Data Processing Agreement

Conbool

Version 1.0 – As of March 2025

Conbool GmbH
Berlepschweg 11
21079 Hamburg
Deutschland

info@conbool.com
https://conbool.com

Inhalt

Data Processing Agreement

In accordance with Article 28(3) GDPR, the contracting parties are required to regulate their data protection obligations through a Data Processing Agreement to ensure the lawful processing of personal data (hereinafter referred to as "Data") within the framework of the General Terms and Conditions (hereinafter referred to as "Main Contract").
The following Data Processing Agreement applies to activities related to the contract where employees of Conbool GmbH (hereinafter referred to as "Processor") or persons commissioned by the Processor process Data on behalf of the Controller. The Controller (hereinafter referred to as "Controller") is the party responsible for determining the purposes and means of processing personal Data in accordance with Article 4(7) GDPR. This agreement is based on the template provided by the Bavarian State Office for Data Protection Supervision.

Note: This English translation is provided for convenience only. In case of discrepancies or disputes, **the German version shall prevail** as the legally binding version.

§ 1 Subject and Duration of Data Processing

1. The subject of this agreement is the rights and obligations of the parties concerning data processing by the Processor on behalf of the Controller in accordance with Article 28 GDPR. This includes all activities necessary for fulfilling the contract that constitute data processing by the Processor.

2. The contractual services will be provided exclusively within a member state of the European Union or a contracting state of the European Economic Area (EEA), unless a transfer of Data to third countries is necessary for service provision. In such cases, the Processor ensures compliance with Articles 44 et seq. GDPR.

3. For specific services, personal Data may be transferred to subcontractors outside the EEA. Processing by subcontractors, such as Supabase, primarily occurs within the EEA. If a transfer to third countries is necessary, it will be safeguarded through Standard Contractual Clauses (SCCs) in accordance with Article 46 GDPR.

4. For Data transfers to third countries, the Processor ensures appropriate safeguards under Article 46 GDPR, particularly through SCCs and additional technical measures such as end-to-end encryption.

5. Data processing begins with the conclusion of the Main Contract and continues indefinitely until either this Data Processing Agreement or the Main Contract is terminated.

6. The Controller has the right to terminate both this agreement and the Main Contract without notice if there is a serious breach of data protection regulations or provisions of this agreement by the Processor.

§ 2 Nature and Purpose of Processing, Types of Personal Data, and Categories of Data Subjects

Nature and Purpose of Processing (as defined in Article 4(2) GDPR):

1. The data processing includes all types of processing under the GDPR necessary for fulfilling the contract.
2. The purpose of processing is to provide the agreed-upon services outlined in the Main Contract, particularly the provision of a SaaS-based email security gateway. This includes: Filtering and analyzing emails, encrypting and decrypting emails, signing and validating emails, and applying security policies to ensure the integrity and confidentiality of email communication.

Types of Personal Data:

- Personal master data (e.g., title, first name, last name, address)
- Contract-related data (e.g., contractual relationships, products/services)
- Communication data (e.g., phone numbers, email addresses, domains)
- Billing and payment data
- Email metadata (e.g., sender, recipient, subject lines)
- Email content data (e.g., text content, attachments)

Categories of Data Subjects (as defined in Article 4(1) GDPR):

- All individuals using services under the Main Contract
- All individuals communicated about via email
- Email senders and recipients
- Employees
- Customers
- Prospective clients
- Business partners and suppliers
- Sales representatives
- Contact persons

§ 3 Responsibility and Processing of Documented Instructions

1. The Controller is solely responsible under this agreement for compliance with the legal provisions of data protection laws, particularly for the lawfulness of the transfer of Data to the Processor and the lawfulness of the data processing (as the "Controller" within the meaning of Article 4(7) GDPR). This also applies to the purposes and means of processing regulated in this agreement.
2. Instructions are initially defined by the Main Contract and may subsequently be amended, supplemented, or replaced by individual instructions provided by the Controller in written or

text form (e.g., via email). Instructions not provided for in the contract will be treated as a request for a change in service and must be agreed upon jointly by the Controller and Processor. Oral instructions must be confirmed promptly in writing or text form by the Controller.

3. If implementing an instruction is unreasonable for the Processor, the Processor is entitled to terminate processing and cancel the contract extraordinarily. The Controller's obligation to pay ceases when services are discontinued by the Processor. Unreasonableness particularly exists if services are provided in an infrastructure shared by multiple Controllers/customers (shared services) and a change in processing for individual Controllers is not feasible or reasonable.
4. The Controller may terminate both the Main Contract and this agreement at any time if the Processor cannot or will not execute an instruction from the Controller or if the Processor unlawfully refuses to grant inspection rights to the Controller.

§ 4 Duties of the Processor

1. The Processor may only process Data covered by this agreement within the scope of the contract and in accordance with the Controller’s instructions, unless an exceptional case under Article 28(3)(a) GDPR applies and its requirements are met (e.g., investigations by law enforcement authorities). In such cases, the Processor shall inform the Controller of these legal requirements before processing, unless the relevant law prohibits such notification due to an overriding public interest.
2. The Processor shall immediately inform the Controller if it believes that an instruction violates applicable laws. The Processor may suspend implementation of the instruction until it is confirmed or amended by the Controller.
3. The Processor ensures that the Data provided for processing is not used for any other purpose, particularly not for its own purposes. Furthermore, the Processor ensures that all persons authorized to process personal Data are bound by confidentiality obligations, which continue even after termination of this agreement. This also applies to obligations under telecommunications secrecy (§ 3 TTDSG), social secrecy, and professional secrecy under § 203 StGB.
4. The Processor shall implement appropriate technical and organizational measures to adequately protect the Controller’s Data in compliance with Article 32 GDPR. These measures must ensure the confidentiality, integrity, availability, and resilience of systems and services related to processing on a continuous basis. The technical and organizational measures are documented by the Processor in Appendix 2 and made available to the Controller for review.
5. The Processor shall reasonably assist the Controller in fulfilling requests and claims from Data Subjects under Chapter III GDPR as well as in complying with obligations under Articles 33 to 36 GDPR. For this support, the Processor may request reasonable compensation unless the request arises from a breach of contract by the Processor.
6. The Processor shall promptly notify the Controller of any known breaches of personal Data protection involving the Controller’s Data. The Processor shall take necessary measures to secure the Data and mitigate potential adverse effects on affected individuals.
7. The Processor shall designate a contact person for data protection matters arising under this agreement.

8. The Processor shall rectify, delete, or restrict processing of personal Data from this agreement as instructed by the Controller.
9. Upon completion of processing services, the Processor shall either delete all personal Data or return it to the Controller at their discretion unless Union or Member State law requires storage of personal Data. If no choice is made by the Controller, deletion is deemed agreed upon. If data return is chosen, reasonable compensation may be requested by the Processor after providing a cost estimate to the Controller.
10. The Processor shall demonstrate compliance with its obligations under this agreement using appropriate means. Upon request, it will provide documented controls and required information to the Controller.
11. The Processor agrees that the Controller is entitled to verify compliance with data protection and security requirements as well as contractual agreements through audits or on-site inspections (Article 28(3)(h) GDPR). The Processor may require confidentiality agreements from auditors but not in a way that prevents evidence submission to supervisory authorities by the Controller. Competitors or individuals working for competitors may be rejected as auditors by the Processor.
12. The Processor assures cooperation during audits conducted by or on behalf of the Controller. For information or support activities during audits, reasonable compensation may be requested unless they arise due to legal or contractual violations by the Processor. A cost estimate will be provided beforehand.
13. The Processor will provide all necessary information to prove compliance with Article 28 GDPR upon request from either the Controller or an auditor appointed by them.
14. The Processor confirms awareness of all relevant data protection regulations under GDPR applicable to data processing activities covered by this agreement.
15. If claims for damages are made against either party under Article 82 GDPR by affected individuals, both parties agree to support each other in defending against such claims within their capabilities. Reasonable compensation may be requested unless claims arise due to breaches of law or contract by the Processor.

§ 5 Rights and Obligations of the Controller

1. The Controller is solely responsible for assessing the lawfulness of processing under Article 6(1) GDPR and for safeguarding the rights of Data Subjects in accordance with Articles 12 to 22 GDPR. Nevertheless, the Processor is obligated to promptly forward any such requests, insofar as they are clearly directed exclusively at the Controller. In fulfilling its obligations, the Processor follows the instructions of the Controller. The Processor shall not be held liable if a request from a Data Subject is not answered, answered incorrectly, or answered late by the Controller.
2. The Controller must promptly and comprehensively inform the Processor if it identifies errors or irregularities in the implementation of this agreement or in compliance with data protection regulations.
3. Upon termination of the contract, the Controller is obligated to delete any personal Data stored in the services before the end of the contract.

4. At the Processor's request, the Controller shall designate a contact person for data protection matters.
5. The Controller is obligated to treat all knowledge gained about trade secrets and data security measures of the Processor as confidential. This obligation remains in effect even after this agreement has been terminated.

§ 6 Authorized Persons of the Controller and Recipients of Instructions for the Processor

1. Authorized Persons of the Controller: The persons authorized to issue instructions on behalf of the Controller are those specified in the customer account's master data.
2. Recipients of Instructions for the Processor: All administrators of Conbool GmbH are designated as recipients of instructions.
3. Form of Instructions: Instructions from the Controller must be issued in writing or in text form via the agreed communication channels provided on the website. In urgent cases, instructions may be given by telephone but must be promptly confirmed in writing or text form.
4. Changes to Authorized Persons: In the event of a change or long-term unavailability of authorized persons, the contracting party must inform the other party without delay and, as a rule, in written or electronic form about successors or representatives.

§ 7 Additional Processors (Subcontractors)

1. The Controller generally permits the Processor to engage additional subcontractors in accordance with Article 28 GDPR for fulfilling contractual obligations. The Processor ensures that agreements with these third parties include sufficient provisions to guarantee appropriate data protection and information security measures.
2. The currently engaged subcontractors are listed in Appendix 1. The Controller agrees to their use.
3. The Controller has the right to object to the engagement of a new subcontractor within 14 days after being notified, provided there is a valid reason for doing so.
4. In the event of an objection, the Processor may either provide the service without involving the proposed subcontractor or, if this is not feasible, terminate the affected service within a reasonable period (at least 14 days) after receiving the objection. In such cases, the Controller is no longer obligated to pay for services that have been discontinued.
5. The Processor commits to regularly reviewing subcontractors' compliance with data protection requirements and providing evidence to the Controller upon request.
6. When engaging additional processors, it is the Processor's responsibility to transfer its data protection obligations under this agreement to those subcontractors. The Processor ensures compliance with technical and organizational measures through regular monitoring.
7. Contracts with subcontractors must be concluded in written form, which may also include electronic formats (in accordance with Article 28(4) and (9) GDPR).

§ 8 Technical and Organizational Measures in Accordance with Article 32 GDPR

1. Within its area of responsibility, the Processor implements appropriate technical and organizational measures to ensure that processing complies with the requirements of the GDPR and guarantees the protection of the rights and freedoms of the Data Subjects. The Controller is responsible for implementing appropriate technical and organizational measures within its own area of responsibility in accordance with Article 32 GDPR, ensuring the confidentiality, integrity, availability, and resilience of systems and services related to processing over the long term.
2. The current technical and organizational measures implemented by the Processor are described in Appendix 2. The Processor clarifies that the technical and organizational measures listed at the link are merely technical descriptions and should not be considered part of this agreement.
3. The Processor conducts regular reviews of the effectiveness of its technical and organizational measures to ensure the security of processing in accordance with Article 32(1)(d) GDPR.
4. Over time, the Processor will adapt its implemented measures to account for developments in the state of technology and changes in risk levels. The Processor may modify its technical and organizational measures as long as this does not result in a level of protection below that required by Article 32 GDPR.

§ 9 Liability

1. Liability and claims for damages are governed by Article 82 GDPR.
2. In the event that a Data Subject asserts a claim for damages under Article 82 GDPR, the parties agree to support each other in clarifying the underlying facts and circumstances.
3. In the case of a data protection breach as defined in Article 33 GDPR, the Processor commits to:
   a. Informing the Controller immediately (no later than within 24 hours).
   b. Taking all necessary measures to contain the incident and prevent further violations.
   c. Supporting the Controller in notifying the competent supervisory authority.

§ 10 Miscellaneous

1. If the property or data of the Controller being processed is endangered by measures taken by third parties (e.g., seizure or confiscation), insolvency or settlement proceedings, or other events, the Processor must inform the Controller without delay.
2. Should any individual provisions of this agreement be invalid, this shall not affect the validity of the agreement as a whole.
3. The Processor reserves the right to amend this agreement if required by legal changes or to implement new technical standards. The Controller will be informed in writing at least four weeks before such amendments take effect and has the right to object within this period. In case of an objection by the Controller, the Processor has an extraordinary termination right.
4. The Controller accepts this agreement as part of the General Terms and Conditions (GTC) for the products they have booked. In case of conflicts, the provisions of this Data Processing Agreement take precedence over those of the Main Contract.
5. If significant changes occur regarding subcontractors or their data protection measures, the Processor will promptly inform the Controller and adapt this agreement accordingly.
6. German law applies.

Appendix 1 Additional Processors

1. **IONOS SE**

   - **Address:** Elgendorfer Straße 7, 56410 Montabaur, Germany
   - **Description of Partial Service:**
     Provision, operation, and maintenance of products, specifically:
     a. Operation, maintenance, and servicing of the products.
     b. Provision of the physical environment for operating the Conbool GmbH website and application.
     c. Operation of the platform and provision of dedicated and virtual servers as well as cloud solutions.

2. **Supabase Inc.**

   - **Address:** 970 Toa Payoh North #07-04, Singapore
   - **Description of Partial Service:**
     Backend database used for storing and processing service-relevant data as well as for user management and authentication.
   - Data processing primarily takes place on servers within the European Union (e.g., Frankfurt am Main).
   - Supabase ensures, through appropriate technical and organizational measures, that the confidentiality, integrity, and availability of processed personal data are maintained. These measures include, among other things the encryption of data during transmission and storage and access controls in accordance with GDPR requirements
   - If a transfer to third countries is required, Supabase ensures that all data protection requirements under Articles 44 et seq. GDPR are met, particularly through the conclusion of Standard Contractual Clauses (SCCs).
   - A corresponding Data Processing Agreement has been concluded with Supabase Inc.
   - The Processor regularly reviews compliance with the contractually agreed data protection measures by Supabase, particularly regarding data transfers to third countries.

Appendix 2 Technical and Organizational Measures (TOMs)

1. **Confidentiality**
   Measures to ensure that only authorized persons have access to personal data:

Physical Access Control at IONOS:

- Security gates and video surveillance in IONOS data centers (certified according to ISO 27001).
- Access only for authorized persons via electronic access controls (e.g., transponders, biometric scanners).
- Visitor registration and accompaniment by authorized personnel.
- Regular review and logging of access rights.

Digital Access Control

- Multi-factor authentication (MFA) for all administrative accesses.
- Strict password policies (regular changes, minimum complexity).
- VPN connections for remote access to internal systems.
- Encryption of mobile storage devices and endpoints.

Data Access Control

- Role-based permission concept based on the principle of least privilege ("need-to-know principle").
- Separation of application and administrative accesses.
- Email content is processed exclusively in-stream and not stored.
- Logging and monitoring of all access attempts to personal data.
- Access to personal data or metadata is restricted to authorized employees with role-based permissions.

Pseudonymization

- Pseudonymization of personal data wherever possible.

Data Encryption

- Encryption of all stored data.

Confidentiality Agreements:

- All employees are bound by confidentiality and data protection obligations in accordance with Article 28(3) GDPR.

2. **Integrity**
   Measures to ensure the immutability and consistency of data:

Data Integrity:

- Use of checksums and hashing methods to validate data integrity.

Transfer Control:

- Encryption of all data transmissions using TLS 1.2 or higher.
- Use of secure communication protocols such as SFTP for data exchange.
- Documentation of all data transfers to subcontractors like Supabase.

Input Control:

- Protection of logs against manipulation through access restrictions and encryption.
- Individual user IDs to ensure traceability of changes.

3. **Availability and Resilience**
   Measures to ensure the availability of systems and services:

Fault Tolerance:

- Use of highly available cloud infrastructures at IONOS with redundant servers.
- Failover systems to minimize downtime.
- Emergency plans for operations during technical disruptions.

Resilience:

- Load testing to verify system stability under peak loads.
- Scalable cloud infrastructure provided by Supabase and IONOS to dynamically respond to increased demands.

Monitoring:

- Continuous monitoring of system resources and automated alerts in case of anomalies.

4. **Transparency**
   Measures to ensure traceability of processing activities:

Documentation:

- Maintenance of a record of processing activities in accordance with Article 30 GDPR.
- Regular Data Protection Impact Assessments (DPIAs) for new processing activities.

5. **Data Protection by Design ("Privacy by Design")**

Default Privacy Settings ("Privacy by Default"):

- Default settings for maximum data minimization in all services.

Data Minimization:

- Collection only of data necessary for the specific purpose.
- Automatic deletion of unnecessary data after defined retention periods.

6. **Training and Awareness**

Organizational measures to promote awareness of data protection:

- Regular training for all employees on data protection policies and IT security.
- Awareness campaigns on handling phishing attacks and social engineering.

7. **Incident Response Management**

Measures for handling security incidents:

- Documented process for detecting, reporting, and addressing data protection breaches.
- Notification to the Controller within 24 hours in the event of an incident, as required by Article 33 GDPR.
- Collaboration with external experts in cases of severe security incidents.

8. **Organizational Measures**

Measures to ensure clear responsibilities:

- Regular internal audits to verify compliance with data protection regulations.
- Continuous updates to security measures according to the state-of-the-art technology standards.
- Procedures for exercising Data Subject rights in accordance with Chapter III GDPR.