Empolis Industrial Knowledge

Data Processing Agreement

Operation & Data Security

Empolis Information Management GmbH
Europaallee 10
67657 Kaiserslautern, Germany

Empolis

Contents

1 Operation of the Solution

1.1 Data Center: Certification and Guidelines

Empolis runs the software using Amazon Web Services (AWS) in the Frankfurt am Main region. As of this date, the AWS computer centers and services are certified in accordance with the standards ISO 27001, ISO 27017, ISO 27018 and the German Cloud Computing Compliance Controls Catalog (C5) of the German Federal Office for Information Security (BSI). The standard ISO 27001 defines the requirements for establishing, implementing, operating, monitoring, inspecting, maintaining and upgrading a documented management system for information security in the context of the totality of business risks of an organization. Ultimately, the standard thus ensures best practices for security processes that help protect information resources.

1.2 Accessing and Transmitting Data

The software is accessed exclusively via a browser. HTTPS is used as the protocol to ensure state-of-the-art secure data transmission. The data is encrypted using SSL/TLS[1]. The standard port for HTTPS is 443. This port must be open to users.

[1] https://tools.ietf.org/html/rfc2818

2 Data Security

2.1 Recital

This section specifies in detail the contractual parties' obligations regarding data protection. These details apply to all activities in relation to the contract where the Contractor's employees or authorized persons process personal data ("data") of the Customer.

2.2 Subject Matter, Duration and Specifications of the Order Processing

The contract specifies the subject matter and duration of the order as well as the type and purpose of the processing. In particular, the following types of data are part of the data processing:

- Type of data: Account, access and customer data
- Type and purpose of data processing: Use of a knowledge management system provided by Empolis for the service area
- Categories of data subjects: Users of the system

Detailed information can be found on the following websites:

https://esc-eu-central-1.empolisservices.com/doc/en/legal/privacy-policy
https://empolis.com/en/terms

The period of validity of the provisions of this section is based on the term of the contract to the extent that the provisions in this section do not contain obligations extending beyond these provisions.

2.3 Scope of Application and Responsibilities

1) The Contractor processes personal data on behalf of the Customer. This includes activities that are specified in the contract and performance specifications. Within the scope of this contract, the Customer is solely responsible for compliance with data protection laws, in particular for the legality of the data provision to the Contractor and the legality of the data processing. (The Customer is the "Controller" within the meaning of Art. 4[7] GDPR).
2) Instructions are initially specified in the contract and can be subsequently modified, amended or replaced by way of individual instructions in writing or in electronic format (text form) addressed to the contact person specified by the Contractor (individual instructions). Instructions not included in the contract are treated like a request for a service change. Verbal instructions must be immediately confirmed in writing or text form.

2.4 Contractor Obligations

1) The Contractor may only process data of data subjects within the scope of the order and according to the Customer's instructions, except for special cases within the meaning of Art. 28(3)(a) GDPR. The Contractor shall notify the Customer without delay if the Contractor thinks that an instruction violates applicable law. The Contractor may suspend implementation of the instructions until confirmed or modified by the Customer.
2) Contractor will configure the internal operational organization so that it meets special data protection requirements. The Contractor will implement technical and organizational measures to reasonably protect the Customer's data in compliance with GDPR (Art. 32 GDPR) requirements.

The Contractor is obliged to implement technical and organizational measures that ensure the continuous confidentiality, integrity, availability and stability of systems and services in relation with the data processing. The Customer is aware of these technical and organizational measures, and the Customer is responsible for ensuring that these measures provide a reasonable level of protection for the risks in relation with the data to be processed.

The Contractor has the right to change the implemented security measures but must ensure that the contractually agreed level of protection is met.

3) The Contractor supports the Customer to the extent possible in the fulfillment of queries and claims of data subjects in accordance with Chapter III GDPR and with respect to compliance with the obligations specified in Articles 33 to 36 GDPR.
4) Contractor ensures that the employees and other parties responsible for the processing of Customer data are not permitted to process these data outside of the scope of the instructions. Moreover, the Contractor ensures that the persons authorized to process personal data have undertaken to maintain confidentiality or are subject to a reasonable statutory obligation to secrecy. The confidentiality/secrecy obligation continues to apply after the contract has been terminated.
5) Contractor notifies the Customer without delay if the Contractor becomes aware of any security breaches regarding the protection of the Customer's personal data.

   The Contractor takes the required measures to secure the data and to mitigate possible negative effects for the data subjects and will immediately consult with the Customer to this end.
6) The Contractor will provide the Customer with the name of the contact person who will respond to any data protection matters within the scope of the contract.
7) The Contractor undertakes to perform its duties under Art. 32(1)(d) GDPR and to set up a process for the regular review of the effectiveness of technical and organizational measures to ensure processing security.
8) The Contractor will correct or erase the data under the contract if instructed accordingly by the Customer and if this falls within the scope of the instructions. If a solution that conforms with data protection provisions or a corresponding restriction of the data processing is impossible, the Contractor will destroy data carriers and other materials in accordance with data protection provisions and based on the Customer's individual instructions or will return these data carriers to the Customer, except as otherwise agreed to in the contract.

   In special cases to be specified by the Customer, the Contractor shall store or transfer data; compensation and protective measures for this are to be agreed upon separately, provided this has not already been agreed in the contract.
9) Data, data carriers and any other materials must be returned to the Customer upon request or erased after order completion.
10) In the event that a data subject asserts any claims against the Customer according to Art. 82 GDPR, the Contractor undertakes to support the Customer in the defense against the claim to the extent possible.

2.5 Customer Obligations

1) The Customer must notify the Contractor fully and without delay if the Customer detects any errors or inconsistencies relating to data protection-related provisions.
2) In the event that a data subject asserts any claims against the Customer according to Art. 82 GDPR, Section 2.4, paragraph 10 applies accordingly.
3) The Customer will provide the Contractor with the name of the contact person who will respond to any data protection matters within the scope of the contract.

2.6 Requests of Data Subjects

1) If a data subject contacts the Contractor with a request for correction, erasure or information, the Contractor will refer the data subject to the Customer if the matter can be related to the Customer based on the information provided by the data subject. The Contractor will forward the data subject's query to the Customer without delay. Where agreed, the Contractor supports the Customer to the extent possible upon instruction. The Contractor is not liable if the query of the data subject is not resolved, is not resolved correctly or is not resolved by the given deadline by the Customer.

2.7 Documenting Compliance

1) The Contractor shall provide evidence to the Customer regarding its compliance with the obligations under this contract using suitable measures, e.g.: self-audits; company-internal policies, including an external certification regarding compliance with these policies; data protection and/or information security certificates (e.g. ISO 27001); permitted codes of conduct according to Art. 40 GDPR; certificates according to Art. 42 GDPR or other evidence to be agreed.
2) If, in individual cases, inspections carried out by the Customer or the auditors authorized by the Customer become necessary, these must be performed during regular business hours without interrupting the ordinary course of business and after making an appointment subject to an appropriate lead time. The Contractor may make its permission for such audits dependent on a prior appointment with an appropriate lead time and on conclusion of a confidentiality agreement which covers the data of other customers and the established technical and organizational measures. If the auditor commissioned by the Customer is a competitor of the Contractor, the Contractor has the right to object to this auditor.

   The Contractor is entitled to request compensation for the support provided during such an audit, where agreed in the contract. The outlays involved for an inspection are generally limited for the Contractor to one day per calendar year.

2.8 Subcontractors (Additional Processors)

1) To process the order, the Contractor uses the following subprocessors:

Contractual Partner	Corporate Headquarters	Software Components
Amazon Web Services EMEA SARL (AWS Europe)	38 Avenue John F. Kennedy, 1855 Neudorf-Weimershof, Luxembourg	Technical Infrastructure AI Features (Nova Language Model)
Amplitude, Inc (formerly Sonalight, Inc)	201 Third Street, Suite 200, San Francisco, CA 94103, USA	User Statistics
Breve Information Technology LLC-FZ (formerly Enozom)	FDRK0153, Compass Building, Al Shohada Road, AL Hamra Industrial Zone-FZ, Ras Al Khaimah, United Arab Emirates	Knowledge Home Mobile Field Service App
DeepL SE	Maarweg 165, 50825 Köln	Translation Feature
Microsoft Ireland Operations Ltd.	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland	AI Features (GPT Language Model)
Sendbird, Inc	400 First Avenue, San Mateo, CA 94401, USA	Community & Team Knowledge
Proalpha Group GmbH	Auf dem Immel 8, 67685 Weilerbach	Development and support; joint project management, if necessary

Table 1: Subcontractors

2) The Contractor shall notify the Customer in advance and in writing before placing orders with new subprocessors or modifying an existing subcontracting relationship. Where good cause exists, the Customer has the right to object to the action announced by the Contractor within four weeks of notification pursuant to sentence 1. Good cause exists in particular if there are reasonable grounds for doubt that the subprocessor will provide the agreed service in accordance with applicable statutory data protection provisions or according to the parties' agreements. If the Contractor is not able to continue providing the services owed due to the objection, or if it is not reasonable to do so, the Contractor has the right to terminate the main contract for good cause. The Contractor will notify the Customer in advance regarding its intention to terminate the contract.
3) The Contractor will conclude agreements with these third parties to the extent necessary to ensure appropriate data protection and information security measures.

2.9 Duty to Inform, Written Form Requirement, Choice of Law

1) The Contractor must inform the Customer without delay if Customer data possessed by the Contractor is jeopardized due to attachment or seizure, insolvency proceedings, a settlement procedure or any other events or measures initiated by third parties. The Contractor will immediately inform any authorized persons in this respect that the jurisdiction and ownership of the data rests exclusively with the Customer as "Controller" within the meaning of the General Data Protection Regulation.
2) Modifications and amendments to this section and all of its integral parts – including any assurances by the Contractor – require the written form, which may also occur in electronic format (text form) with an explicit reference that this is a modification of or amendment to the respective provision. This also applies for a waiver of the format requirement.
3) In the event of any inconsistencies, the provisions of this section regarding data protection have priority over other provisions of the contract. If individual parts of this section are ineffective, this does not affect the effectiveness of the remaining parts.
4) German law shall apply.

2.10 Liability and Compensation for Damages

The Customer and Contractor are liable to data subjects according to the provisions of Art. 82 GDPR.

Unless expressly agreed otherwise, a liability clause agreed to between the contractual parties with regard to the performance of services also applies for order processing.

3 Technical and Organizational Measures According to GDPR

3.1 Requirements

1) Before starting the processing, the Contractor shall document implementation of the required technical and organizational measures specified before the order was placed, particularly with regard to executing the specific order, and to provide said documentation to the Customer for review. If the Customer accepts the documented measures, they will form the basis of the order. To the extent that a review/audit by the Customer indicates a need for adjustments, these must be implemented with mutual consent.
2) The Contractor shall ensure that data security is maintained in accordance with Art. 28(3)(c) and Art. 32 GDPR, particularly in conjunction with Art. 5(1) and (2) GDPR. Overall, the measures to be implemented are data security measures and ensure an appropriate security level commensurate with the respective risk regarding confidentiality, integrity, availability and stability of the systems. The Contractor shall take into account the state of the art, the implementation costs and the type, scope and purpose of the processing as well as the likelihood of occurrence and degree of risk to the rights and freedoms of natural persons within the meaning of Art. 32(1) GDPR.
3) The technical and organizational measures are subject to technical progress and development. In view of that, the Contractor is permitted to implement adequate alternative measures. The alternative measures must not result in a security level that is lower than that of the specified measures. Material changes must be documented.

3.2 Implementation

3.2.1 Confidentiality

(Art. 32(1)(b) GDPR)

3.2.1.1 Physical Access Control

For the Empolis Information Management GmbH offices, there are appropriate building security measures in place at each location as well as a documented ID/key system for all employees. Video surveillance cameras are installed in certain places. People external to the company are allowed entry only subject to an agreement and/or with an accompanying person. Regular service providers who may carry out their tasks outside of business hours (e.g., cleaning staff) are bound to confidentiality. Empolis Information Management GmbH is certified according to ISO 9001 and DIN ISO/IEC 27001.

Entering buildings, data floors, and dedicated customer areas in the commissioned data centers is only possible with individually programmed entry cards containing biometric or visual identification, which means only one individual person is allowed to enter in each case. The computer center is manned by security personnel 24 hours a day and 365 days a year. In addition, the entry areas and outdoor facilities, as well as all sensitive areas indoors, are monitored by cameras.

3.2.1.2 System Access Control

All Empolis Information Management GmbH systems are password-protected. Employees must make their passwords complex; this rule cannot be circumvented. There is a company agreement regarding the use of electronic media; furthermore, all employees promise to maintain confidentiality at the start of their employment relationship.

Entry to dedicated customer areas of the data center is only possible with individually programmed entry cards containing biometric and visual identification, meaning that only one individual person may enter in each case.

3.2.1.3 Data Access Control

The Empolis Information Management GmbH systems are secured with a differentiated role and user-permissions scheme to prevent unauthorized use of any kind.

Empolis Information Management GmbH does not carry out any tasks in the commissioned data processing center that would allow direct access to the Customer's IT systems or any data stored or processed in these IT systems. As a rule, no data protection-relevant activities are planned in the framework of the contractual relationship between the Customer and Empolis Information Management GmbH, but rather only system monitoring and troubleshooting tasks in the event of a fault. These tasks are generally performed on the basis of a customer report.

3.2.1.4 Application Control

Empolis Information Management GmbH employs an internal customer separation system to keep the data of different customers entirely separate. Production and test environments are also separated from one another. Empolis Information Management GmbH is certified according to DIN ISO/IEC 27001.

Analogous certifications apply to the data processing centers: DIN ISO/IEC 27001, TÜV-certified data processing center, Datacenter Star Audit, PCI DSS-approved.

3.2.1.5 Pseudonymization

(Art. 32(1)(a) GDPR; Art. 25(1) GDPR)

This is defined as the processing of personal data in such a way that data can no longer be linked to a specific data subject without the use of additional information. The additional information is stored separately and is subject to appropriate technical and organizational measures. This task is the responsibility of the Customer.

3.2.2 Integrity

(Art. 32(1)(b) GDPR)

3.2.2.1 Transfer Control

Empolis Information Management GmbH always works via secure VPN connections.

In the commissioned data processing center, Empolis Information Management GmbH never carries out any tasks that would allow direct access to the Customer's IT systems/data or to any data stored or processed in these IT systems. Exceptions to this are the instances where access is obtained for the purpose of system monitoring and troubleshooting. The physical security measures are described under "Physical Access Control" and "System Access Control." Access by the Customer is via dedicated, secure connections.

3.2.2.2 Input Control

Within its systems, Empolis Information Management GmbH works with suitable system protocols: Inputs into the software systems provided to the Customer are made by the Customer only.

In the commissioned data processing center, Empolis Information Management GmbH never carries out any tasks that would allow direct access to the Customer's IT systems/data or to any data stored or processed in these IT systems. The physical security measures are described under "Physical Access Control" and "System Access Control." Access by the Customer is via dedicated, secure connections.

3.2.2.3 Order Control

Empolis Information Management GmbH carries out the order based only on the signed contract and the associated appendix. Subcontractors are carefully selected and monitored.

3.2.2.4 Organizational Control

Empolis Information Management GmbH operates according to an ISO-9001-certified Quality Management System and is also DIN ISO/IEC 27001-certified. The related targets, process descriptions and continuous improvement activities ensure compliance with statutory requirements and an organized and traceable handling of data and information.

3.2.2.5 Quality Assurance and Training Involving Standard Software

The above agreements are without prejudice to the terms of use of standard software and the resulting use of Customer data for purposes of quality assurance and training. For these purposes, customer data is accessed and processed accordingly with due regard to the provisions of the order processing agreement and the rules on the security of processing according to Art. 32 GDPR.

3.2.3 Availability and Stability

(Art. 32(1)(b) GDPR)

3.2.3.1 Availability Control

Empolis Information Management GmbH systems are protected with suitable back-up procedures, with an uninterruptible power supply, and with up-to-date anti-virus and firewall measures. Empolis Information Management GmbH is certified according to DIN ISO/IEC 27001.

The data processing centers that are used are likewise selected so that an appropriate level of availability is assured through their certifications (DIN ISO/IEC 27001 or comparable certifications) and the SLAs in effect.

3.2.3.2 Quick Recoverability

(Art. 32(1)(c) GDPR)

This requirement is fulfilled by the certification of Empolis Information Management GmbH according to DIN ISO/IEC 27001.

3.2.4 Regular Review, Assessment and Evaluation Processes

(Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

This requirement is fulfilled by the certification of Empolis Information Management GmbH according to DIN ISO/IEC 27001.