# Data Processing Agreement (DPA)

pursuant to art. 28 General Data Protection Regulation (GDPR)

by and between

**empower® Customer**
each legal entity and/or individual user where
a) empower GmbH processes and/or stores personal data
b) no other valid data processing agreement has been agreed

- the Controller -

and

**empower GmbH**
Im Mediapark 8
50670 Köln

- the Processor -

## 1 Subject matter, term, personal data processed and categories of data subjects

### 1.1 Subject matter

The subject matter of this DPA consists of the appointment of the Processor by the Controller and the provision of instructions for the processing of personal data. The processing activities that the Processor shall carry out are strictly limited to those necessary to fulfil the scope (as applicable) of a) a software trial phase, b) a proof-of-concept phase, c) a software license contract and potentially d) a cloud service contract agreed between the parties.

For the avoidance of doubt, here a summary of the relevant activities that the Processor shall carry out on behalf of the Controller:

- Regular commercial processes such as storing contracts incl. contact details, storing support tickets, sending invoices and receiving payments.
- As defined by the applicable scope, potentially the following activities shall be performed by the Processor: Installation support, maintenance and support activities, potentially also for a cloud-based database that stores Microsoft Office templates (PowerPoint templates, Word templates etc.) as well as User business contact information (in order to update Word templates or Outlook signatures etc.) of the Controller. The Processor will not access the database or its content for any other activity than technical maintenance and support activities.
- Remote Support services in case of issues with the software products of the Processor. During such remote support services the Processor will request and (if approved by Controller) get access to local computers of the Controller to analyze issues. The Processor could potentially see personal data of the Controller. Both parties will try to avoid this.

### 1.2 Term

The term of this DPA corresponds to the term of the applicable contract.

### 1.3 Categories of personal data

The categories of personal data processed are:

- personally identifiable information (e.g. name, surname, email, business contact information)
- billing, invoicing and payment data
- other data that the Controller stores within cloud template library

### 1.4 Categories of Data Subjects

The personal data collected and processed related to:

- employees, associates, staff members
- potentially: customers, suppliers

## 2 Data Transfer Abroad

(1) The Processor undertakes not to transfer or store any personal data abroad (*i.e.* outside the territory of the Controller + the countries defined in the relevant contracts) without the prior written authorization of the Data Controller.

(2) Any data transfer or storage abroad, and processing activities thereof, will be carried out (on request by Controller) in strict compliance with the Controller's documented and specific instructions.

## 3 Technical and Organizational Measures

(1) The Processor undertakes to adopt all the necessary technical and organizational security measures described in Appendix A.

(2) Such measures are subject to the Controller's scrutiny and to its approval. Upon the Controller's approval, such security measures, documented as above, will become an integral and substantial part of this agreement and are hereby incorporated. Insofar as an inspection/audit by the Controller shows the necessity for amendments, such amendments shall be implemented by mutual agreement.

(3) The Processor warrants that it has taken all the security measures in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. Such measures shall guarantee data security and a protection level adequate to the level of risk concerning confidentiality, integrity, availability, and resilience of the systems. According to Article 32, par. 1 GDPR the following must be taken into account when assessing the appropriateness of the security measures adopted: whether or not the measures can be reasonable considered to be state-of-the-art, the implementation costs, the nature, scope and purposes of processing as well as the likelihood of data breaches and the severity of risks to the rights and freedoms of natural persons.

(4) The technical and organizational measures are subject to technical and technological progress and development. Hence, the Processor may adopt alternative adequate measures which are up to date with the changed technological environment. When doing so, the processing security level may not be reduced. Substantial changes must be documented.

# 4 Data subjects rights

(1) The Processor undertakes to provide full cooperation and assistance, as it may be reasonably possible, in order to assist the Controller in responding to data subjects' requests for the exercising of their rights.

(2) In particular, the Processor undertakes to (i) immediately communicate to the Controller any request received by data subjects concerning the exercising of their rights and, if feasible and appropriate, to (ii) enable the Controller to design and deploy all the technical and organizational measures necessary to answer the data subjects' requests.

(3) Notwithstanding the fact that the Controller bears the responsibility to respond to the data subjects' requests, the Processor can accept to be tasked with the fulfilment of some specific requests, provided that such tasks do not require disproportionate efforts from the Processor and that the Controllers provides detailed instructions in writing.

# 5 Further duties of the Processor

In addition to complying with the provisions of this DPA, the Processor commits to meet all applicable statutory requirements set forth at Articles 28 to 33 GDPR. To this end, the Processor warrants compliance with the following sections 5.1 to 5.4

## 5.1 Appointment of a Data Protection Officer (DPO)

The contact details of the current DPO:

empower GmbH
Data Protection Officer
Im Mediapark 8
50670 Cologne
Germany
data-privacy@empowersuite.com

The Processor shall inform the Controller about any changes of Data Protection Officer.

## 5.2 Confidentiality

Processing activities under this DPA shall only be performed by individuals (such as employees, agents, or staff members) that have been instructed by the Processor on the appropriate way to process data and have been contractually subjected to confidentiality pursuant to art. 28 par. 3 (b) and art. 32 GDPR. The Processor, and any person acting under its authority who has access to the personal data, shall not process that data unless acting upon instructions given by the Controller — including the powers granted under this DPA - unless they are required to do so by statutory law.

### 5.3 Technical and Organizational Measures

Implementation of, and compliance with, all appropriate technical and organizational measures in the framework of this DPA, in particular as set forth at art. 32 GDPR. The Processor shall periodically monitor the internal processes and the technical and organizational measures to ensure that processing activities pertaining to it are carried out in accordance with the requirements of applicable data protection law and the protection of data subjects' rights. The Processor shall grant verifiability of the technical and organizational measures to the Controller as part of the Controller's supervisory powers referred to in sec. 7 of this contract.

### 5.4 Cooperation with Supervisory Authorities

The Controller and the Processor shall cooperate, on request, with the supervisory authority. The Controller shall be informed immediately of any inspections and measures executed by the supervisory authority, insofar as they relate to the activities under this DPA. This also applies insofar as the Processor is under investigation or is party to an investigation by a competent authority in connection with infringements to any provision regarding the processing of personal data in connection with the processing of this DPA. Insofar as the Controller is subject to an inspection by the supervisory authority, an administrative fine, a preliminary injunction or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the processing of data by the Processor as of this DPA, the Processor shall make every effort to support the Controller.

## 6 Sub-processors

(1) The Controller authorizes the Processor to outsource part of the processing activities pursuant to this DPA to sub-processors. The sub-processors shall, as legally required, be subject to the same contractual obligations resulting from this agreement, pursuant to art. 28 par. 4 GDPR.

(2) At the date of signature of this agreement, the parties mutually acknowledge and agree that the Processor currently commissions the following sub-processors on the condition of a contractual agreement in accordance with Article 28 paragraph 4 GDPR:

| | Company | Link for GDPR information | Purpose |
|---|---|---|---|
| 1 | Microsoft Corporation | Microsoft Online Services Terms (https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=14943) | Outsourced cloud storage and processing activity |

(3) It is understood between the parties that the communication of personal data to any sub-processor shall only take place after all conditions set out in paragraph (1) for the appointment of sub-processors have been met.

(4) The Processor must maintain and keep an updated a list of sub-processors. The Controller shall be notified of any change to such list without undue delay, giving the Controller the option to object. In case of objection, the Processor retains the right to terminate the contract in place with the Controller.

(5) The Processor shall bear full responsibility and liability for the activities of its sub-processors vis a vis the Controller.

(6) Should a sub-processor provide its services outside the EU/EEA, the Processor shall ensure compliance with the rules regarding data transfer abroad, as described under sec. 2 of this DPA.

# 7 Audits

(1) The Controller has the right to carry out reasonable inspections or to have them carried out by an auditor appointed on a case-by-case basis. The auditor may assess Processor's compliance with this DPA in its business operations by means of checks, of which the Processor will be notified in advance.

(2) The Processor shall allow the Controller to verify compliance with its obligations as provided by Article 28 GDPR. The Processor undertakes to give the Controller the necessary information on request and to demonstrate the implementation of the technical and organizational measures but may protect its own IT Security as well as other client data.

(3) Evidence of the implementation of such measures, which may not only concern the activities under this DPA, may also be provided by
- compliance with approved Codes of Conduct pursuant to Article 40 GDPR;
- certification according to an approved certification procedure in accordance with Article 42 GDPR;
- current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, data protection officer, IT security department, data protection auditor);
- a suitable certification by IT security or data protection auditing.

(4) The Processor may charge a reasonable fee to the Controller for enabling inspections.

# 8 Assistance to the Controller

(1) The Processor shall assist the Controller in complying with the obligations concerning the security of personal data, reporting of data breaches, data protection impact assessments and prior consultations set forth at Articles 32 to 36 of the GDPR, including
- ensuring adequate protection standards through technical and organizational measures, taking into account the type, circumstances and purposes of processing, the likelihood of data breaches and the severity of the risk to natural persons possibly resulting thereof
- ensuring immediate detection of infringements
- reporting data breaches without undue delay to the Controller
- assisting the Controller in answering to data subjects' requests for the exercising of their rights

(2) The Processor may charge the Controller a reasonable fee for support services which are not included in the description of the services and which are not attributable to the Processor's misconduct, mistakes or infringements.

# 9 Directive powers of the Controller

(1) The Processor shall not process any personal data under this DPA except on the Controller's documented instructions, unless required to do so by Union or Member State law.

(2) In case the Controller should require any change in the processing of personal data set forth by the documented instructions mentioned at sec. 2, the Processor shall immediately inform the Controller if it considers such changes likely to result in infringements to data protection provisions. The Processor may refrain from carrying out any activity that may result in any such infringement.

# 10 Liability

(1) Each party to this DPA commits to indemnify the other party for damages or expenses resulting from its own culpable infringement of this DPA, including any culpable infringement committed by its legal representative, subcontractors, employees or any other agents. Furthermore, each party commits to indemnify the other party against any claim exerted by third parties due to, or in connection with, any culpable infringement by the respectively other party.

(2) Art. 82 GDPR stays unaffected.

# 11 Deletion and return of personal data

(1) The Processor shall not create copies or duplicates of the data without the Controller's knowledge and consent, except for backup copies, insofar as they are necessary for ensuring that data is processed correctly or built-in of used services (e.g. Microsoft Azure), and where the retention of such data is required by law.

(2) After conclusion of the provision of services, the Processor shall, at the Controller's choice, either delete in a data-protection compliant manner or return to the Controller, all the personal data collected and processed under this DPA, unless any applicable legal provision requires further storage of the personal data.

(3) In any case, the Processor may retain beyond termination of the contract all the information necessary to demonstrate the compliance of the processing activities carried out.

(4) The documentation referred to under point (3) above, shall be stored by the Processor in accordance with the applicable retention periods, statutory or otherwise determined. The Processor may hand the documentation over to the Controller upon termination of the agreement. In such case, the Processor is relieved from any obligation to keep such documentation.

# Appendix A - Technical and Organizational Measures

## *I. Confidentiality (Art. 32 Sec. 1 lit. b GDPR)*

1. Control of admission

Measures that prevent unauthorized access to data processing systems dealing with personal data:

1. Predefined security sections
2. Safeguarding of point of access
3. Setup of admission modalities for internal and external employees (e.g. custodial staff)
4. Legitimization of admission authorization and inspection of admission
5. Components for implementation: personal monitoring, electronic keycards, door locking systems, technical monitoring systems, and distribution of security keys in individual cases

2. Control of physical access

Measures that prevent unauthorized use of data processing systems and procedures:

1. Setup of access modalities for internal and external employees (e.g. maintenance personnel, visitors, etc.)
2. Legitimization of access authorization, and inspection of access
3. Access to PC workstations and laptops, incl. general access to data storage devices
4. Components for implementation: password protected user master record, personal user account, dedicated application and approval procedure and technically assisted adherence to password standards

3. Control of accessibility

Measures that exclusively permit access to personal data to approved users of data processing systems within the limitation of their access authorization:

1. Setup and legitimization of access modalities and user authorization for access to data, esp. personal data
2. Execution of access and user monitoring
3. Physical and logical security of data processing systems
4. Components for implementation: deployment of “need-to-know” and “need-to-do”, demand actuated authorization policies and profiles, dedicated application and approval procedures, technically assisted adherence and record.

4. Control of isolation

Measures that ensure that data compiled for different purposes is processed separately:

1. Systems and applications that are logically and/or physically separated by client, as well as physically separate production and development systems
2. Provided that storage of client databases is a requirement:
   completely separate environments for each individual client

5. Pseudonymization (Art. 32 Sec. 1 lit. a GDPR; Art. 25 Sec. 1 GDPR)

Processing of personal data in a manner that does not allow allocation of specific entities and their connected personal data without additional information, provided this additional information is stored separately and technical and organizational measures are required to be taken.

In our circumstances of data processing the above has thus far proven to be irrelevant

## *II. Integrity (Art. 32 Abs. 1 lit. b GDPR)*

1. Control of transfer

Measures that ensure that personal data cannot be read, copied, altered or deleted during electronic transfer or during transportation, as well as when saving to data storage devices without authorization. Further it will be ensured and determined which entities are to receive personal data via facilities for data transfer:

1. Determination of approved sites of receipt
2. Determination and legitimization of approved entities for transport and/or transfer/forwarding and holding of documentation verifiable by third parties
3. Determination of authorized entities who may administer data storage devices and of domains that are permitted to contain data storage devices, DP-facilities, etc. Also, physical safeguarding of these determined domains
4. Determination and safeguarding of procedures and transport routes
5. Components for implementation: integrity during storage of internal and external data forwarding with validity checks and verification procedures, graded safety and encryption procedures, firewall systems, virus inspection software, SSL encryption, VPN and use of “closed” networks.

2. Control of data entry

Measures that ensure that it is verifiable if personal data in data processing systems was entered, altered or deleted, and by whom:

1. Documentation of entry procedures (write and read, if required)
2. Ensure possibilities for later inspection of data entries and transactions (if required)
3. Components for implementation: documentation von entries in systems and applications as well as their output (if required), primarily automated coordination procedures and inspections

## *III. Availability and capacity (Art. 32 Sec. 1 lit. b GDPR)*

1. Availability check

Measures that allow protection of personal data against unintentional loss or destruction:

Extensive backup concept available, which will not be detailed due to data security regulations. General description: setup and implementation of data securing and emergency concept as well as its regular updating and testing (backup and/or disaster management).

2. Quick recovery (Art. 32 Sec. 1 lit. c GDPR)

Is provided. Details will not be disclosed due to data security regulations.

## *IV. Procedures for regular review, assessment and evaluation (Art. 32 Sec. 1 lit. d GDPR; Art. 25 Sec. 1 GDPR)*

1. Data protection management

Annual review or technical and organizational measures.

2. Incident-Response-Management

An Incident-Response-Plan has been developed and established which contains 6 stages:

1. Preparation
2. Identification: establishment to determine if an occurrence is a security concern.
3. Containment: The damage caused by the occurrence is to be contained, affected systems will be isolated to avoid further damage.
4. Eradication: The cause of the occurrence is to be identified; the affected systems will be removed from the productive environment.
5. Recovery: Affected systems are to be reintegrated into the productive environment once it has been ensured that no further threats persist.
6. Acquired insights: extension of incident documentation and analysis to transfer knowledge to team or company. This way it will be ensured that future occurrences can be dealt with more effectively.

3. Data protection by design and by default (Art. 25 Sec. 2 GDPR)

Currently not relevant in our cases of data processing.

4. Control of assignment

   Measures to ensure that personal data processed in the course of an assignment can only be handled in accordance to the guidelines set by the client:

   1. Setup of explicit terms of contract
   2. Setup of inspection of contract implementation or fulfilment
   3. Processing exclusively within the limitations of contractual stipulation, competence and inspection measures integrated in operating procedures in agreement with the client