DATA PROCESSING AGREEMENT (DPA)

-

PURSUANT TO ART. 28 OF EU REGULATION 2016/679

BETWEEN

Customer (also “DATA CONTROLLER”)

And

TecAlliance (also “DATA PROCESSOR”),

hereinafter, jointly, the "Parties" and severally a "Party".

This Data Processing Agreement ("**DPA**") forms part of TecAlliance's General Terms & Conditions of Business (the "**Agreement**" or **"GTCs**). This DPA will become effective on the Effective Date and remain in force for the term of the Agreement. Unless otherwise specified in this DPA, the terms of the Agreement will continue in full force and effect. Any privacy or data protection related clauses or agreement previously entered into by TecAlliance and the Customer, with regards to the subject matter of this DPA, will be superseded by and replaced with this DPA.

WHEREAS,

a. The Customer, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons regarding the processing of Personal Data (hereinafter "GDPR"), is qualified as a "Data Controller" of Personal Data; and

b. TecAlliance shall provide the services set forth in the Agreement (collectively, the "Services") for the Customer, as described in the Agreement; and

c. While providing the Services pursuant to the Agreement, TecAlliance will process Personal Data on behalf of the Customer, in the capacity of a "Data Processor", pursuant to the GDPR; and

d. The Parties, pursuant to art. 28 GDPR, wish to set forth the arrangements concerning the Processing of Personal Data (defined below) in this DPA within the context of the Services and agree to comply with the related provisions, with respect to any Personal Data, each acting reasonably and in good faith.

NOW THEREFORE, in consideration of the mutual promises set forth herein and other good and valuable considerations, the receipt and sufficiency of which are hereby acknowledged, the Parties, intending to be legally bound, agree as follows:

1. Definitions and Interpretation

1. The recitals are an integral part of this DPA;

2. References to sections, clauses or paragraphs are references to the sections, clauses or paragraph of this DPA, unless otherwise stated;

3. Words used in the singular include the plural and vice versa, as the context may require;

4. The term "including" shall be construed as if it was followed by the words "by way of example only" to provide a non-exhaustive list of examples;

5. All capitalized terms not defined in Section 1 or otherwise in this DPA will have the meanings set forth in the Agreement;

6. In this DPA, the following terms and expressions shall have the meanings associated with them as set forth below:

   "Affiliate" means affiliated companies as defined in §§ 15 et seq. German Stock Corporation Act.

   "Controller" or **"Data Controller"** means the entity which determines the purposes and means of the Processing of Personal Data, as specified under the Data Protection Laws and Regulations, pursuant to art. 4, paragraph 1, no. 7) of the GDPR. For the purposes of this DPA only, and except where indicated otherwise, the term "Data Controller" shall include the Customer, the Organization and/or the organization's authorized Affiliates.

   "**Adequacy Decision**" means a decision of the European Commission based on art. 45(3) of the European Regulation through which the laws of a certain country are considered capable of guaranteeing an adequate level of protection regarding the Processing of Personal Data, as provided for by the legislation in force;

   "Agreement" means the order or contract mutually entered into between TecAlliance and the Customer, in addition to TecAlliance' General Terms & Conditions of Business (also "GTCs);

"**Applicable Law**" means the European Regulation and any laws and/or regulations implementing or issued pursuant to it or in force of the legislation in force prior to the European Regulation and which are still applicable by virtue of the principle of consistency, as well as any binding provision issued by the competent Supervisory Authorities in the matter;

"Customer" or **"You"** means a natural person, legal entity or legally responsible partnership acting within the framework of its commercial or independent professional work when carrying out a legal transaction.;

"Data Protection Laws and Regulations" means (a) European Union or Member State laws, including GDPR, with respect to Organization's Personal Data which is subjected to EU Data Protection Laws; (b) the California Consumer Privacy Act of 2018 ("CCPA") with respect to any of Organization's Personal Data in respect of which Organization's is subject to the CCPA, and (c) any other applicable law with respect to any of Organization's Personal Data in respect of which Organization is subject to any other Data Protection Laws.

"Data Subject" means the identified or identifiable person to whom the Personal Data relates, pursuant to art. 4, paragraph 1, no. 1) of the GDPR;.

"**Effective Date**" means the date on which this DPA is signed and becomes legally binding and enforceable between the Parties. Unless otherwise specified, the Effective Date shall be the date on which the last Party signs the Agreement. From this date onward, all rights, obligations, and responsibilities outlined herein shall commence;

"Information Security and Privacy document" means the document describing the measures that TecAlliance implements to secure Personal Data, which can be found here.

"Member State" means a country that belongs to the European Union and/or the European Economic Area.

"GDPR" means the 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 Dataand on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Personal Data" means any information relating to an identified or identifiable natural person, pursuant to art. 4, paragraph 1, no. 1) of the GDPR; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Personal Data Breach**" or "**Data Breach**" means a breach of security resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data processed on behalf of the Data Controller, pursuant to art. 4, paragraph 1, no. 12) of the GDPR.

"Processing" or **"Processing Activity"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, pursuant to art. 4, paragraph 1, no. 2) of the GDPR.

"Processor" or **"Data Processor"** means the natural or legal person, public authority, agency or other body that processes Personal Data on behalf of the Controller, pursuant to art. 4, paragraph 1, no. 8) of the GDPR;

"**Services**" means the services provided by TecAlliance to the Customer, as described in the Agreement entered into between the Parties;

"Standard Contractual Clauses" or **"SCCs"** means (i) the standard contractual clauses for the transfer of Personal Data to Data Processors established in third countries which do not ensure an adequate level of protection as set out in Regulation (EU) 2016/679 of the European Parliament and of the Council from June 4, 2021, as available here, as updated, amended, replaced or superseded from time to time by the European Commission; or (ii) where required from time to time by a Supervisory Authority for use with respect to any specific restricted transfer, any other set of contractual clauses or other similar mechanism approved by such Supervisory Authority or by Applicable Laws for use in respect of such Restricted Transfer, as updated, amended, replaced or superseded from time to time by such Supervisory Authority or Data Protection Laws and Regulations;

"**Sub-Processor**" means a third party acting under the instructions of the Data Processor, meaning that they may process individuals' personal data on behalf of the Data Processor. A Sub-Processor can be a legal person, a public authority, an agency or other body.**"Supervisory Authority"** means an independent public authority which is established by an EU Member State pursuant to the GDPR;

"Technical and Organizational Measures" or **"TOMs"** means the safeguards and controls implemented by an organization to ensure the security, confidentiality, integrity, and availability of Personal Data, in compliance with Data Protection Laws and Regulations.

"Union" means the European Union.

2. Obligations of the Data Controller

The Data Controller shall provide the Data Processor with clear, complete, and timely instructions for the Processing of Personal Data, in accordance with applicable Data Protection Laws and Regulations, including but not limited to the GDPR and any other relevant national or international laws. All instructions must be lawful, documented, and consistent with the scope and purposes of the Processing Activities agreed under this DPA.

The Data Controller is solely responsible for:
a) Ensuring compliance with all obligations under applicable Data Protection Laws and Regulations, including transparency to Data Subjects, establishing valid legal bases for Processing, and ensuring the accuracy, relevance, and lawfulness of the Personal Data provided to the Data Processor;
b) Guaranteeing that Personal Data transferred to the Data Processor is adequate, relevant, and limited to what is necessary for the intended Processing purposes;
c) Promptly informing the Data Processor of any changes in the legal basis for Processing or other circumstances that may affect the lawfulness of the Processing Activities.

Where additional measures or changes to Processing are required to maintain compliance, the Data Controller shall, without undue delay:
a) Provide updated and detailed instructions regarding the purposes, methods, and procedures for Processing;
b) Cooperate with the Data Processor to identify and implement appropriate Technical and Organizational Measures;
c) Bear full responsibility for any failure to provide timely, lawful, or adequate instructions, and for any resulting non-compliance, delays, or liabilities incurred by the Data Processor.

The Data Processor shall not be liable for any consequences arising from inaccurate, incomplete, or unlawful instructions or data provided by the Data Controller.

3. Obligations of the Data Processor

In carrying out the Processing on behalf of the Data Controller, the Data Processor shall:

1. Process Personal Data in accordance with applicable Data Protection Laws and Regulations, respecting the rights and freedoms of data subjects, and applying reasonable measures to ensure confidentiality and integrity.
2. Perform only the Processing activities necessary to fulfill the purposes outlined in the Agreement, and only within the scope of documented and lawful instructions provided by the Data Controller.
3. Ensure that Processing is conducted in line with the principles of lawfulness, fairness, transparency, data minimization, and accuracy, to the extent applicable to the Data Processor's role.
4. Not be held liable for any Processing carried out in accordance with the Data Controller's instructions unless such instructions are manifestly unlawful and the Data Processor has failed to notify the Data Controller.

5. Ensure that personnel authorized to process Personal Data are subject to appropriate confidentiality obligations, either contractually or by law.
6. Inform the Data Controller of any intended changes to Sub-Processors, allowing reasonable time for objection on substantiated legal grounds.
7. Ensure that any appointed Sub-Processor is contractually bound to materially equivalent data protection obligations and provide sufficient guarantees of compliance. The Data Processor remains responsible for the performance of Sub-Processors, except where breaches arise from circumstances beyond its reasonable control and due diligence has been exercised.
8. Provide reasonable assistance, where technically feasible and proportionate, to support the Data Controller in responding to Data Subject requests under Articles 15–22 of the GDPR. The Data Processor shall not respond directly unless explicitly authorized in writing and only where necessary.
9. Maintain a record of Processing Activities where required under Article 30(2) of the GDPR.
10. Assist the Data Controller, upon request and at the Controller's expense, in meeting obligations under Articles 32–36 of the GDPR, to the extent such obligations relate directly to the Data Processor's activities and available information.
11. Inform the Data Controller of any material issues arising under applicable Privacy Legislation, including regulatory inquiries or confirmed Data Subject complaints, where such issues directly relate to the Processing Activities performed under this DPA.
12. Upon written request and subject to applicable law, delete or return Personal Data after completion of the Processing Activities. The Data Processor may retain data, as set out under Section 12 of this DPA.
13. Cooperate with audits initiated by the Data Controller, as set out under Section 13 of this DPA.
14. Notify the Data Controller if, in its reasonable opinion, an instruction violates this DPA or applicable Data Protection Laws and Regulations. In such cases, the Data Controller shall provide lawful, clear, and specific instructions within seven (7) business days of receiving such notice. If the Data Controller fails to do so, the Data Processor reserves the right to suspend the relevant Processing Activities until such instructions are received, without incurring any liability for such suspension.

4. Security Obligations (Art. 32 GDPR)

The Data Processor shall implement and maintain appropriate technical and organizational measures, consistent with industry standards and considering the state of the art, nature, scope, context, and purposes of Processing, as well as the risks to the rights and freedoms of Data Subjects. These measures are intended to ensure a level of security appropriate to the risk, including protection against unauthorized or unlawful Processing, accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to Personal Data.

The Data Processor shall apply, at a minimum, the measures described in Annex II and as outlined in the Information Security and Privacy document, which is deemed accepted by the Data Controller. These measures may be updated from time to time to reflect evolving risks, technologies, and regulatory requirements.

Upon reasonable written request and at the Data Controller's expense, the Data Processor shall use commercially reasonable efforts to assist the Data Controller in meeting its obligations under Articles 32 to 36 of the GDPR, to the extent such obligations relate directly to the Processing Activities performed by the Data Processor.

The Data Processor shall identify authorized personnel with access to Personal Data and assign access rights based on the principles of least privilege and need-to-know. If access to the Data Controller's systems is required, the Data Processor shall limit such access strictly to what is necessary for the performance of the Agreement and shall comply with any applicable access protocols.

The Data Processor shall assess risks inherent in the Processing and implement appropriate safeguards, such as encryption and pseudonymization, where feasible. These measures shall be proportionate to the risk and designed to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services. The Data Processor shall not be liable for any residual risk that remains despite the implementation of reasonable and proportionate security measures, in accordance with Article 32 of the GDPR, provided such measures are reasonable, proportionate to the risk, and industry-standard.

5. System Administrators

The Data Processor shall designate system administrators only where necessary for the performance of Processing under this DPA. The designation shall be based on a reasonable assessment of the individual's experience, reliability, and competence, and shall be documented internally.

The Data Processor shall maintain an internal list of designated system administrators and review it periodically. Upon reasonable written request by the Data Controller, the Data Processor may provide a summary of the current list, subject to confidentiality and security considerations.

The Data Processor shall conduct periodic internal reviews of system administrator activities to ensure compliance with applicable Data Protection Laws and Regulations and security requirements. The results of such reviews may be shared with the Data Controller upon reasonable written request, provided that doing so does not compromise the Data Processor's internal security protocols or proprietary information.

6. Data Breach

The Data Processor shall use reasonable efforts to notify the Data Controller without undue delay upon becoming aware of a confirmed Personal Data Breach that is likely to result in a risk to the rights and freedoms of Data Subjects. The notification shall include, to the extent reasonably available, relevant information to assist the Data Controller in meeting its obligations under Data Protection Laws and Regulations applicable, including the obligation to notify the Supervisory Authority within 72 hours.

The Data Processor shall not be responsible for assessing the severity or reportability of the breach under the GDPR, which remains the sole responsibility of the Data Controller. The Data Processor's obligation to provide information is limited to what is reasonably available.

Upon request by a competent Supervisory Authority and where required by law, the Data Processor shall make available the register of Processing Activities carried out on behalf of the Data Controller, provided that such disclosure does not compromise the Data Processor's confidentiality obligations or internal security measures.

7. Communications

Unless otherwise agreed, any formal communication from the Data Processor to the Data Controller under this DPA shall be made via email to the address designated by the Data Controller for privacy-related matters: CorporatePrivacy@tecalliance.net. The Data Processor may rely on the latest contact information provided by the Data Controller and shall not be responsible for delays or failures in communication resulting from outdated or incorrect contact details.

The Data Processor reserves the right to use alternative secure communication channels where appropriate, including secure portals or encrypted messaging, provided such channels ensure confidentiality and integrity of the information transmitted.

8. Requests from Data Subjects

The Data Processor shall implement reasonable procedures and adopt appropriate technical and organizational measures to assist the Data Controller, upon request, in responding to Data Subjectrequests under Articles 15–22 of the GDPR. Such assistance shall be provided only to the extent that the Data Processor is technically capable, and the request relates directly to Processing Activities performed under this DPA.

If the Data Processor receives a Data Subjectrequest directly, it shall, where feasible, forward the request to the Data Controller within two (7) working days, without being obligated to assess its validity or respond to the Data Subject.

The Data Processor shall not respond to any Data Subjectrequest unless explicitly authorized in writing by the Data Controller and only where necessary. In such cases, the Data Processor shall act strictly within the scope of the authorization and shall not assume any responsibility for the Data Controller's obligations under applicable Data Protection Laws and Regulations.

The Data Controller shall remain solely responsible for fulfilling Data Subjectrights and for any consequences arising from failure to do so.

9. Sub-Processor

The Data Processor may engage Sub-Processors for the performance of specific Processing Activities under this DPA, subject to prior general written authorization from the Data Controller. The Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of Sub-Processors, allowing the Data Controller a reasonable period to object on substantiated and documented legal grounds. Objections must be raised in writing and must not unreasonably delay or hinder the provision of Processing.

The list of authorized Sub-Processors is provided in Annex I and may be updated from time to time. The Data Processor shall ensure that each Sub-Processor is contractually bound to data protection obligations that are materially equivalent to those set forth in this DPA, including appropriate technical and organizational measures in accordance with the GDPR.

The Data Processor shall remain responsible for the performance of its Sub-Processors under this DPA. However, the Data Processor shall not be held liable for any breach by a Sub-Processor where such breach arises from circumstances beyond the Data Processor's reasonable control, provided that the Data Processor has exercised commercially reasonable due diligence in the selection, onboarding, and oversight of the Sub-Processor.

10. Transfer of Personal Data Abroad

If Personal Data is processed, even partially, in countries outside the European Union or the European Economic Area that are not subject to an Adequacy Decision by the European Commission, the Parties agree that such transfers shall be governed by the applicable SCCs adopted by the European Commission for the transfer of Personal Data to third countries.

Where the Data Processor engages a Sub-Processor located in such a third country, the Data Processor shall ensure that the SCCs are executed between the Data Processor and the Sub-Processor, and that the Sub-Processor provides sufficient guarantees to implement appropriate technical and organizational measures in accordance with the GDPR.

The Data Processor shall not be held liable for any failure of the Sub-Processor to comply with the SCCs, unless the Data Processor has failed to exercise due diligence in the selection and onboarding of the Sub-Processor.

11. Duration

This DPA is conditional upon and coextensive with the underlying Agreement between the Parties. It shall automatically terminate upon expiration or termination of the Agreement, regardless of the reason, without requiring separate notice or action.

The Data Processor shall not be obligated to continue any Processing Activities following termination of the Agreement, except where explicitly required by Applicable Law or expressly agreed in writing by both Parties. In such cases, the Data Processor shall be entitled to charge reasonable fees for any post-termination Processing or data handling obligations. Any additional Processing, support, or compliance efforts beyond the scope of the Agreement or this DPA shall require a separate written agreement and may be subject to additional fees.

The Data Processor shall not be liable for any delays or consequences resulting from the termination of Processing Activities, provided such termination is in accordance with this DPA and the underlying Agreement.

12. Termination

Upon termination, for any reason, of the Processing Activities by the Data Processor, the Data Processor shall:

1. return to the Data Controller the Personal Data subject to the Processing operations, or, upon written request, arrange for its deletion;
2. in either case, provide written confirmation of the action taken, only if requested by the Data Controller within a reasonable time.

The Data Processor shall not be required to delete or return Personal Data to the extent that retention is:

a) required by Applicable Law,
b) necessary for the establishment, exercise, or defense of legal claims, or
c) justified by legitimate interests, provided that such data remains subject to appropriate safeguards and is not processed for any other purpose.

The Data Processor shall ensure that any retained data continues to be protected in accordance with the Technical and Organizational Measures, outlined in this DPA.

13. Monitoring

The Data Controller may conduct audits of the Data Processor solely for the purpose of verifying compliance with this DPA and applicable Data Protection Laws and Regulations. Any such audit shall be subject to the following conditions:

1. The Data Controller must provide written notice at least thirty (30) working days in advance, specifying the scope and purpose of the audit.
2. Audits shall be conducted no more than once per calendar year.
3. Audits shall be conducted during regular business hours and in a manner that does not disrupt the Data Processor's normal operations or compromise the confidentiality of other clients or proprietary information.
4. The Data Controller shall bear all costs and expenses associated with the audit, including any internal resources required by the Data Processor to support the audit, unless material non-compliance is identified.
5. The Data Processor reserves the right to limit access to sensitive or confidential information not directly related to the Processing Activities covered by this DPA.

14. Indemnity and Liability

Each Party shall comply with its respective obligations under applicable Data Protection Laws and Regulations and this DPA.

Each Party agrees to indemnify and hold harmless the other Party from any direct damages, losses, or liabilities (including third-party claims) arising from its own breach of applicable Data Protection Laws and Regulations or this DPA. Indemnification shall not extend to indirect, incidental, consequential, or punitive damages unless caused by gross negligence or willful misconduct.

The Data Controller acknowledges and agrees that the Data Processor shall not be held liable for any Processing Activities carried out in accordance with the documented instructions of the Data Controller, unless such instructions are manifestly unlawful and the Data Processor has failed to notify the Data Controller of such unlawfulness in writing.

The Data Processor shall not be responsible for:

1. verifying the legality, accuracy, or adequacy of the Personal Data provided by the Data Controller;
2. assessing the validity of the legal basis for Processing;
3. ensuring compliance with the Data Controller's obligations under applicable Data Protection Laws and Regulations.

These responsibilities remain solely with the Data Controller.

The Data Controller further acknowledges that the Data Processor shall not be liable for any damages arising from the Data Controller's failure to fulfill its obligations under applicable Data Protection Laws and Regulations, including but not limited to providing accurate, lawful, and complete instructions or data.

The Parties acknowledge that liability shall be interpreted in accordance with Article 82 of the GDPR and the Applicable Law. The Data Processor's total aggregate liability under this DPA shall be limited to the total fees paid under the Agreement in the twelve (12) months preceding the event giving rise to the claim, unless proven gross negligence or willful misconduct by the Data Processor or otherwise required by law.

1. Applicable Law – Jurisdiction

In the event of a dispute arising out of or in connection with this DPA, the Parties shall first seek to resolve the matter amicably within sixty (60) business days from the date one Party notifies the other of the dispute.

If no resolution is reached within this period, and unless otherwise agreed in writing, any dispute shall be governed as stipulated in the Agreement mutually entered into and subject to the exclusive jurisdiction of the competent courts.

Annex I: List of Sub-Processors

Subcontracting relationships

The contractually agreed Processing or the service components described below shall be carried out by a Sub-Processor, specifically:

Name and address of the subcontractor	Description of the service component(s)
Amazon AWS, 410 Terry Avenue North, Seattle, Washington 98109-5210 U.S.A	Cloud-Hosting (DPA and SCCs)
Zendesk, 1019 Market Street, San Francisco, California 94103, U.S.A	Ticket-System (DPA and SCCs)
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, U.S.A	Cloud-Hosting (DPA und SCCs)

Annex II: TOM

Technical and Organizational Measures (in accordance with Art. 32 General Data Protection Regulation)

1 Confidentiality

In accordance with Art. 32 (1) b) GDPR.

Access control

No unauthorised access to data processing systems.

- For example using: magnetic or chip cards, keys, electric door openers, factory security or a doorman, alarm systems, video systems.
- Realised measures:
  Access control management, magnetic token, chip card, doorman, video system, alarm system

Access control

No unauthorised use of the system.

- For example using: (secure) passwords, automatic blocking mechanisms, two-factor authentication, encryption of data media.
- Realised measures:
  Secure passwords, automatic blocking mechanism

Access control

No unauthorised reading, copying, altering or deleting within the system.

- For example using: authorisation concepts and needs-oriented access rights, access logs.
- Realised measures:
  Authentication and authorization concept, “need-to-know”-principle, functional separation between permission and assigning of authorisation

Separation control

Separate Processing of data which was collected for different purposes.

- For example using: multi-client capability, sandboxing.
- Realised measure:
  Multitenancy, separation between testing and productive system

Pseudonymisation

The Processing of Personal Datain such a way that the data can no longer be assigned to a specific person

without consulting additional information, provided that this additional information is stored separately and is subject to appropriate technical and organisational measures (in accordance with Art. 32 (1) a) GDPR; Art. 25 (1) GDPR).

- Realised measures:
  Pseudonymisation

2 Integrity

In accordance with Art. 32 (1) b) GDPR.

Transmission control

No unauthorised reading, copying, altering or deleting during electronic transmission or transport.

- For example using: encryption, virtual private networks (VPN), electronic signature.
- Realised measures:
  Encryption/VPN, TLS

Input control

Determination of whether and by whom Personal Data in data processing systems has been entered, altered or deleted.

- For example using: logging, document management.
- Realised measures:
  Logging

3 Availability and capacity

In accordance with Art. 32 (1) b) and c) GDPR.

Availability control

Protection from accidental or willful destruction or loss.

- For example using: backup strategy (online/offline; on-site/off-site), uninterrupted power supply (UPS), anti-virus protection, firewall, reporting channels and emergency plans; fast recoverability).
- Realised measures:
  Backup concept, uninterruptable power supply, disaster recovery plan, malware protection, firewall

4 Procedures for regular checking, assessment and evaluation

In accordance with Art. 32 (1) d); Art. 25 (1) GDPR.

Data protection management

- Realised measures:
  Regular auditing

Incident response management

- Realised measures:
  Incident management process

Privacy by default settings

In accordance with Art. 25 (2) GDPR

- Realised measures:
  Process to ensure privacy-by-design/privacy-by-default

Job control

No contract processing in terms of Art. 28 GDPR without a corresponding instruction from the customer.

- For example using: clear contract design, formalised order management, strict selection of the service provider, sufficient guarantees in advance, follow-up checks.
- Realised measures:
  Unambiguous contracting, formalized order management