Order Processing Agreement According to Art. 28 GDPR

between

the responsible

and

EXEC IT Solutions GmbH
Südstraße 24
56235 Ransbach-Baumbach

(Processor)

together "the parties“

Note: generally the Order Processing Agreement in German language apply and not this English translation.

Content

1 General

[1] This Supplementary Agreement sets out in more detail the obligations of the Parties under data protection law arising from the respective main agreements concluded between the Parties.

[2] It shall apply to all activities in which the Processor collects, processes and/or uses personal data on behalf of the Controller. The following regulations are to be understood as a supplement to the main contracts.

[3] This Agreement uses the terms and definitions used by the European Directive and Regulation Maker when adopting the General Data Protection Regulation (GDPR).

[4] This agreement replaces all previous data protection regulations between the parties regarding the processing of personal data by the commissioned processor on behalf of the controller.

2 Subject matter and duration of the commissioned processing

[1] The subject of this agreement is the processing of personal data exclusively for the performance of the services by the processor for the controller as described in more detail in the respective main contracts.

[2] The provision of the contractually agreed data processing takes place exclusively in Germany.

[3] The nature and purpose of the processing as well as the type of personal data and the categories of data subjects are set out in the lists of processing activities to be kept by the controller pursuant to Article 30 (1) of the GDPR. The categories of processing operations result from the lists of processing activities to be kept by the processor pursuant to Article 30 (2) of the GDPR. These can be found in the annex to this agreement.

[4] The duration of the respective commissioned processing corresponds to the duration of the respective main contract.

3 Bound by instructions

[1] The Processor and And the individual person subordinated to him who have access to personal data shall process the personal data only on the documented instructions of the Controller. This shall not apply to situations in which the Processor or the natural person under its control is required to process data for compelling legal reasons. In such situations, the Processor shall inform the Controller of the relevant legal requirements prior to the start of the processing, unless the relevant law prohibits such notification.

[2] The responsible person shall confirm verbal instructions in text form without delay.

[3] The Processor shall inform the Controller without delay if it is of the opinion that an instruction violates the GDPR or other relevant data protection provisions or other legal bases. The Processor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Controller.

4 Duties of the Processor

[1] The processor shall ensure that the persons authorized to process personal data have committed themselves to confidentiality.

[2] The Processor shall, where possible, and taking into account the nature of the processing, support the Controller with appropriate technical and organizational measures to comply with its obligation to respond to requests for the exercise of the data subject's rights referred to in Chapter III of the GDPR.

[3] The Processor shall assist the Controller in complying with the obligations referred to in Articles 32 to 36, taking into account the nature of the Processing and the information available to the Processor.

[4] Upon completion of the Processing Services, the Processor shall, at the Controller's option, either delete or return all Personal Data, unless there is an obligation to store the Personal Data due to mandatory legal provisions.

[5] In accordance with Article 30 of the GDPR, the Processor shall keep a list of all processing activities for which it is responsible.

[6] If the Processor becomes aware of a personal data breach, it shall notify the Controller thereof without delay.

5 Duties of the responsible party

[1] The Controller is solely responsible for assessing the permissibility of data processing and for safeguarding the rights of the data subjects. The controller shall ensure within its responsibility that the legally necessary prerequisites are created so that the processor can provide the agreed services without violating the law (e.g. by obtaining consent for the processing of the data). Vis-a-vis streichen und durch ein einfaches "to" ersetzen.

[2] The controller is responsible for the information obligations resulting from Art. 33, 34 GDPR to the supervisory authority or the persons affected by a personal data breach.

[3] Pursuant to Art. 30 GDPR, the controller shall keep a register of all processing activities under its responsibility.

[4] The Controller is obliged to treat all knowledge of trade secrets and data security measures of the Processor obtained within the framework of the contractual relationship as confidential .

[5] The Controller shall inform the Processor immediately and in full if errors or irregularities, in particular with regard to data protection provisions, are discovered during the examination of the results of the order.

6 Data protection officer

If one of the parties is obliged to appoint a data protection officer in accordance with Article 37 of the GDPR or other relevant legal provisions, it shall notify the other party of the data protection officer's contact details and any changes to these details, cf. Annex 1.

7 Cooperation with the Regulatory Authority

The Controller and Processor shall cooperate with the Supervisory Authority in the performance of their duties upon request.

8 Technical-organizational measures

[1] Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of individual persons, the controller and processor shall implement appropriate technical and organisational measures to ensure a level of protection appropriate to the risk, in accordance with Article 32 GDPR.

[2] Compliance with approved rules of conduct pursuant to Art. 40 or an approved certification procedure pursuant to Art. 42 GDPR may be used to demonstrate compliance with these measures.

[3] The technical and organisational measures are subject to technical progress and further development. In this respect, the processor is permitted to implement alternative adequate

measures. In doing so, the security level of the specified measures must not be undercut. Significant changes must be documented.

[4] A description of the respective technical and organisational measures taken by the Processor can be found in the Annexes to this Agreement.

9 Control rights

[1] The Processor shall provide the Controller with all the information necessary to demonstrate compliance with the obligations set out in this Agreement and shall enable and contribute to verifications - including inspections - carried out by the Controller or another auditor appointed by the Controller.

[2] To this end, the Controller shall have the right, in consultation with the Processor, to carry out inspections or to have them carried out by a competent third party to be named in the individual case, who is bound to secrecy and who may not be in a competitive relationship with the Processor. It shall have the right to satisfy itself of the Processor's compliance with this Agreement by means of spot checks, which must generally be notified in good time, without disrupting the Processor's business operations, insofar as this is indicated for urgent reasons, but not more frequently than every 12 months.

[3] The Processor shall ensure that the Controller can satisfy itself of the Processor's compliance with its obligations under Article 28 GDPR. The Processor is committed to provide the Controller with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organisational measures. Proof of such measures may be provided by

a. compliance with approved codes of conduct (Art. 40 GDPR)

b. certification in accordance with an approved certification procedure (Art. 42 GDPR)

c. current certificates, reports, report extracts from independent instances (e.g. auditors)

d. appropriate certification by IT security or data protection audit (e.g. BSI-Grundschutz) take place.

[4] The Controller shall inform the Processor immediately and completely if it discovers errors or irregularities during the audit, in particular with regard to data protection provisions.

10 Subcontractors

[1] The Processor shall be entitled to use the services of other Processors as stated in the description of services. In doing so, it shall always inform the Controller of any intended change with regard to the use or replacement of other Processors. In this case, the controller shall be given the opportunity to object to such changes.

[2] Where the processor uses the services of another processor to carry out certain processing activities on behalf of the controller, the same data protection obligations as those laid down in this contract between the controller and the processor shall be imposed on that other processor by way of a contract. In particular, sufficient guarantees must be provided that the appropriate technical and organisational measures are implemented in such a way that the processing is carried out in accordance with the requirements of this contract.

11 Liability

[1] The controller and the processor shall be jointly and severally liable to the data subject for any damage caused by a processing operation which does not comply with the GDPR (Article 82 GDPR).

[2] [2] The processor shall be liable for the damage caused by a processing operation in accordance with Article 82(2) of the GDPR only if it

a. has failed to comply with its obligations under the GDPR specifically imposed on processors; or

b. has acted in disregard of the lawfully given instructions of the data controller; or

c. acted contrary to those instructions.

[3] If a data subject asserts a claim against the Processor pursuant to paragraph 1, the Controller shall indemnify the Processor upon first request, unless the Controller proves a breach of the Processor's obligations pursuant to paragraph 2 in the internal relationship.

[4] In the internal relationship, the following shall also apply to the Processor's liability towards the Controller for damage resulting from a breach of this Agreement caused by the Processor:

a. In the event of breaches due to intent or gross negligence as well as breaches of the Product Liability Act, the Processor shall be liable without limitation.

b. In addition, the Processor shall only be liable in the event of a breach of a material obligation under this Agreement and only to the extent of the damage typically foreseeable at the time of the conclusion of the Agreement.

[5] This liability clause shall apply with equal priority to other liability provisions made between the parties, in particular in main contracts..

12 Remuneration

The Processor may claim reasonable remuneration from the Controller for any performance under this Agreement which is not already part of the performance of the relevant main contract and which is not due to the Processor's misconduct.

13 Duration of contract

[1] This agreement is concluded for an indefinite period. It may be terminated by either party with 3 months' notice to the end of the year.

[2] Termination of this Agreement shall not affect the validity and term of any principal contracts.

[3] If termination of this Agreement by the Controller - through no fault of the Processor - results in the Processor no longer being able to fulfil its performance obligation under a Principal Contract, the Processor shall be released from the performance obligation with regard to the scope and duration of this restriction, without this releasing the Controller from the payment of the remuneration agreed in the Principal Contract.

14 Other

[1] If the data of the data controller at the data processor are endangered by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the data processor shall immediately inform the data controller thereof. The Processor shall immediately inform all relevant parties in this context that sovereignty and ownership of the data lies exclusively with the Controller.

[2] Amendments and supplements to this agreement must be made in writing. This shall also apply to any disclaimer of this formal requirement.

[3] Should a provision of this agreement be or become invalid, or should a provision which is necessary in itself not be included, the validity of the remaining provisions of this agreement shall not be affected thereby.

[4] German law shall apply to the exclusion of the UN Convention on Contracts for the International Sale of Goods.

[5] The place of jurisdiction is Montabaur, unless the law mandatorily prescribes otherwise.

(Effective: 01.03.2023)

Data Protection Officer of the Processor

(Effective: 01.03.2023)

IT Process & Audit GmbH Wirtschaftsprüfungsgesellschaft
Mr. Thomas Martin
Bruder-Kremer-Straße 6
65549 Limburg a. d. Lahn
E-mail: datenschutzbeauftragter@exec.de
Phone: +49 (6431) 969-200

Directory of processing activities (processor) pursuant to Article 30 (2) GDPR

Name of the processing activity	Operation of hardware and software
Processor **(Art. 30 para. 2 lit. a GDPR)**	EXEC IT Solutions GmbH Südstraße 24 56235 Ransbach-Baumbach Phone: 02623 9879 0 E-mail: info@exec.de
Data Protection Officer **(Art. 30 para. 2 lit. a DSGVO)**	See Order Processing Agreement as amended from time to time.
Person responsible (principal) **(Art. 30 para. 2 lit. a DSGVO)**	Name and contact details see individual contract
Categories of processing carried out on behalf. **(Art. 30 para. 2 lit. b DSGVO)**	Operation of the systems listed in the respective individual contract in a computer centre. The operation of the systems includes the provision and monitoring of the required remote access, the server hardware and the system software.
If applicable, transfer of personal data to a third country or to an international organisation **(Art. 30 para. 2 lit. c DSGVO)**	Such data transmission does not take place.
Technical and organisational measures (TOM) pursuant to Art. 32 (1) DSGVO **(Art. 30 para. 2 lit. d DSGVO)**	s. TOM „Operation“
Valid from	1.6.2022

Technical-organisational measures

- Operation -

Version:	1.4
status:	14.12.2022
next validation:	01.02.2025

erstellt von:

EXEC IT Solutions GmbH
Südstraße 24
56235 Ransbach-Baumbach
www.exec.de

Inhalt

1 Scope of application

[1] This document describes the technical and organisational measures pursuant to Article 32 of the EU General Data Protection Regulation (GDPR) that EXEC IT Solutions GmbH (EXEC) takes as a processor pursuant to Article 30 (2) (d) in the context of processing on behalf of a controller pursuant to Article 28 (3) (c) of the GDPR.

[2] The technical and organisational measures described here apply to the following categories of activities carried out by EXEC as a processor on behalf of a controller:

a. Operation of software in a data centre commissioned by EXEC

2 Pseudonymisation

Pseudonymisation is only carried out on the instructions of the person responsible to the extent determined by him/her at times defined by him/her.

3 Encryption

Measures for the encryption of personal data:

a. All data transmission shall take place via encrypted lines.

b. All mobile workstations (notebooks) are provided with encrypted data carriers.

c. Data shall be stored on encrypted media.

4 Ensuring confidentiality

[1] Physical access control measures that prevent unauthorised persons from physically approaching the systems, data processing equipment or procedures with which personal data are processed:

a. Key management/documentation of key allocation

b. Access control system

c. Door locks

d. Plant security/ gatekeeper

e. Alarm system

f. Video surveillance

g. Special protective measures of the server room

h. Restricted areas

[2] Access control measures that ensure that unauthorised access to data processing systems is prevented:

a. Personal and individual user login when logging on to the system or company network.

b. Password procedure

c. BIOS passwords

d. Additional system login for certain applications

e. Automatic locking of clients after a certain period of time without user activity

f. Regular software updates / patching

g. Regular vulnerability scans

[3] Access control measures that ensure that those authorised to use a data processing system can only access the data under their access authorisation and that personal data cannot be read, copied, modified or removed without authorisation during processing:

a. Inventory of information technology

b. Administration and documentation of authorisations

c. Differentiated authorisations

d. Task-related profiles

e. Task-related roles

f. Approval routines

g. Regularly checking that access rights are up to date

h. Evaluations/ logging

i. Testing/auditing

j. Encryption of external data carriers and laptops

k. Password identification

l. Logging of access to systems

m. Monitoring access to systems

[4] Transfer control measures to ensure that personal data cannot be read, copied, modified or removed by unauthorised persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which bodies personal data are intended to be transferred by means of data transmission equipment:

a. Encryption of external data carriers and laptops

b. Tunneled remote data connections (VPN = Virtual Private Network)

c. Secured WLAN

d. SSL/TLS encryption

e. Regulations for the destruction of data media

5 Ensuring integrity

[1] Input control measures which ensure that it is possible to verify and establish ex post whether and by whom personal data have been entered into, altered or removed from data processing systems:

a. Access rights

b. System logging

c. Functional responsibilities

[2] Job control measures that ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions:

a. Binding security guidelines

b. Training of all employees with access rights

c. Regular follow-up training

d. Regular data protection audits by the company data protection officer.

[3] Measures to comply with the separation requirement that ensure that data collected for different purposes can be processed (e.g. deleted) separately:

a. Separate databases

b. Rights and role concepts

c. Separation through access regulations

6 Ensuring availability

Availability control measures that ensure that personal data is protected against accidental destruction or loss or can be recovered quickly:

a. Service Level Agreements (SLAs) with service providers

b. Backup procedures

c. Virus/malware protection

d. Secure storage for backups

e. Redundancy

f. redundant supply

g. Suitable archiving facilities

h. Firewall, IDS/IPS

i. Fire protection and extinguishing water protection

j. Monitoring of alarms

k. Failure/ disaster/ recovery plans

7 Ensuring the resilience of the systems

Measures and responsibilities to ensure the resilience of the systems and services related to the processing on an ongoing basis:

a. Automated monitoring of the systems

b. Thresholds to identify problem situations and load

c. Regular adjustment of system resources to ensure agreed performance

8 Restoring availability

Measures and responsibilities to rapidly restore the availability of and access to personal data in the event of a physical or technical incident:

a. Contingency plans

b. Conduct emergency drills

9 Periodic review, assessment and evaluation

Measures and responsibilities to periodically review, assess and evaluate the effectiveness of the technical and organisational measures to ensure the security of the processing:

a. Regular review of logged accesses

b. Regular evaluation of the measures by an IT security officer