

Agreement on Data Processing on order for EMPAL Services

I.	Definitions and Clarifications.....	1
II.	Preamble.....	1
III.	Agreement on Data Processing on order.....	2
	§1 Subject matter and duration of processing.....	2
	§2 Order content in detail	2
	§3 Technical and organizational measures	4
	§4 Authority to issue instructions.....	4
	§5 Obligation of confidentiality	5
	§6 Assignment of subcontracted processors.....	5
	§7 Obligations and rights of the Customer; support of the Customer by EMPAL.....	6
IV.	Quality Assurance	7
	§8 Deletion or return after completion of processing	8
	§9 Liability	8
	§10 Final Clauses	8

I. Definitions and Clarifications

EMPAL GmbH (as data processor - hereinafter referred to as "**EMPAL**") and the Customer (as data controller - hereinafter referred to as "**CUSTOMER**") (hereinafter individually or collectively also referred to as "**PARTIES**") have concluded a service agreement on the provision of software products of ATOSS Software AG and related technical services. The following agreement on data processing on order serves as the basis for the fulfilment of the legal provisions on data protection regarding the existing contractual relationships of the parties on the provision of services.

In this context, it concerns the software solutions (on-premises-solution or cloud solution) of ATOSS Software AG used by the Customer.

To the extent that EMPAL processes personal data of the Customer's employees (hereinafter: commissioned data) in this context, the terms and conditions of the following agreement on commissioned data processing shall apply.

II. Preamble

Legal Basis: The legal basis is formed by the provisions of the EU General Data Protection Regulation (hereinafter: DS-GVO) and the Federal Data Protection Act as amended (hereinafter: BDSG). Unless expressly defined otherwise within the scope of this agreement, the terms used, e. g. "personal data", "processing", "responsible party" or "pseudonymization" have the same meaning as in Art. 4 DS-GVO.

Responsibility of the customer: The customer shall also be responsible within the scope of this agreement for compliance with the statutory provisions on data protection, in particular for the lawfulness transfer of data to EMPAL, for the lawfulness processing personal data by EMPAL as well as for the protection of the rights of the data subjects.

III. Agreement on Data Processing on order

§1 Subject matter and duration of processing

Subject matter: EMPAL provides services to the customer regarding the software products distributed by ATOSS Software AG. These services regularly also include matters of commissioned processing, as EMPAL processes personal data of the Customer, according to the instructions of and in the interest of the Customer during their performance. The agreement applies accordingly to (remote) testing and maintenance of automated processes or data processing systems if access to personal data of the Customer cannot be excluded in the process.

Duration: The term of this Agreement shall correspond to the duration of the cooperation of the parties based on the respective service agreements.

§2 Order content in detail

Types: The customer and EMPAL have a business relationship under which EMPAL provides services to the customer. In accordance with the underlying service agreement, these may include the following types:

- Customizing in the sense of parameterization of the standard software provided by ATOSS Software AG as an on-premises solution or as a cloud solution (support in creating employee master records in the database of the standard software provided to the customer by ATOSS Software AG for use, in setting up working time models and time accounts, etc.) and adaptation or scripting of standard interfaces.
- Software maintenance services relating to the standard software provided by ATOSS Software AG as an on-premises solution or as a cloud solution (support in the event of software release changes as well as in the elimination of malfunctions reported by the customer).
- Testing and maintenance work of automated processes or of data processing systems to ensure the operational readiness of the standard software provided as part of the Cloud Solution.
- Managed service performances concerning the administration of personal data according to the scope are defined in the respective individual contract (in particular active support in the administration of personal data of the customer's employees in the standard software provided by EMPAL).

Part of the service provision may also be:

- On-site at the customer's facility (according to the customer's choice by direct access to its IT systems or by establishing a connection between a client computer of EMPAL and the customer's IT systems), remote access via a suitable software solution for remote access provided by the customer (e.g. VPN, desktop sharing), which is executable on current Windows server operating systems (incl. necessary license).

In all cases, the possibility of read and write access by EMPAL to the order data located in the database of the standard software cannot be excluded.

Purpose: The purpose of the processing is to ensure the functionality and, if necessary, the up-to-dateness of the software solution provided to the Customer by EMPAL.

a) Categories of personal data

Generally, EMPAL processes the following categories of personal data provided by the customer within the scope of this contractual relationship. Which categories of personal data are processed in the respective contractual relationship depends on which data the customer specifically provides to EMPAL for processing.

- **Employee master data and time management information**
 - Master Data such as:
 - Personnel number
 - Title, surname, first name
 - Date of birth

- Card number(s) of the ID card(s)
 - Employee category (e.g. assignment to payroll model)
 - Other contract-relevant data such as entry, exit and regrouping data
 - Agreements on working time as well as start and end of time management consideration
 - Contact data (such as address, email, telephone numbers)
 - Employee photo
 - Other organizational characteristics
 - Information about affiliation to certain regions / countries / languages
 - Information about work locations and travel times
 - Information about supervisor, employee, and deputy relationships
 - Other personal data stored by end users in freely definable fields
 - Information about qualifications and training
 - Information about time balances / time accounts
 - Information about individual contractual, collective bargaining and other compensation, vacation and time off entitlements of employees:
 - general agreements
 - values and balances
 - Information on planned and actual absences
 - Information about bookings / clock-ins incl. time and place of booking / clock-ins
 - Information about actual attendance, (call) on-call and working hours
 - Information about affiliation to organizational units, projects, orders, cost centers, workplaces, etc. and the times worked for them
 - Canteen bookings
 - Manual annotations to master and transaction data
 - System warnings and error messages in case of deviations from specifications or rules
 - **Information from workforce planning**
 - Information about contractual and planning availability of employees
 - Information about planning requests of employees
 - Information on employee scheduling and actual-hours worked
 - Information about plan changes
 - Information about shift swaps of employees
 - Information about performance profiles of employees
 - **Request and task management**
 - Requests for absences incl. approval history and approval status
 - Requests for activities relevant to working time or duty scheduling, including approval history and approval status
 - Pending and completed tasks
 - Information about E-Mail and SMS notifications sent by the system
 - **Access management information**
 - Information about access authorizations for specific devices, zones, and time periods
 - Access identifiers
 - PIN for input at device
 - Identification features for biometric access security (fingerprint method, etc.)
 - Information on actual or attempted access or exiting of zones incl. time and place of booking
 - **Systemrelated information**
 - System access information
 - Information about authorizations for specific objects and interactions as a user of the system
 - Last used system settings and preferences
 - Logged in users of the system
 - Logon attempts
 - Logs of user interactions that modify data in the system.
- b) Categories of data subjects

The categories of persons affected by the processing include: Employees as defined in Section 26 (8) BDSG.

c) Material and local restriction of processing

Factual: EMPAL is not permitted to process order data beyond the scope of this agreement. Processing for other purposes, in particular the unauthorized transfer of order data to third parties, is not permitted. EMPAL is obliged to process the order data of different customers separately.

Locally: The provision of the contractually agreed data processing shall generally take place in a member state of the European Union (hereinafter: EU) or in another contracting state of the Agreement on the European Economic Area (hereinafter: EEA).

EMPAL will provide the contractually agreed service, if applicable, from the service locations agreed in Annex 2 through the approved subcontracted processors (see § 6).

These sub-processors are partly not located in a member state of the EU or in another contracting state of the EEA (hereinafter: third country). However, a data transfer to a sub-processor in a third country only takes place if the special requirements of Art. 44 et seq. DS-GVO (principles of transfer of personal data to third countries) are met beforehand (cf. § 6 para. (2) lit. b of this agreement).

§3 Technical and organizational measures

Ensuring data security: EMPAL shall observe the principles of proper data processing and monitor compliance with them (cf. Art. 5 DS-GVO). EMPAL assures that EMPAL complies with the regulations of Art. 28 para. 3 lit. c, 32 DS-GVO. EMPAL has taken appropriate data security measures and ensures an adequate level of protection regarding the confidentiality, integrity and resilience of the systems, while continuously making any necessary adjustments. In order to determine the appropriate level of protection, particular account shall be taken of the risks associated with processing, through destruction, loss or alteration, whether accidental or unlawful, or unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed. In doing so, the state of the art, implementation costs and the type, scope and purposes of the processing as well as the varying probability and severity of the risk to the rights and freedoms of individuals shall be continuously considered.

Documentation and submission of measures: EMPAL shall document the technical and organizational measures prior to the start of the processing with a view to the specific execution of the order and shall make this documentation available to the customer upon request.

Current state of the technology and technical adaptations: The technical and organizational measures are subject to technical progress and further development. In this respect EMPAL is permitted to implement alternative adequate measures. In doing so, the security level of the measures specified in this agreement must not be undercut. Significant changes to the technical and organizational measures shall be documented and communicated to the customer in a suitable manner, e.g. on an online portal accessible via EMPAL's website. In this case, EMPAL shall provide the customer with an updated description of these measures upon request, which shall enable the customer to verify compliance with the requirements of Section 3 (1) of this Agreement. By making these available, EMPAL grants the customer the opportunity to object to these changes within four weeks. The customer shall only be entitled to contradict if the changes do not comply with the requirements of § 3 para. 1 and § 3 para. 2 of this Agreement. If the customer does not object to the changes within the objection period, the consent to the changes shall be deemed granted. In the event of a contradiction, EMPAL may suspend the part of the service affected by the customer's contradiction.

§4 Authority to issue instructions

Documented instruction: The customer has the right to issue instructions to EMPAL regarding the type, scope and procedure of data processing. The customer shall decide solely and exclusively on the purposes and methods of processing the commissioned data. EMPAL may only process the order data according to the documented instructions of the customer, unless EMPAL is legally obligated to process such data.

Specificity and form of the instruction: Instructions must be given in a specific manner (law of instruction clarity). Instructions can be given in writing, in text form or, in urgent cases, verbally. Verbal instructions must be confirmed by the Customer in writing or in text form without delay.

Notification in case of illegality: EMPAL must inform the customer immediately if EMPAL considers an instruction to be unlawful. This duty to notify does not include a comprehensive legal examination. EMPAL is entitled to suspend the execution of the corresponding instruction until it is confirmed or changed by the customer.

Rights of the affected persons: EMPAL may only provide information to affected persons or third parties affected by the commissioned processing after prior instruction by the customer. If an affected person contacts EMPAL directly in this regard, EMPAL shall forward this request to the customer without delay.

Instructions outside the scope of the order: EMPAL shall decide on the execution of instructions of the customer which goes beyond the services regulated in this agreement. In this case EMPAL may claim separate remuneration.

Regress: Should EMPAL be exposed to a justified liability claim as a result of the implementation of an unlawful instruction, it may indemnify the customer to this extent.

§5 Obligation of confidentiality

Data and telecommunications secrecy: EMPAL and any person subordinate to EMPAL who has access to commissioned data shall be obliged to maintain confidentiality, in particular in accordance with the provisions of Art. 5 Para. 1 f), Art. 28 Para. 3 b), Art. 29 and Art. 32 Para. 4 DS-GVO as well as Art. 88 TKG. The obligation to confidentiality shall continue to exist after termination of this agreement.

Instruction of all persons used for commissioned processing: EMPAL shall ensure through appropriate measures such as trainings on data protection that the persons subordinate to it and authorized to process order data are familiar with the relevant provisions on data secrecy and telecommunications secrecy.

§6 Assignment of subcontracted processors

Definition of Subcontracted Processor: Subcontracted relationships within the meaning of these regulations are those services that relate directly to the provision of the main service. This does not include ancillary services which EMPAL provides, for example, as telecommunications services, postal/transport services, maintenance and user services or the disposal of documents and data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, EMPAL is obligated to implement appropriate and legally compliant contractual agreements as well as control measures to ensure data protection and the security of the customer's data, even in the case of outsourced ancillary services.

Conditions for the permissibility of commissioning: The commissioning of subcontracted processors shall only be possible with the consent of the customer.

- **General requirements:** Each sub-processor shall be required to undertake (on record), prior to commencement of the processing activities, to comply with the same data protection obligations as agreed in this agreement, unless expressly agreed otherwise.

The sub-processing agreement shall ensure at least the level of data protection required under this agreement. Each Sub-processor shall undertake to comply with the agreed technical and organizational security measures pursuant to Art. 32 DS-GVO and to provide EMPAL with a list of the implemented technical and organizational measures, which shall be made available to the customer upon request. The measures of the subcontracted processor may deviate from what has been agreed between the customer and EMPAL, but may not fall below the level of data protection ensured by EMPAL's measures. If a sub-processor refuses to submit to the same data protection obligations as set forth in this agreement, the customer may consent thereto, provided that such consent shall not be unreasonably withheld.

- **Sub-processors in third countries:** If a sub-processor is not established in a third country which provides an adequate level of data protection in accordance with Art. 45 DS-GVO, EMPAL will take sufficient account of this circumstance. EMPAL shall establish a contract for data processing on behalf with such sub-processor based on the EU standard contractual clauses (Decision 2021/914 - Module Three - Transfer of Processors to Processors) or other standard data protection clauses for processors, in addition to the provisions listed in (a) above, as far as they are permitted under Art. 46 (2) (c) DS-GVO. EMPAL is also entitled to conclude standard contractual clauses or other standard data

protection clauses on behalf of and in favour of the customer. The customer hereby authorizes EMPAL to conclude such an agreement in its own name.

- **Current Sub-Processors:** Regarding the affiliated companies of EMPAL within the meaning of §§ 15 et seq. AktG (German Stock Corporation Act) as well as the other subcontracted processors, all of which are listed in Annex 2 to this Agreement, the customer shall be deemed to have given its consent upon conclusion of this Agreement.
- **Further subcontracted processors:** The further outsourcing to subcontracted processors or the change of existing subcontracted processors are permissible under the conditions of § 6 para. 2 of this agreement also without separate consent of the customer, provided that EMPAL notifies the customer of the outsourcing to (other) subcontracted processors in text form in an appropriate time in advance and the following provisions are fulfilled. Alternatively, EMPAL may provide a website or other form of notification listing all sub-processors accessing customer's personal data and the limited or ancillary services they provide. At least two weeks prior to approving access to personal data by a new sub-processor, EMPAL will notify customer of this and, if relevant, update the website. By notifying the customer, EMPAL grants the customer the right to object to the change within two weeks for justified reasons. If the customer does not object within this objection period, the consent shall be deemed granted. Upon the customer's request, EMPAL shall provide all necessary information to prove that the sub-processor complies with all data protection requirements of this agreement. If the customer objects to the outsourcing, EMPAL may choose not to commission the sub-processor or to terminate the service agreement in writing with a notice period of two months.
- **Validity of the provisions of this agreement also for subcontracted processors:** Upon request of the customer, EMPAL shall provide the customer with information on relevant data protection obligations of the subcontracted processor, which shall include, but not be limited to, granting the necessary access to the relevant contractual documents. EMPAL shall regularly review its sub-processors and shall confirm compliance with data protection law and the obligations of the sub-processor under the contract processing agreement concluded with it at the request of the customer. Only if there are justified reasons, the customer shall be entitled to issue instructions to EMPAL to carry out further checks, which EMPAL shall carry out within the scope of what is permissible.

§7 Obligations and rights of the Customer; support of the Customer by EMPAL

The customer shall be obligated to protect the rights of the affected person (Art. 12 et seq. DS-GVO or §§ 32 et seq. BDSG), to take technical and organizational measures, to report and notify in case of data breaches, to cooperate with the supervisory authority (Art. 32 to 36 DSGVO) and to ensure quality (Art. 28 para. 1 DS-GVO). EMPAL supports the customer in complying with these obligations. In this context, it shall provide it with all information insofar as the customer does not have this information itself. EMPAL is not obliged to procure information for the purpose of support which it does not have itself. EMPAL shall support the customer as follows:

- **Preservation of the rights of the affected persons:** The Customer shall be responsible for preserving the rights of the affected persons. To the extent necessary, EMPAL shall support the customer in the event of the exercise of rights by the affected persons.

Technical and organizational measures: EMPAL shall support the customer in ensuring an appropriate level of protection by technical and organizational measures that consider the circumstances and purposes of the processing as well as the predicted probability and severity of a possible infringement of rights due to security breaches and allow for a timely detection of relevant infringement events. In this context, the customer shall ensure in a suitable form, appropriate to the need for protection, that the software solutions provided by EMPAL as well as the associated technical interfaces are secured against unauthorized access (e.g., by assigning only temporarily valid access IDs and / or regular password changes and / or restrictions of the IP address range authorized for access or other comparable measures).

Reporting- and notification obligation: In the event of a breach of the protection of order data by EMPAL, EMPAL shall be obliged to notify the customer regarding to its

- obligation to notify the competent supervisory authority and
- obligation to notify the persons concerned.

In the event of a serious operational disruption, suspected data protection violations or violations of this agreement, whether caused by the customer, a third party or EMPAL, EMPAL shall immediately and fully inform the customer of the time, type and scope of the affected order data. The customer shall be provided with all relevant information for the fulfilment of the reporting obligation to the supervisory authority without delay.

Cooperation with the Supervisory Authority: The parties shall cooperate with the competent supervisory authority in the performance of its duties to the extent necessary in accordance with the following principles.

- **Logging of Processing Operations:** Both parties undertake to access the order data located in the database of the software solutions provided by EMPAL in each case exclusively using separate User-IDs. This requires that the customer assigns EMPAL separate User-IDs for use in the context of the order processing and/or cooperates in the creation of such User-IDs to the extent required. EMPAL shall make access identifications available exclusively to the persons concerned and, if applicable, to an employee responsible for the administration of the access identifications and shall secure them against unauthorized inspection and/or use by taking suitable and appropriate measures.
- **Control Actions at EMPAL or customer:** EMPAL shall inform the customer without delay about control actions and measures of the supervisory authority as far as they relate to this order. This shall also apply as far as a competent authority investigates within the scope of administrative offence or criminal proceedings regarding the processing of commissioned data during the commissioned processing at EMPAL.

To the extent that the Customer, for its part, is subject to an inspection by the supervisory authority, administrative offense or criminal proceedings, the liability claims of a affected person or a third party or any other claim in connection with the Order Processing at EMPAL, EMPAL shall support it to the best of its ability.

- **Data Protection Impact Assessment:** To the extent that there is a legal obligation for the customer to prepare a data protection impact assessment, EMPAL shall support the customer in carrying out the data protection impact assessment as well as in any required prior consultation with the supervisory authority to the extent necessary. This includes the transmission of any required documents at the corresponding request of the customer.

IV. Quality Assurance

Inspections: The customer shall have the right to convince himself of EMPAL's compliance with the legal obligations and the obligations assumed in this agreement in the course of business operations during normal business hours by means of spot checks which must be notified to EMPAL with a reasonable lead time. The customer may carry out these inspections himself or have them carried out at his expense by third parties to be named by him and bound to confidentiality in accordance with § 5 of this agreement. Third parties in this sense may not be representatives of competitors of EMPAL. EMPAL may object to the review by an external auditor if the auditor selected by the customer is in a competitive relationship with EMPAL.

Documentation: EMPAL shall ensure that the customer can convince itself of EMPAL's compliance with its obligations under Article 28 of the GDPR in the context of the commissioned processing. EMPAL commits to provide the customer with the necessary information upon request and, in particular, to provide the documentation of the technical and organizational measures.

Proof of the documentation of the technical and organizational measures can thereby also be provided through compliance with approved rules of conduct pursuant to Art. 40 DS-GVO or suitable certification through an IT security or data protection audit.

Data protection officer: The contact details of the data protection officer can be found on the website www.empal-consulting.com.

Other support services: EMPAL may claim separate compensation for other support services not included in the Service Agreements or not resulting from EMPAL's misconduct.

§8 Deletion or return after completion of processing

Electoral Law: Upon completion of the contractually agreed work or earlier upon request by the customer - latest with termination of the service agreements - EMPAL shall return to the customer at its own expense all documents, data carriers, created processing and utilization results as well as data files related to the commissioned processing, or shall delete or destroy them in accordance with data protection requirements, at the customer's discretion. The same applies to test and reject material.

Copies of the commissioned data: Copies or duplicates of the order data shall not be made without the knowledge of the customer. Exceptions to this are security copies, as far as these are necessary to ensure proper data processing, the production and intermediate storage of screenshots of order data within the framework of the parameterized standard software on IT systems of EMPAL for the purpose of error analysis concerning malfunctions reported by the Customer, as well as data which are necessary regarding the compliance with statutory retention obligations.

Retention periods: Documentation which serves as proof of orderly and proper data processing shall be retained by EMPAL beyond the end of the contract in accordance with the respective statutory retention periods. EMPAL may hand them over to the customer at the end of the contract in order to relieve the customer.

Costs: The customer shall be liable for any additional costs incurred as a result of the customer's instructions which deviate from or go beyond the provisions of this § 8 Para.

§9 Liability

External liability: The customer and EMPAL shall each be liable for damages of affected persons pursuant to Art. 82 DS-GVO (external liability).

Internal liability: Each party is entitled to reclaim from the other party that part of the indemnity which corresponds to the part of the other party's responsibility for the damage (internal liability).

Liability Agreement: Regarding the internal liability and without an effect on the external liability towards the affected persons, the parties agree that, regardless of the provisions contained herein, EMPAL's liability for the breach of this Order Processing Agreement shall be subject to the limitations of liability agreed in the Service Agreement. The customer shall defend, indemnify and hold EMPAL harmless from and against all claims and damages in excess of the limitations of liability set forth in the Framework Agreement, to the extent EMPAL has suffered such damages in connection with claims by affected persons based on an alleged breach of provisions of the GDPR or this Order Processing Agreement.

§10 Final Clauses

Replacement clause; amendments and additions: This agreement shall enter into validity with the signing of the Service Agreement on which the commissioned data processing is based and shall replace all existing agreements on commissioned (data) processing between the parties within its scope of application upon its entry into validity.

All amendments and supplements to this agreement as well as all ancillary agreements must be executed in writing or in text form in order to be effective.

Non-applicability of the Customer's General Terms and Conditions of Business / Purchase: It is agreed between the parties that "General Terms and Conditions of Business" and / or "General Terms and Conditions of Purchase" of the customer shall not apply to this agreement.

Exclusion of § 273 BGB (German Civil Code): The objection of the right of retention according to §273 BGB is excluded regarding to the processed order data and the associated data carriers.

Obligation of confidentiality: The parties undertake to treat as confidential all knowledge of trade and business secrets and data security measures of the other party obtained during processing the order. Trade and business secrets are considered to be all facts, facts and processes relating to the company of one of the parties which are not in the public domain but are only accessible to a limited group of persons and in the non-disclosure of which the party concerned has a justified interest. Data security measures are all technical and organizational measures taken by a party as defined in Annex 1 to this agreement. This confidentiality obligation shall continue after termination of this agreement.

Obligation to inform in case of endangerment of the order data: If the order data at EMPAL is endangered by seizure, by confiscation, by insolvency-/ composition proceedings, measures of third parties, or by other events EMPAL is obliged to inform the customer thereof without delay.

Place of jurisdiction: The sole place of jurisdiction for all disputes arising from and in connection with this agreement shall be Stuttgart, subject to any exclusive statutory place of jurisdiction.

Applicable law: This agreement shall be governed by German law.

Severability clause: If singular parts of this agreement are or become invalid or unenforceable in whole or in part, this shall not affect the validity of the remaining provisions. The parties undertake to replace the invalid or unenforceable provision with a valid and enforceable provision that comes as close as possible to the originally intended meaning and purpose of the invalid or unenforceable provision. This shall apply accordingly in the event of a loophole.