

Attachment: Order Processing Contract

1 Preamble

This Annex specifies the obligations of the contracting parties to data protection resulting from the contract concluded between the parties (General Terms and Conditions). It applies to all activities in connection with the contract in which employees of customweb or personal data (hereinafter referred to as "data") of the contractual partner are processed. In the following appendix we understand under the term client the customer or contractual partner of customweb. Partially also referenced as customer in the General Terms and Conditions.

2 Subject matter, duration and specification of order processing

Details regarding the service of customweb are regulated in the respective contract between customweb and the contract partner (hereinafter "contract").

The subject matter and duration of the order as well as the type and purpose of the processing result from the contract, unless otherwise stated in this Annex.

The term of this Annex is based on the term of the contract, provided that the provisions of this Annex do not give rise to obligations in excess thereof.

3 Scope and responsibility

customweb processes the data mentioned in appendix A on behalf of the client for the purpose mentioned in the contract. This includes activities which are specified in the contract and in this Annex.

Within the framework of this contract, the client is responsible for compliance with the statutory provisions of data protection laws, in particular for the legality of the transfer of data to customweb as well as for the legality of data processing ("responsible person" in the sense of Art. 4 No. 7 GDPR).

The instructions are initially defined by the contract and can then be changed, supplemented

or replaced by the client in written form or in an electronic format (text form). Instructions that are not present in the contract are treated as a request for a change in performance. Oral instructions must be followed up immediately in writing or in text form by the client.

4 Purpose of data collection

customweb provides the client with a payment service with which he can receive, manage and send transaction-related data received via his e-commerce site or other manual or automatic distance selling systems to the financial service providers he has selected to process the payments (transactions), provided that this selection is available and compatible with the Contractor's service.

The purpose of the processing of personal data is the processing of transaction-related data (such as but not limited to requests for authorization of a payment) and all supplementary or related activities that are necessary for the processing of transaction-related data.

Processing consists of collecting, consolidating, comparing, encrypting, decrypting, organising, checking, analysing, checking, registering, calculating, how-deriving, extending, copying, duplicating and transferring personal data to subcontractors, financial service providers or other (legal or natural) persons using the e-commerce platform ordered by the client and the tools connected to it via network connections and standard protocols that are involved in the processing of the transactions.

The personal data which are the subject of such processing are data which have been transmitted in encrypted form by the system of the customer to the system of the contractor and which have been recorded and processed during the processing of the transactions. In addition, personal data of the client's employees are also processed in the course of order processing.

5 Place of data processing

The provision of the contractually agreed data processing takes place exclusively in a member state of the European Union or in Switzerland. Any transfer to a third country may only take place if the special requirements of Art 44 ff. GDPR are fulfilled. Information on the location

of data processing at subcontractors can be found in the corresponding list.

6 Duties of customweb

1. customweb may collect data from data subjects for the aforementioned purposes, unless there is an exceptional case within the meaning of Article 28 para. 3 a) GDPR. customweb informs the client immediately if we believe that an instruction violates applicable laws. customweb may suspend the implementation of the instruction until it has been confirmed or amended by the client.
2. customweb will design the internal organization in his area of responsibility in such a way that it meets the special requirements of data protection. Customweb will take technical and organizational measures for the adequate protection of the client's data that meet the requirements of the Basic Data Protection Ordinance (Art. 32 GDPR). customweb must take technical and organisational measures to ensure the long-term confidentiality, integrity, availability and resilience of the systems and services in connection with the processing. The client is aware of these technical and organisational measures and is responsible for ensuring that they offer an appropriate level of protection for the risks of the data to be processed.
3. The measures taken by customweb are described in appendix B. The technical and organisational measures are subject to technical progress and further development. In this respect, customweb is allowed to implement alternative adequate measures. The safety level of the defined measures must not be undershot. Significant changes must be documented.
4. To the extent agreed, customweb supports the client within the scope of its possibilities in fulfilling the requests and claims of the persons concerned pursuant to Chapter III of the GDPR and in complying with the obligations set out in Articles 33 to 36 GDPR.
5. customweb guarantees that employees involved in the processing of the client's data and other persons working for customweb are prohibited from processing the data outside the instructions. Furthermore, customweb guarantees that the persons authorised to process the personal data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality.
6. customweb informs the client immediately if it becomes aware of violations of the protection of the client's personal data. customweb takes the necessary measures to secure the data and to reduce possible adverse consequences of the affected persons and agrees immediately with the client.
7. customweb names the following contact person for data protection questions arising in the context of the contract to the client: Inquiries are to be directed to info@customweb.com
8. customweb guarantees to comply with its obligations under Art. 32 para. 1 lit. d) GDPR to establish a procedure for regularly checking the effectiveness of technical and organisational measures to ensure the security of processing. customweb corrects or deletes the contractual data, if the client instructs this and this is included in the instruction framework. If a deletion in conformity with data protection or a corresponding restriction of data processing is not possible, customweb takes over the destruction of data carriers and other materials in conformity with data protection on the basis of an individual order by the client.
9. customweb will automatically delete personal data after termination of the contract and achievement of the purpose of this contract. At the request of the client, personal data must be deleted after the end of the contract. If additional costs arise due to deviating specifications in the surrender or deletion of the data, these shall be borne by the customer.
10. customweb undertakes to support the client in the defence of the claim within

the scope of the available and reasonable possibilities in the case of a claim against the client by a person concerned with regard to possible claims according to Art. 82 GDPR.

11. services in this section are to be paid to customweb according to the current hourly rates or external expenses.
12. The client is granted the right of inspection and control of the data processing facilities with regard to the processing of the data provided by him, including third parties commissioned by him. The contractor undertakes to provide the principal with the information necessary to monitor compliance with the obligations set out in this agreement.

7 Obligations of the client

The client is fully responsible for the legality of his instructions to customweb. In particular, it is the responsibility of the client to check whether the integration of a service / service / product, which customweb provides, does not violate data protection regulations. In addition, the customer has the following obligations:

1. The client has to inform customweb immediately and completely if he detects errors or irregularities regarding data protection regulations in the order results.
2. In the event of a claim against the principal by a data subject with regard to any claims under Art. 82 GDPR, paragraph 6 (10) shall apply mutatis mutandis.
3. The client names customweb the contact person for data protection questions arising in the context of the contract, if this deviates from the contact persons already named by the client.

8 Inquiries of persons concerned

If a person concerned contacts customweb with claims for correction, deletion or information, customweb will refer the person concerned to the client, provided that an assignment to the

client is possible according to information of the person concerned.

customweb forwards the request of the person concerned immediately to the client. customweb supports the client within the scope of his possibilities on instruction as far as agreed.

customweb is not liable if the request of the person concerned is not answered by the client, not correctly or not on time.

9 Audit

customweb proves to the client compliance with the obligations laid down in this Annex by suitable means. This is done through a self-audit and/or certification according to PCI DSS.

Should inspections be necessary in individual cases by the client or an auditor commissioned by the client, they shall be carried out during normal business hours without disrupting operations after notification, taking into account an appropriate lead time. customweb may make this conditional on prior notification with a reasonable lead time and on the signing of a non-disclosure agreement regarding the data of other customers and the technical and organisational measures set up. If the examiner commissioned by the client is in a competitive relationship with customweb, customweb has a right of objection against him.

Should a data protection supervisory authority or another sovereign supervisory authority of the contracting authority carry out an inspection, paragraph 2 shall apply mutatis mutandis. The signing of a confidentiality obligation is not required if this supervisory authority is subject to professional or legal secrecy, in which a violation is punishable under the Criminal Code.

For the possibility of controls by the client customweb can assert a remuneration claim.

10 Subcontractor

The assignment of subcontractors by customweb is permitted, as far as they fulfil the requirements of this appendix within the scope of the subcontract. A list of the current subcontractors is available here: <https://wallee.com/subcontractor.html>

Excluded are additional services, which customweb uses e.g. as telecommunication services, postal/transport services, maintenance and user services as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems.

The client agrees that customweb consults subcontractors. customweb informs the client before calling in or replacing the subcontractors. customweb is obliged to inform the client about the assignment of a subcontractor by updating the above overview. The overview must be updated at least 14 days in advance. The client will regularly inspect the overview. The client can object to the change - within 14 days - for an important reason - to customweb. If there is no objection within this period, consent to the change shall be deemed given. If there is an important reason under data protection law and if an amicable solution cannot be found between the parties, customweb is granted a special right of termination.

If customweb places orders with subcontractors, it is incumbent upon customweb to data protection obligations from this system to the subcontractor. Subcontractors who have no access to customer data or do not process customer data are excluded from this chapter and will therefore not appear in this list.

11 Information Duties

Should the client's data be endangered by seizure or confiscation, by insolvency or composition proceedings or by other events or measures of third parties, customweb has to inform the client immediately. customweb will immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the client as "responsible person" in the sense of the basic data protection regulation.

12 Liability

Liability is governed by the contract.

13 Miscellaneous

In all other respects, the provisions of the contract shall apply. In the event of contradictions between

The provisions of this Annex and the provisions of the contract shall take precedence over this Annex. Should individual parts of this Annex be ineffective, this shall not affect the effectiveness of the contract and the rest of the Annex.

The Annexes are an integral part of this Agreement.

Appendix A to the order processing contract

Subject of the order	Processing of personal data of the client within the scope of his use of the services of customweb as Software as a Service.
Nature and purpose of the intended processing of data	<p>The personal data processed by the client are transferred to customweb within the scope of the Software as a Service services. customweb processes this data exclusively according to the agreement made or the selected product.</p> <p>Depending on the selected service / product customweb transmits further data to this service provider (e.g. Shopify). The client is responsible for ensuring that this transfer does not infringe any rights of his customers.</p>
Type of personal data	<p>The supplementary agreement covers the following data types and categories:</p> <ul style="list-style-type: none"> • Person master data • Communication data (e.g. telephone, e-mail) • Online identification (IP address, cookie) • Payment data (details of orders placed and payments made) • Contract master data (contractual relationship, order data, product or contractual interest) • information (e.g. credit assessment of payment providers) • user behaviour
Categories of persons concerned	<p>The group of persons concerned by this Supplementary Agreement:</p> <ul style="list-style-type: none"> • customers and interested parties of the client • employees and suppliers of the client
Deletion, blocking and correction of data	Requests for deletion, blocking and correction are to be addressed to the client; otherwise the provisions of the contract apply.

Annex B to the order processing contract

Technical and organisational measures pursuant to Art. 30 para. 1 lit. g in conjunction with Art. 32 para. 1 GDPR

1 Physical access control

Access control (no unauthorized access to data processing systems) takes place. This includes the following measures:

- Key / allocation of keys
- door protection (electric door opener, etc.)
- Access to the processing servers and computers is protected in accordance with PCI DSS requirements (chapter 9) see also <https://aws.amazon.com/de/compliance/data-center/controls>.
- logging of access

2 System Access Control

Access control (no unauthorized system use) takes place. This includes the following measures:

- Password procedures (including special characters, minimum length, regular password changes)
- Two-factor authentication is used
- Automatic blocking (e.g. pause switching)
- Secure transmission of authentication secrets (credentials) in the network

3 Data access control

Access control takes place. This includes the following measures:

- Creation of an authorization concept
- Implementing access restrictions
- Assignment of minimum authorizations
- Administration and documentation of personal access rights
- Logging of data access

4 Transport / transfer control

A transport and transfer control takes place. This includes the following measures:

- Secure data transfer between server and client
- Securing the transfer in the backend
- Securing the transfer to external systems
- Implementation of security gateways at the network transfer points
- Hardening of the backend systems
- Description of all interfaces and the transmitted personal data fields
- Machine Machine Authentication
- Data carrier management (procedure)
- Collection and disposal process
- Data protection-compatible erasure/destruction procedure

5 Input control

An input check takes place. This includes the following measures:

- Documentation of input authorizations
- Logging of the entries

6 Order control

An order control takes place. This includes the following measures:

- Documentation of input authorizations
- Logging of the entries

7 Availability control:

Availability control takes place. This includes the following measures:

- backup concept
- Emergency plan
- Storage of backups
- testing of emergency facilities
- virus protection / firewall

8 Separation rule

Separation control / purpose of use control (separate processing of data collected for different purposes) takes place. This includes the following measures:

- Internal multi-client capability" is established
- Control of earmarking
- Separation of functions: production, staging, testing
- Separate processing