carriers of the Controller at the Processor are digitized, encrypted and subsequently remaining data carriers are destroyed.
    - Remote data access by the Processor is carried out in accordance with the Controller's encryption procedures or in accordance with the Processor's SSH standard.

5. Input Control, by means of which it can subsequently be verified and determined whether and by whom personal data have been entered into, modified in or removed from data processing systems:
    - Data processing operations in Xentral are logged by the Processor

6. Order Control, which ensures that personal data processed on behalf of the Controller can be processed only in accordance with the Controller's instructions:
    - The Controller and its employees are identified by the access credentials provided to them for Xentral's ticket center.

7. Availability Control, i.e. measures must be taken to ensure that personal data are protected against accidental destruction or loss:
    - Virus control for incoming files by email
    - The Processor maintains a firewall concept.
    - The Processor carries out regular data backups; backups are stored in encrypted form.

8. Separation Control, which ensures that data collected for different purposes can be processed separately:
    - Separation is ensured via individual and password-protected access through the Customer's Xentral instance to which the Processor has access.
    - There is a separation between Xentral's development, test and production systems**.**

C. Measures to Ensure Availability of Personal Data and Rapid Restoration After Physical or Technical Incidents

See Section:

- B.7. item 3

D. Procedures for Regular Review, Assessment and Evaluation of the Effectiveness of Technical and Organizational Measures

- Data protection organization
- Formalized processes for data protection incidents
- Documentation of Controller instructions
- SLAs for conducting audits

Annex 2 – List of Subprocessors

Subprocessor	Address/Location	Processing Activity
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855 Luxembourg	Hosting, Infrastructure/Platform/Software as a Service
Zendesk Inc.	989 Market St San Francisco, CA 94103(888), USA	Support-Ticket-System
Planhat AB	c/o WeWork, Regeringsgatan 29, 111 53 Stockholm, Sweden	Onboarding/Support-System
Atlassian Corp.	Level 6, 341 George Street Sydney NSW 2000, Australia	Jira: ticket system for error handling by software development team
Chargebee Inc.	340 S Lemon Avenue, 1537 California, 91789 USA	Subscription management platform, customer invoicing
Hubspot Germany GmbH	AM Postbahnhof 17 10243 Berlin	Inbound Marketing-, CRM-, Sales-Plattform
Google Cloud EMEA Limited	70 Sir John Rogerson's Quay, Dublin 2, Ireland	Document processing, spreadsheets, general data storage, collaborative work, Gmail; Looker (analytics software for demo and software usage)