Data Processing Agreement (Art 28 GDPR)

This data processing agreement ("DPA") applies to all processing of personal data carried out by TECHWAVE GmbH, Linke Wienzeile 4/2/DG2, AT-1060 Vienna ("TECHWAVE"), on behalf of one or more controller(s) or processor(s) ("CUSTOMER") (together, the "PARTIES"), on the basis of an underlying service contract relating to the provision of IT services ("SERVICE AGREEMENT").

The DPA applies whenever, in the course of delivering services under the SERVICE AGREEMENT, personal data of the CUSTOMER is processed, and becomes an integral part of the SERVICE AGREEMENT to that extent. It is within the obligations of the CUSTOMER to ensure that only the personal data necessary for the processing is transmitted to TECHWAVE. If the personal properties of data, which is transmitted by the CUSTOMER to TECHWAVE, are not actually required for the processing purpose, the CUSTOMER shall implement appropriate data masking procedures for those personal data fields that are not needed.

For the purposes of this agreement, the CUSTOMER is to be regarded as a controller, processor, or sub-processor within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, "GDPR"). The CUSTOMER instructs TECHWAVE, within the scope of the SERVICE AGREEMENT, to act as a processor (if the CUSTOMER qualifies as a controller under Art. 4(7) GDPR) or as a sub-processor (if the CUSTOMER itself qualifies as a (sub-)processor under Art. 4(8) GDPR) for the processing of certain personal data in accordance with the service description defined in the SERVICE AGREEMENT.

1 Clauses on Data Processing

Any conflicting terms or data-protection agreements between the CUSTOMER and any third parties (including related agreements on data processing on behalf) shall not affect the contractual provisions set out in this section.

1.1 Purpose and Scope

(1) The purpose of these standard contractual clauses („CLAUSES") is to ensure compliance with Article 28 (3) and (4) GDPR.
(2) The PARTIES listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) GDPR.
(3) These CLAUSES apply to the processing of personal data as specified in Annex II of the DPA.
(4) „Annex I", „Annex II", „Annex III" and „Annex IV" of the DPA are an integral part of the CLAUSES.
(5) These CLAUSES are without prejudice to obligations to which the CUSTOMER is subject by virtue of GDPR.
(6) These CLAUSES do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of GDPR.

1.2 Invariability of the Clauses

(1) The PARTIES undertake not to modify the CLAUSES, except for adding information to the Annexes or updating information in them
(2) This does not prevent the PARTIES from including the standard contractual clauses laid down in these CLAUSES in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the CLAUSES or detract from the fundamental rights or freedoms of data subjects.

1.3 Interpretation

(1) Where these CLAUSES use the terms defined in GDPR respectively, those terms shall have the same meaning as in the GDPR.
(2) These CLAUSES shall be read and interpreted in the light of the provisions of the GDPR respectively.
(3) These CLAUSES shall not be interpreted in a way that runs counter to the rights and obligations provided for in the GDPR or in a way that prejudices the fundamental rights or freedoms of the data subjects.

1.4 Hierarchy

(1) In the event of a contradiction between these CLAUSES and the provisions of related agreements between the PARTIES existing at the time when these CLAUSES are agreed or entered into thereafter, these CLAUSES shall prevail.

1.5 Docking Clause

(1) Any entity that is not a Party to these CLAUSES may, with the agreement of all the PARTIES, accede to these CLAUSES at any time as a controller or a processor by completing the Annexes and signing Annex I.
(2) Once the Annexes referred in section 1.5 are completed and signed, the acceding entity shall be treated as a Party to these CLAUSES and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.
(3) The acceding entity shall have no rights or obligations resulting from these CLAUSES from the period prior to becoming a Party.

1.6 Description of Processing(s)

(1) The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the CUSTOMER, are specified in Annex II of this DPA.

1.7 Obligations of the Parties

1.7.1 Instructions

(1) TECHWAVE shall process personal data only on documented instructions from the CUSTOMER, unless required to do so by Union or Member State law to which TECHWAVE is subject. In this case, TECHWAVE shall inform the CUSTOMER of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the CUSTOMER throughout the duration of the processing of personal data. These instructions shall always be documented.
(2) TECHWAVE shall immediately inform the CUSTOMER if, in TECHWAVE's opinion, instructions given by the CUSTOMER infringe the GDPR or the applicable Union or Member State data protection provisions.

1.7.2 Purpose Limitation

(1) TECHWAVE shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II of the DPA, unless TECHWAVE receives further instructions from the CUSTOMER.

1.7.3 Duration of the Processing of Personal Data

(1) Processing by TECHWAVE shall only take place for the duration specified in Annex II of the DPA.

1.7.4 Security of Processing

(1) TECHWAVE shall at least implement the technical and organisational measures specified in Annex III of the DPA to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (hereafter "PERSONAL DATA BREACH"). In assessing the appropriate level of security, the PARTIES shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.
(2) TECHWAVE shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the SERVICE AGREEMENT. TECHWAVE shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

1.7.5 Sensitive Data

(1) If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereafter "SENSITIVE DATA"), TECHWAVE shall apply specific restrictions and/or additional safeguards.

1.7.6 Documentation and Compliance

(1) The PARTIES shall be able to demonstrate compliance with these Clauses.
(2) TECHWAVE shall deal promptly and adequately with inquiries from the CUSTOMER about the processing of data in accordance with these CLAUSES.
(3) TECHWAVE shall make available to the CUSTOMER all information necessary to demonstrate compliance with the obligations that are set out in these CLAUSES and stem directly from the GDPR. At the CUSTOMER's request, TECHWAVE shall also permit and contribute to audits of the processing activities covered by these CLAUSES, at reasonable intervals

or if there are indications of non-compliance. In deciding on a review or an audit, the CUSTOMER may take into account relevant certifications held by TECHWAVE.

(4) The CUSTOMER may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of TECHWAVE and shall, where appropriate, be carried out with reasonable notice.

(5) The PARTIES shall make the information referred to in this clause, including the results of any audits, available to the competent supervisory authority/ies on request.

1.7.7 Use of Sub-Processors

(1) TECHWAVE has the CUSTOMER's general authorisation for the engagement of sub-processors which are listed in "Annex IV" of the DPA. TECHWAVE shall specifically inform in writing the CUSTOMER of any intended changes of that list through the addition or replacement of sub-processors at least two weeks in advance, thereby giving the CUSTOMER sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). TECHWAVE shall provide the CUSTOMER with the information necessary to enable the controller to exercise the right to object.

(2) Where TECHWAVE engages a sub-processor for carrying out specific processing activities (on behalf of the CUSTOMER), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on TECHWAVE in accordance with these CLAUSES. TECHWAVE shall ensure that the sub-processor complies with the obligations to which TECHWAVE is subject pursuant to these CLAUSES and to the GDPR.

(3) At the CUSTOMER's request, TECHWAVE shall provide a copy of such a sub-processor agreement and any subsequent amendments to the CUSTOMER. To the extent necessary to protect business secret or other confidential information, including personal data, TECHWAVE may redact the text of the agreement prior to sharing the copy.

(4) TECHWAVE shall remain fully responsible to the CUSTOMER for the performance of the sub-processor's obligations in accordance with its contract with TECHWAVE. TECHWAVE shall notify the CUSTOMER of any failure by the sub-processor to fulfil its contractual obligations.

(5) TECHWAVE shall agree a third party beneficiary clause with the sub-processor whereby - in the event TECHWAVE has factually disappeared, ceased to exist in law or has become insolvent - the CUSTOMER shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

1.7.8 International Transfer

(1) Any transfer of data to a third country or an international organisation by TECHWAVE shall be done only on the basis of documented instructions from the CUSTOMER or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of the GDPR.

(2) The CUSTOMER agrees that where TECHWAVE engages a sub-processor in accordance with section 1.7.8 for carrying out specific processing activities (on behalf of the CUSTOMER) and those processing activities involve a transfer of personal data within the meaning of Chapter V of the GDPR, TECHWAVE and the sub-processor can ensure compliance with Chapter V of the GDPR by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) GDPR, provided the conditions for the use of those standard contractual clauses are met.

1.8 Assistance to the CUSTOMER

(1) TECHWAVE shall promptly notify the CUSTOMER of any request TECHWAVE has received from the data subject. TECHWAVE shall not respond to the request itself, unless authorised to do so by the CUSTOMER.

(2) TECHWAVE shall assist the CUSTOMER in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with clause 1.8.1 and 1.8.2, TECHWAVE shall comply with the CUSTOMER's instructions

(3) In addition to TECHWAVE's obligation to assist the CUSTOMER pursuant to clause 1.8.2, TECHWAVE shall furthermore assist the CUSTOMER in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to TECHWAVE:

a. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a "DATA PROTECTION IMPACT ASSESSMENT") where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

b. the obligation to consult the competent supervisory authority/ies prior to processing where a DATA PROTECTION IMPACT ASSESSMENT indicates that the processing would result in a high risk in the absence of measures taken by the CUSTOMER to mitigate the risk;

c. the obligation to ensure that personal data is accurate and up to date, by informing the CUSTOMER without delay if TECHWAVE becomes aware that the personal data it is processing is inaccurate or has become outdated;
d. the obligations in Article 32 GDPR.

(4) The PARTIES shall set out in Annex III of the DPA the appropriate technical and organisational measures by which TECHWAVE is required to assist the CUSTOMER in the application of this clause as well as the scope and the extent of the assistance required.

1.9 Notification of Personal Data Breach

(1) In the event of a PERSONAL DATA BREACH, TECHWAVE shall cooperate with and assist the CUSTOMER for the CUSTOMER to comply with its obligations under Articles 33 and 34 GDPR where applicable, taking into account the nature of processing and the information available to the TECHWAVE.

1.9.1 Data Breach concerning Data Processed by the CUSTOMER

In the event of a PERSONAL DATA BREACH concerning data processed by the CUSTOMER, TECHWAVE shall assist the CUSTOMER:

(1) in notifying the PERSONAL DATA BREACH to the competent supervisory authority/ies, without undue delay after the CUSTOMER has become aware of it, where relevant/(unless the PERSONAL DATA BREACH is unlikely to result in a risk to the rights and freedoms of natural persons);
(2) in obtaining the following information which, pursuant to Article 33 (3) GDPR, shall be stated in the CUSTOMER's notification, and must at least include:
   a. the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   b. the likely consequences of the PERSONAL DATA BREACH;
   c. the measures taken or proposed to be taken by the CUSTOMER to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

   Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
(3) in complying, pursuant to Article 34 GDPR, with the obligation to communicate without undue delay the PERSONAL DATA BREACH to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

1.9.2 Data breach concerning data processed by TECHWAVE

(1) In the event of a PERSONAL DATA BREACH concerning data processed by TECHWAVE, TECHWAVE shall notify the CUSTOMER without undue delay after TECHWAVE having become aware of the breach. Such notification shall contain, at least:
   a. a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
   b. the details of a contact point where more information concerning the PERSONAL DATA BREACH can be obtained;
   c. its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.
(2) Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
(3) The PARTIES shall set out in Annex III of the DPA all other elements to be provided by TECHWAVE when assisting the CUSTOMER in the compliance with the CUSTOMER's obligations under Articles 33 and 34 GDPR.

1.10 Non-compliance with the CLAUSES and Termination

(1) Without prejudice to any provisions of the GDPR, in the event that TECHWAVE is in breach of its obligations under these CLAUSES, the CUSTOMER may instruct TECHWAVE to suspend the processing of personal data until the latter complies with these CLAUSES or the SERVICE AGREEMENT is terminated. TECHWAVE shall promptly inform the CUSTOMER in case it is unable to comply with these CLAUSES, for whatever reason.

(2) The CUSTOMER shall be entitled to terminate the SERVICE AGREEMENT insofar as it concerns processing of personal data in accordance with these CLAUSES if:

a. the processing of personal data by TECHWAVE has been suspended by the CUSTOMER pursuant to point 1.10.1 and if compliance with these CLAUSES is not restored within a reasonable time and in any event within one month following suspension;

b. TECHWAVE is in substantial or persistent breach of these CLAUSES or its obligations under the GDPR or any other privacy laws;

c. TECHWAVE fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these CLAUSES or the GDPR or any other privacy laws.

(3) TECHWAVE shall be entitled to terminate the SERVICE AGREEMENT insofar as it concerns processing of personal data under these CLAUSES where, after having informed the CUSTOMER that its instructions infringe applicable legal requirements in accordance with section 1.7.1.2, the CUSTOMER insists on compliance with the instructions.

(4) Following termination of the SERVICE AGREEMENT, TECHWAVE shall, at the choice of the CUSTOMER, delete all personal data processed on behalf of the CUSTOMER and certify to the CUSTOMER that it has done so, or, return all the personal data to the CUSTOMER and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, TECHWAVE shall continue to ensure compliance with these CLAUSES.

Vienna, 15.06.2026

.....	.....
Place, Date	TECHWAVE GmbH
.....	.....
Place, Date	Customer

A.1 Annex I – List of Parties

(1) Details of the CUSTOMER acting as controller (or (sub-)processor), who instructs TECHWAVE with the processing of personal identifiable information:

Name:	See SERVICE AGREEMENT
Addresse	See SERVICE AGREEMENT
Contact Person:	See SERVICE AGREEMENT
Signature:	

(2) Details of TECHWAVE, who acts as (sub-)processor and processes personal identifiable information on behalf of the CUSTOMER:

Name:	TECHWAVE GmbH
Addresse	Linke Wienzeile 4/2/DG2, AT-1060 Vienna, Austria
Contact Person:	See SERVICE AGREEMENT For inquries related to privacy topics: datenschutz@techwave.at
Signature:	

A.2 Annex II – Description of the Processing

Categories of data subjects whose personal data is processed	• Customers / Contact persons of customers • Employees of business customers • Users of IT systems of business customers
Categories of personal data processed	• Log Data: Log data from IT systems managed as part of service delivery. • Customer System Data: Selected content data stored on managed IT systems is processed as required for service delivery (e.g., for troubleshooting, data recovery, or handling IT incidents). *Note: Processing is limited to mere access - actual use and further detailed processing of such customer system data is not carried out.* • Communication Data: Meta and content data of communication between TECHWAVE and CUSTOMERS. • Company and Job Titles: Company affiliation and job titles of contact persons who are entrusted with handling IT orders on the customer's side and/or third parties attributable to the customer's sphere. • Personal Master Data: Contact and master data (name, address, email, phone) of contact persons who are entrusted with the commissioning or execution of customer orders and contracts on the customer's side and/or third parties covered by the service order. *Note: In accordance with the principle of data minimization, only data that is strictly necessary for service processing or the initiation/management of the business relationship is processed.*
Nature of the processing	Inspection, storage, processing, evaluation, and deletion of data necessary for the proper provision of services in accordance with the SERVICE AGREEMENT and the resulting individual orders of the CUSTOMER.
Purpose(s) for which the personal data is processed on behalf of the CUSTOMER	Provision of services, sales activities, and IT product/service deliveries within the framework of the SERVICE AGREEMENT and the resulting individual orders of the CUSTOMER.
Duration of the processing	The processing takes place for the duration of the SERVICE AGREEMENT. After the termination of the SERVICE AGREEMENT, performance and billing-relevant data will be retained for a minimum period of 7 years. Furthermore, existing data stocks will be deleted immediately after the termination of the SERVICE AGREEMENT, as long as there is no legal interest in continued retention.

A.3 Annex III – Technical and organisational measures including technical and organisational measures to ensure the security of the data

TECHWAVE operates a certified information security management system (ISMS) according to ISO/IEC 27001:2022.
(Certificate will be provided upon request)

Measures of pseudonymisation and encryption of personal data	**ISO/IEC 27001:2022 Reference**
• Storage and transfer encryption of data • Secure encryption standards and procedures	A.5.10 A.8.24 – A.8.27
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	**ISO/IEC 27001:2022 Reference**
• Operation of a certified information security management system according to ISO/IEC 27001:2022, including comprehensive application of reference controls according to ISO/IEC 27001:2022 Annex A.	Kapitel 4 bis 10
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	**ISO/IEC 27001:2022 Reference**
• Processes and emergency plans for handling information security incidents and emergency scenarios.	A.5.24 – A.5.30, A.5.34 A.8.14
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	**ISO/IEC 27001:2022 Reference**
• Operation of a certified information security management system according to ISO/IEC 27001:2022, including comprehensive application of reference controls according to ISO/IEC 27001:2022 Annex A.	Kapitel 4 bis 10
Measures for user identification and authorisation	**ISO/IEC 27001:2022 Reference**
• Policies and processes for the systematic and controlled management of access rights as well as secure identification and authentication	A.5.15 – A.5.18 A.8.3
Measures for the protection of data during transmission	**ISO/IEC 27001:2022 Reference**
• Storage and transfer encryption of data • Secure encryption standards and procedures • Guidelines and procedures for secure information transfer	A.5.10, A.5.14, A.5.19 – A5.23 A.8.24 – A.8.27
Measures for the protection of data during storage	**ISO/IEC 27001:2022 Reference**
• Storage and transfer encryption of data • Secure encryption standards and procedures	A.5.10 A.8.24 – A.8.27
Measures for ensuring physical security of locations at which personal data are processed	**ISO/IEC 27001:2022 Reference**
• Physical security concept and security perimeter • Policies and procedures for access control • Regulations for working in security areas • Regulations and procedures for handling data carriers and documents	A.7.1 – A.7.14
Measures for ensuring events logging	**ISO/IEC 27001:2022 Reference**

• Policies and procedures for the collection and evaluation of log data • Technical logging/monitoring of systems	A.6.8 A.8.15 – A.8.16
Measures for ensuring system configuration, including default configuration	**ISO/IEC 27001:2022 Reference**
• Policies and procedures for secure IT operations • Policies and processes for configuration management • Processes for IT change management	A.5.35 – A.5.37 A.7.13 A.8.9, A.8.26, A.8.29 und A.8.34
Measures for internal IT and IT security governance and management	**ISO/IEC 27001:2022 Reference**
• Operation of a certified information security management system according to ISO/IEC 27001:2022, including comprehensive application of reference controls according to ISO/IEC 27001:2022 Annex A.	Kapitel 4 bis 10
Measures for certification/assurance of processes and products	**ISO/IEC 27001:2022 Reference**
• Operation of a certified information security management system according to ISO/IEC 27001:2022, including comprehensive application of reference controls according to ISO/IEC 27001:2022 Annex A.	Kapitel 4 bis 10
Measures for ensuring data minimisation	**ISO/IEC 27001:2022 Reference**
• Limitation of data collection to the minimum necessary • Procedures for data masking and anonymization • Procedures for the collection, evaluation, and monitoring of personal data processing	A.5.31 und A.5.34 A.8.10 und A.8.11
Measures for ensuring data quality	**ISO/IEC 27001:2022 Reference**
• Structured and documented operational procedures • Regular review and auditing of systems and processes	8.1, 9.1 und 9.2 A.5.37 A.8.34
Measures for ensuring limited data retention	**ISO/IEC 27001:2022 Reference**
• Determination and monitoring of retention periods • Procedures for secure data deletion • Processes for compliance with data subject rights	A.5.31, A.5.34 und A.5.36 A.8.10
Measures for ensuring accountability	**ISO/IEC 27001:2022 Reference**
• Operation of a certified information security management system according to ISO/IEC 27001:2022, including comprehensive application of reference controls according to ISO/IEC 27001:2022 Annex A.	Kapitel 4 bis 10
Measures for allowing data portability and ensuring erasure]	**ISO/IEC 27001:2022 Reference**
• Procedures for secure data deletion • Processes for compliance with data subject rights	A.5.31, A.5.34 und A.5.36

A.4 Annex IV – List of Sub-Processors

(1) The list of sub-processors utilized by TECHWAVE under this DPA can be found under https://www.techwave.at/avv