Data Processing Agreement

Version: January 2026

Agreement

between the **Controller**

_____

_____

_____

hereinafter referred to as **Client**

and

web-me.de Internet Service e.K. Rainer Thieringer Merowingerstraße 6 D-78662 Bösingen, Germany

hereinafter referred to as **Processor**,

hereinafter jointly referred to as **Party/Parties**.

A customer account exists as part of a registration at https://www.teammessage.de under customer number

_____ .

Contact person for data protection / Data Protection Officer designated by the Processor: Dipl. Ing. (FH) Rainer Thieringer (+49-7404-910386, dsb@web-me.de / dsb@teammessage.de).

_____

Preamble

1. The Processor provides gateway functionality for sending SMS and email messages. The Client and the Processor may have already concluded an individual contract as part of a registration via the website https://www.teammessage.de. Under this name, the Processor offers the forwarding of incoming messages.
2. The Parties wish to document the agreement of the Parties regarding the processing of personal data in compliance with the applicable data protection laws and regulations, in particular in compliance with Article 28 of the EU General Data Protection Regulation.
3. With regard to the processing of personal data, the provisions of this Agreement between the Client and the Processor replace all previous agreements and arrangements between the Parties. In case of conflicts between the provisions of the individual contract and this Agreement between the Controller and the Processor, the latter shall prevail.

_____

Definitions and Interpretation

Agreement means this agreement including the attached annexes.

Ancillary Services means services that are independent of the subject matter of this Agreement, such as telecommunications services, postal/transport services, maintenance and support services for users, or the disposal of data carriers, as well as other measures to ensure

the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems.

Annex means any annex to this Agreement that is to be considered an integral part of the contract.

Sub-processor means a data processor engaged by the Processor in the course of providing the Services.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Protection Laws means EU data protection laws as well as the BDSG (German Federal Data Protection Act) in the version effective from May 25, 2018, and, where applicable, the data protection laws of any other country.

EEA means the European Economic Area and consists of all countries of the European Union, Liechtenstein, Norway and Iceland.

GDPR means REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of April 27, 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).

Personal Data means any information relating to an identified or identifiable natural person (data subject). 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.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated 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.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

Services means all services provided by the Processor as agreed in the Service Agreement.

Service Agreement means the contract concluded by the Parties regarding the provision of services by the Processor.

"SMSC" means a server that delivers SMS short messages to mobile network operators so that the SMS short message can be delivered to a mobile subscriber.

---

1) Subject Matter and Duration of the Agreement

(1) Subject Matter of the Agreement

The Processor provides gateway functionality for sending SMS and email messages. The service includes the immediate forwarding of incoming messages to the operators of mobile networks and mail servers.

The Processor processes the data exclusively according to the instructions of the Client. The Processor has no decision-making authority over the transmitted data and its processing.

Apart from transmission to subordinate telecommunications service providers, disclosure of data to third parties is excluded.

Persons authorized to give instructions on behalf of the Client: 1. Acting Managing Directors 2. IT Administrators 3. Data Protection Officer

Persons authorized to receive instructions on behalf of the Processor: 1. Managing Director (CEO) 2. Technical Director (CTO)

(2) Duration of the Agreement

The agreement is concluded for an indefinite period and may be terminated by either Party at the end of each monthly payment period.

---

2) Specification of the Agreement Content

(1) Type and Purpose of the Intended Data Processing

The service primarily consists of sending text messages via SMS or email to the addressees that the Client implements as a service on behalf of their customers or addresses to their own customers.

This data processing is performed exclusively in Germany or a Member State of the European Union or in another Contracting State of the Agreement on the European Economic Area. Any relocation of the service to a third country requires the prior consent of the Client and may only take place if the special requirements of Articles 44 ff. GDPR are met.

(2) Types of Data

1. Communication data (telephone number, mobile phone number, email address)
2. Subject and textual content of the message submitted by the Client for transmission

The following types of data are excluded from transmission for processing: 1. Health data 2. Data concerning sex life or sexual orientation 3. Genetic data 4. Data revealing racial or ethnic origin 5. Data revealing trade union membership 6. Data relating to criminal convictions or offenses

(3) Categories of Data Subjects

The categories of persons affected by data processing from the Client's perspective include one or more of the following groups: 1. Customers of the Client 2. Employees of affiliated companies of the Client 3. Processors 4. Prospects 5. Contact persons in companies

---

3) Technical and Organizational Measures

(1) The Processor shall document the implementation of the technical and organizational measures presented and required prior to contract award before the start of processing, particularly with regard to the specific contract execution, and submit them to the Client for review. Upon acceptance by the Client, the documented measures become the basis of the agreement. If the Client's review/audit identifies a need for adjustment, this shall be implemented by mutual agreement.

(2) The Processor shall establish security in accordance with Art. 28(3)(c), 32 GDPR, particularly in conjunction with Art. 5(1), (2) GDPR. Overall, the measures to be taken are measures for data security and for ensuring an appropriate level of protection regarding the confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the nature, scope and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32(1) GDPR, shall be taken into account. The technical and organizational measures are documented in Annex 1.

(3) The technical and organizational measures are subject to technical progress and development. In this respect, the Processor is permitted to implement alternative adequate measures. The security level of the defined measures must not be reduced. Significant changes must be documented and brought to the Client's attention.

(4) The services provided by the Processor are subject to the GDPR and BDSG (German Federal Data Protection Act) as well as the Telecommunications Act (TKG), the Digital Services Act (DDG) and the Telecommunications-Digital Services Data Protection Act (TDDDG) in their respective valid versions. The Processor is obliged to comply with these and any additional legal requirements.

---

4) Rectification, Restriction and Erasure of Data

(1) The Processor may not rectify, erase or restrict the processing of data processed under the agreement on its own authority, but only according to documented instructions from the Client. If a data subject contacts the Processor directly in this regard, the Processor shall forward this request to the Client without delay.

(2) Erasure, rectification, implementation of the right to information, the right to be forgotten and data portability according to documented instructions from the Client shall be ensured directly by the Processor. The Processor shall assist the Client, where possible, in fulfilling the Client's obligation to respond to requests for the exercise of data subject rights. These rights include the right to be forgotten as well as the rights to rectification, data portability and information.

(3) If no separate documented instruction is provided by the Client, the data submitted for processing will be successively deleted according to the Processor's standard procedure:

1. The text portion of incoming messages is reduced in length so that the text fits into one SMS message; this text portion as well as sender, recipient, time and delivery status information are stored by the Processor in a local database as proof of service.
2. Processed emails are deleted after no more than 2 weeks.
3. The text portion of processed messages is deleted from the database after 400 days.

---

5) Quality Assurance and Other Obligations of the Processor

The Processor has statutory obligations pursuant to Art. 28 to 33 GDPR in addition to compliance with the provisions of this Agreement; in this respect, the Processor ensures compliance with the following requirements in particular:

1. **Designation of a contact person or Data Protection Officer.** The Client shall be informed immediately of any changes in this regard. Note: Based on documented self-assessment regarding company size and protection requirements of the processed data, the Processor is not obliged to appoint a Data Protection Officer.

2. **Maintaining a record of processing activities.**
3. **Maintaining confidentiality** pursuant to Art. 28(3) sentence 2(b), 29, 32(4) GDPR. The Processor only uses employees who are committed to confidentiality and have been familiarized with the relevant data protection provisions prior to their work. The Processor and any person acting under the Processor's authority who has access to personal data may only process this data in accordance with the Client's instructions, including the powers granted in this Agreement, unless they are legally obligated to process.
4. **Implementation and compliance with all technical and organizational measures** required for this agreement pursuant to Art. 28(3) sentence 2(c), 32 GDPR (see Annex).
5. **The Client and the Processor shall cooperate with the supervisory authority** in the performance of its tasks upon request.
6. **Immediate notification to the Client** about control actions and measures by the supervisory authority insofar as they relate to this agreement. This also applies if a competent authority investigates the Processor in the context of administrative offense or criminal proceedings regarding the processing of personal data in the context of order processing.
7. If the Client is subject to a supervisory authority inspection, administrative offense or criminal proceedings, a liability claim by a data subject or a third party, or any other claim in connection with the order processing at the Processor, **the Processor shall support the Client to the best of its ability**.
8. **The Processor regularly monitors internal processes** as well as technical and organizational measures to ensure that processing within its area of responsibility is in accordance with the requirements of applicable data protection law and that the protection of the data subject's rights is ensured.
9. **Verifiability of the technical and organizational measures** taken vis-à-vis the Client within the scope of its control powers under Section 7 of this Agreement.

---

6) Sub-processing Relationships

(1) Sub-processing relationships within the meaning of this provision are to be understood as services that directly relate to the provision of the main service. This does not include ancillary services that the Processor uses, for example, as telecommunications services, postal/transport services, maintenance and user support, or disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Processor is obliged to take appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security of the Client's data even for outsourced ancillary services.

(2) The Processor may only engage sub-processors (further processors) with the prior express written or documented consent of the Client. **Exempted from this express consent are SMSC service providers and mobile network operators**, insofar as they ensure compliance with the legal requirements of the German Telecommunications Act (TKG), the Digital Services Act (DDG) and the Telecommunications-Digital Services Data Protection Act (TDDDG).

The Client agrees to the engagement of the following sub-processors subject to a contractual agreement in accordance with Art. 28(2-4) GDPR:

1. **Hostsharing eG**, Flughafenstraße 52a, 22335 Hamburg | Country: Germany | Service: Responsible hoster for the operation of the server infrastructure.

2. **Several unnamed SMSC service providers** | Countries: Germany, Ireland and Denmark | Service: Redundantly structured SMSC infrastructure for handing over SMS messages to mobile network operators. These service providers are subject to telecommunications and communication secrecy according to TKG. Any disclosure of personal data to third parties is also prohibited to sub-contracted service providers.

A change of existing sub-processors is permissible if: 1. The Processor notifies the Client in writing or in text form of such outsourcing to sub-processors a reasonable time in advance, and 2. The Client does not object in writing or in text form to the planned outsourcing to the Processor by the time of data transfer, and 3. A contractual agreement in accordance with Art. 28(2-4) GDPR is established.

(3) The transfer of personal data of the Client to the sub-processor and its initial activity are only permitted when all requirements for sub-contracting are met.

(4) If the sub-processor provides the agreed service outside the EU/EEA, the Processor shall ensure data protection compliance through appropriate measures. The same applies if service providers within the meaning of paragraph 1 sentence 2 are to be used.

(5) When using sub-processors, the Processor ensures data protection compliance through appropriate measures.

(6) Any further outsourcing by the sub-processor requires the express consent of the main client (at least in text form).

(7) The Processor performs all processing in data centers within the Federal Republic of Germany. This also applies to any sub-processors. The handover of processed messages to mobile network operators and SMSCs is carried out via servers in Germany.

All contractual provisions in the contractual chain shall also be imposed on further sub-processors.

---

7) Control Rights of the Client

(1) The Client has the right to carry out inspections in consultation with the Processor or to have them carried out by auditors to be designated on a case-by-case basis. The Client has the right to satisfy itself of the Processor's compliance with this Agreement in the Processor's business operations through spot checks, which are generally to be announced in advance.

(2) The Processor shall ensure that the Client can verify compliance with the Processor's obligations under Art. 28 GDPR. The Processor undertakes to provide the Client with the necessary information upon request and, in particular, to demonstrate the implementation of the technical and organizational measures.

(3) Evidence of such measures, which do not only concern the specific order, can be provided by:

1. Compliance with approved codes of conduct pursuant to Art. 40 GDPR;
2. Certification according to an approved certification procedure pursuant to Art. 42 GDPR;
3. Current attestations, reports or report excerpts from independent bodies (e.g., auditors, internal audit, data protection officer, IT security department, data protection auditors, quality auditors);
4. Appropriate certification through IT security or data protection audit (e.g., according to BSI baseline protection).

(4) The Processor may claim compensation for enabling controls by the Client.

8) Notification of Violations by the Processor

(1) The Processor supports the Client in complying with the obligations set out in Articles 32 to 36 GDPR regarding the security of personal data, notification obligations in the event of data breaches, data protection impact assessments and prior consultations. This includes, among other things:

1. Ensuring an appropriate level of protection through technical and organizational measures that take into account the circumstances and purposes of processing as well as the predicted probability and severity of a possible legal violation through security gaps and enable immediate detection of relevant violation events.
2. The obligation to report personal data breaches to the Client without delay.
3. The obligation to support the Client in the context of its duty to inform the data subject and to provide all relevant information without delay in this connection.
4. Supporting the Client with its data protection impact assessment.
5. Supporting the Client in the context of prior consultations with the supervisory authority.

(2) For support services not included in the service description or not attributable to misconduct by the Processor, the Processor may claim compensation.

---

9) Client's Right to Issue Instructions

(1) Verbal instructions shall be confirmed by the Client without delay (at least in text form).

(2) The Processor shall inform the Client immediately if it believes that an instruction violates data protection regulations. The Processor is entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the Client.

---

10) Deletion and Return of Personal Data

(1) Copies or duplicates of the data are not made without the Client's knowledge. Excluded from this are backup copies insofar as they are necessary to ensure proper data processing or for billing and proof of the service provided, as well as data required for compliance with legal retention obligations.

(2) After completion of the contractually agreed work or earlier upon request by the Client, but at the latest upon termination of the service agreement, the Processor shall hand over all documents, processing and usage results, and data files that have come into its possession and that are related to the contractual relationship to the Client, or destroy them in a data protection-compliant manner with prior consent. The same applies to test material. The deletion log shall be presented upon request.

(3) Documentation that serves as proof of proper and orderly data processing shall be retained by the Processor beyond the end of the contract in accordance with the respective retention periods. The Processor may hand them over to the Client at the end of the contract for its own discharge.

---

11) Support Obligations

(1) The Processor shall support the Client in fulfilling the obligations concerning the security of personal data, notification obligations in the event of personal data breaches, data protection impact assessments and prior consultations in accordance with Articles 33 to 36 GDPR.

This includes in particular: 1. The obligation to report a personal data breach to the Client without delay. 2. The obligation to support the Client with regard to the Client's obligation to provide information to the data subject and to provide all relevant information to the Client without delay. The minimum information to be transmitted includes the nature of the personal data breach, the categories and number of data subjects affected, the categories and number of data records, and the likely consequences of the personal data breach. 3. Supporting the Client with a data protection impact assessment. 4. Supporting the Client with regard to the record of processing activities. 5. Supporting the Client with regard to consultation with the supervisory authority.

The Processor may claim compensation for the support.

---

12) Liability and Sanctions

The statutory provisions, in particular Article 82 GDPR, apply in the case of claims for damages or liability.

---

13) Final Provisions

(1) Any amendment or supplement to this Agreement requires written form and signature by duly authorized representatives of both Parties.

(2) If the Client's data becomes subject to a search and seizure, an attachment order, confiscation in the context of bankruptcy or insolvency proceedings, or similar events or measures by third parties while in the Processor's area of responsibility, the Processor shall notify the Controller without delay. The Processor shall immediately inform all parties involved in such measures that the data concerned is exclusively owned by the Client and is within the Client's area of responsibility, that the Controller has sole authority over this data, and that the Client is responsible for the application of data protection law.

(3) Should any provision of this Agreement be found invalid, unlawful or unenforceable for any reason whatsoever, the provision in question shall be excluded and the remaining provisions of this Agreement shall remain in full force and effect as if this Agreement had been concluded without the invalid provision.

(4) This Agreement is subject to EU law.

Annexes:

1. Technical and Organizational Measures

Client / Controller: _____

Place / Date: _____

Signature: _____

Contractor / Processor: Rainer Thieringer, web-me.de Internet Service e.K.

Place / Date: _____

Signature: _____

—

TOM - Technical and Organizational Measures

Created: Sunday, May 6, 2018 Last modified: May 6, 2018

The Processor shall document the implementation of the technical and organizational measures presented and required prior to contract award before the start of processing, particularly with regard to the specific contract execution, and submit them to the Client for review. Upon acceptance by the Client, the documented measures become the basis of the agreement. If the Client's review/audit identifies a need for adjustment, this shall be implemented by mutual agreement.

The Processor shall establish security in accordance with Art. 28(3)(c), 32 GDPR, particularly in conjunction with Art. 5(1), (2) GDPR. Overall, the measures to be taken are measures for data security and for ensuring an appropriate level of protection regarding the confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the nature, scope and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32(1) GDPR, shall be taken into account (see Annex for details).

The technical and organizational measures are subject to technical progress and development. In this respect, the Processor is permitted to implement alternative adequate measures. The security level of the defined measures must not be reduced. Significant changes must be documented.

TOM001 Confidentiality

Created: May 6, 2018 Last modified: May 30, 2022

(Art. 32(1)(b) GDPR)

The operation of the server infrastructure is outsourced to a sub-processor - referred to here as hoster. The processor from the end customer's perspective is web-me.de Internet Service e.K.

Access Control (Physical)

Access control serves to protect data processing systems from unauthorized physical access. The commissioned hoster implements access control through the following multi-level security measures:

1. Access to the data centers is secured by video surveillance at entrances and exits, security locks and cages (extra-secured areas within the Berlin data center location). Access to the data center is only permitted when accompanied by authorized personnel. Access to the data centers is controlled and logged.

2. Access to the cages is secured by a locking system and monitored by camera.
3. Access to individual cages is only permitted when accompanied by authorized personnel.
4. Access to the racks (the server cabinets within the cages) is secured by an additional locking system and is only permitted when accompanied by authorized personnel.
5. Access is granted after authentication with access card and PIN. Keys are issued exclusively to authorized employees and customers. Each customer only has access to their own racks.

System Access Control

System access control serves to protect data processing systems from unauthorized logical access. The commissioned hoster implements system access control through the following multi-level security measures:

1. Access to server administration is exclusively via a protected connection.
2. Access is protected by public key procedures; access is via personal user accounts.
3. Access for administrative operations is via two-stage access security with logging.
4. The commissioned hoster is responsible for access control regarding security and updates of the operationally maintained software.
5. The Processor is responsible for access control regarding security and updates of the self-managed installed software. In particular the content management system and the programs for message distribution.

Data Access Control

Data access control serves to protect data from unauthorized reading, copying, modification or deletion of personal data within the system. The commissioned hoster implements data access control through the following multi-level security measures:

1. Support staff generally have no access to data in databases or in customer user directories.
2. A binding authorization procedure is defined for the hoster's employees.
3. In the event of security vulnerabilities becoming known, security updates should be installed immediately.
4. The hoster ensures that defective data carriers that cannot be securely erased are destroyed (shredded) directly in the data center.
5. The commissioned hoster is responsible for data access control regarding security and updates of the operationally maintained software.
6. web-me.de is responsible for data access control regarding security and updates of the self-managed installed software. In particular the content management system and the programs for message distribution.

Separation Control

Data from different clients (master data, connection data, mobile phone numbers, personal names used) are stored in a relational database for technical reasons. Accesses are secured via customer number and a unique key (UID) so that data from different customers cannot be mixed in a query result. For special protection needs and against a separate order and additional operating costs, the data can be processed completely separately.

In case of a deletion order, the data can be selectively deleted as requested by the Client.

Pseudonymization

(Art. 32(1)(a) GDPR; Art. 25(1) GDPR)

The storage of submitted data technically enables the assignment of a text message to an email address or mobile phone number. At the discretion and responsibility of the Client, the first name and last name (real name) of a person can also be submitted or pre-created (team lists / distribution lists created by the Client in the protected area). To best preserve the anonymity of recipients, the Client can use any other pseudonym instead of the real name.

When forwarding messages to recipients, only the most necessary data is passed on to other service providers. In addition to the message text, this is the mobile phone number for SMS and the email address for email.

Apart from technically necessary truncations, no content changes are made to the message text. The responsibility for adequate pseudonymization of this content lies entirely with the Client.

Data Minimization

The Processor uses personal data for the operation of its services only to the extent necessary for the guarantee of operations. Beyond this, the Clients are responsible for data economy within the framework of the applications they operate. As a rule, only email address and mobile phone number are essential for operation, but not the public name of the recipient.

TOM002 Integrity

Created: May 6, 2018 Last modified: May 30, 2022

(Art. 32(1)(b) GDPR)

The operation of the server infrastructure is outsourced to a sub-processor - referred to here as hoster. The processor from the end customer's perspective is web-me.de Internet Service e.K.

Transfer Control

Transfer control serves to protect against unauthorized reading, copying, modification or deletion of personal data during electronic transmission or transport. The Processor and the commissioned hoster implement transfer control through the following multi-level security measures:

1. The commissioned hoster implements transfer control by limiting storage to the designated data centers and server systems.
2. The commissioned hoster instructs all employees who come into contact with personal data according to Art. 32(4) GDPR and obligates them to confidentiality and to ensure data protection-compliant handling of personal data.
3. The Processor uses exclusively encrypted data transmission for the transfer of personal data.
4. The commissioned hoster ensures data protection-compliant deletion of data after termination of the order.
5. A third party can only retrieve, display or modify data after successful login within this temporary session that is linked to their unique customer number and unique key (UID).

Input Control

Input control serves to ensure the traceability of reading, copying, modifying or deleting personal data. The Processor and commissioned hoster implement input control through logging

of inputs made during administrative access and daily backup of data.

TOM003 Availability and Resilience

Created: May 6, 2018 Last modified: May 6, 2018

(Art. 32(1)(b) GDPR)

The operation of the server infrastructure is outsourced to a sub-processor - referred to here as hoster. The processor from the end customer's perspective is web-me.de Internet Service e.K.

Availability Control

Availability control serves to protect personal data against accidental or intentional destruction or loss as well as rapid recoverability (Art. 32(1)(c) GDPR). The commissioned hoster implements availability control through the following multi-level security measures:

The commissioned hoster: 1. Uses protection systems (spam filters, firewalls, virus scanners, encryption, (D)DoS defense). 2. Supports the availability of production systems through the use of redundant power supply, power supplies, storage systems and network components. 3. Supports the availability of production systems by mirroring all virtual machines in production in real time to standby servers or alternatively redundant configuration at software level. 4. Mirrors all customer systems in real time to standby servers, which can immediately take over tasks with current data in case of failure of the primary system. 5. Performs daily backups of configuration and server data, which are stored on separate servers in a separate data center at another location. 6. Has a partial (individual files) and complete (virtual machines) backup and recovery concept. 7. Monitors the productive systems from an external location. 8. Alerts the technical on-call staff via two independent channels in case of error. 9. Has defined an escalation chain for all internal systems that specifies who is to be informed in case of error in order to restore failed systems immediately.

These measures and procedures of the hoster are regularly checked by the Processor for functionality and changes.

TOM004 Procedures for Regular Review, Assessment and Evaluation

Created: May 6, 2018 Last modified: May 6, 2018

(Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

The operation of the server infrastructure is outsourced to a sub-processor - referred to here as hoster. The processor from the end customer's perspective is web-me.de Internet Service e.K.

For regular review, assessment and evaluation of procedures, the commissioned hoster has implemented the following concepts:

1. Data protection management
2. Incident response management
3. Privacy by design in software development (Art. 25(2) GDPR)

Order Control

Order control serves to protect personal data against non-instructed, unauthorized processing.

The regulation-compliant implementation of order processing according to Art. 28 GDPR is realized through clear contract design, careful selection of the processor, prior verification and follow-up checks, particularly with regard to expertise, reliability and resources.

1. The Processor concludes written agreements on services or order processing with the commissioned hosters and other sub-processors before the start of order processing, so that the data is treated confidentially or processed only in accordance with instructions. At a minimum, technical and organizational measures corresponding to the purpose and intent of the GDPR are agreed.
2. The Processor contractually excludes use or disclosure of data by employees.
3. The Processor obligates the hoster or other processors to accept instructions only from authorized employees. These orders are in text form and can be subsequently verified.
4. The hoster has data protection officers as well as an information security officer.
5. The service descriptions contain detailed information about the purpose limitation of the Client's personal data.

Document Date: January 2026