Order processing contract
in terms of §28 (3) of the General Data Protection Regulation (GDPR)

In case of differences between the German and English version of this Agreement, only the German version shall be decisive and applicable.

Preamble

This annex specifies the obligations of the contracting parties with regard to data protection. It shall apply to all activities which are connected with the contract and in which employees of the contractor or persons commissioned by the contractor process personal data ("data") of the customer.

1. Subject matter, duration and specification of the commissioned processing

The subject and duration of the order as well as the type and purpose of the processing result from the contract. In particular, the following data are part of the data processing:

Type of data	Nature and purpose of data processing	Categories of affected persons
Data of the client's customers (esp. names, address data, prefe-rence data)	Order fulfillment	Customers of the client
Contact information of the client's employees	Order fulfillment	Employees of the client
Billing address of the client (incl. contact)	Order accounting	Employees of the client

The term of this annex shall be governed by the term of the contract unless the provisions of this annex impose obligations in excess thereof.

2. Scope and responsibility

2.1. The contractor shall process personal data on behalf of the client. This includes activities that are specified in the contract and in the service description. Within the scope of this contract, the client shall be solely responsible for compliance with the statutory provisions of the data protection laws, in particular for the lawfulness of the transfer of data to the contractor as well as for the lawfulness of the data processing ("controller" within the meaning of article 4 No. 7 GDPR).

2.2. The instructions shall initially be stipulated by the contract and may thereafter be amended, supplemented, or replaced by individual instructions (individual instructions) by the customer in writing or in an electronic format (text form) to the place designated by the contractor. Instructions not provided for in the contract shall be treated as a request for a change in performance. Verbal instructions shall be confirmed immediately in writing or in text form.

3. Obligations of the contractor

3.1. The contractor may only process data of data subjects within the scope of the order and the client's instructions, unless there is an exceptional case within the meaning of article 28 (3) a) of the GDPR. The contractor shall inform the client without undue delay if it is of the opinion that an instruction violates applicable laws. The contractor may suspend the implementation of the instruction until it has been confirmed or amended by the client.

3.2. The contractor shall organize the internal organization in its area of responsibility in such a way that it meets the special requirements of data protection. It shall take technical and organizational measures for the adequate protection of the customer's data that meet the requirements of the data protection regulation (Art. 32 GDPR). The contractor shall take technical and organizational measures to ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with the processing on a permanent basis. The customer is aware of these technical and organizational measures and is responsible for ensuring that they provide an appropriate level of protection for the risks associated with the data to be processed.
These technical and organizational measures are listed in the attached **appendix "Technical and Organizational Measures"**. The contractor reserves the right to change the security measures taken, however, it must be ensured that the contractually agreed level of protection is not undercut.

3.3. The contractor shall support the client - to the extent agreed - within the scope of its possibilities in fulfilling the requests and claims of data subjects pursuant to chapter III of the GDPR and in complying with the obligations set forth in articles 33 to 36 of the GDPR.

3.4. The contractor warrants that the employees involved in the processing of the client's data and other persons working for the contractor are prohibited from processing the data outside the scope of the instruction. Furthermore, the contractor warrants that the persons authorized to process the personal data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality. The confidentiality/confidentiality obligation shall continue to exist even after termination of the order.

3.5. The contractor shall inform the client without delay if it becomes aware of any violations of the client's personal data protection.
The contractor shall take the necessary measures to secure the data and to mitigate possible adverse consequences for the persons concerned and shall consult with the client on this without delay.

3.6. The contractor shall inform the customer of the contact person for data protection issues arising within the scope of the contract.

3.7. The contractor shall ensure that it complies with its obligations under article 32 (1) d) of the GDPR to implement a procedure for the regular review of the effectiveness of the technical and organizational measures to ensure the security of the Processing.

3.8. The contractor shall correct or delete the contractual data if the client instructs it to do so and this is covered by the scope of the instructions. If deletion in compliance with data protection or a corresponding restriction of data processing is not possible, the contractor shall undertake the destruction of data carriers and other materials in compliance with data protection on the basis of an individual order by the customer or shall return these data carriers to the customer, unless already agreed in the contract.
In special cases to be determined by the client, storage or transfer shall take place. Protective measures for this are to be agreed separately, unless already agreed in the contract.

3.9. Data, data carriers and all other materials shall be either surrendered or deleted at the request of the client after the end of the order.
If additional costs are incurred due to deviating specifications for the return or deletion of the data, these shall be borne by the client.

3.10. In the event of a claim against the client by a data subject with regard to any claims pursuant to art. 82 of the GDPR, the contractor undertakes to support the client in defending the claim within the scope of its possibilities.

4. Obligations of the customer

4.1. The customer shall inform the contractor immediately and in full if it discovers errors or irregularities in the results of the order with regard to provisions of data protection law.

4.2. In the event of a claim against the client by a data subject with regard to any claims pursuant to art. 82 of the GDPR, section 3 (10) shall apply accordingly.

4.3. The customer shall inform the contractor of the contact person for data protection issues arising within the scope of the contract.

5. Requests from affected persons

If a data subject approaches the contractor with requests for correction, deletion or information, the contractor shall refer the data subject to the client, provided that an assignment to the client is possible according to the data subject's information. The contractor shall immediately forward the request of the data subject to the customer. The contractor shall support the client within the scope of its possibilities upon instruction to the extent agreed. The contractor shall not be liable if the request of the person concerned is not answered by the client, is not answered correctly, or is not answered in due time.

6. Verification possibilities

6.1. The contractor shall prove to the client compliance with the obligations set forth in this agreement by appropriate means.

6.2. If, in individual cases, inspections by the customer or an inspector commissioned by the customer are necessary, these shall be carried out during normal business hours without disrupting operations after notification and taking into account a reasonable lead time. The contractor may make such inspections dependent on prior notification with a reasonable lead time and on the signing of a confidentiality agreement with regard to the data of other customers and the technical and organizational measures implemented. If the auditor appointed by the customer is in a competitive relationship with the contractor, the contractor shall have a right of objection against him.
The customer agrees to the appointment of an independent external auditor by the contractor, provided that the contractor provides a copy of the audit report.
The expenditure of an inspection is generally limited to one day per calendar year for the contractor.

6.3. Should a data protection supervisory authority or another sovereign supervisory authority of the client carry out an inspection, paragraph 2 shall apply accordingly. It shall not be necessary to sign a confidentiality agreement if this supervisory authority is subject to a professional or statutory confidentiality obligation for which a violation is punishable under the German Criminal Code.

7. Subcontractors (other processors)

7.1. The processor shall inform the contractor prior to any intended change with regard to the use or replacement of a subcontractor. The contractor may object to the intended use or replacement of a subcontractor for good cause under data protection law. A subcontractor relationship subject to approval exists if the contractor commissions other contractors to perform all or part of the work agreed in the contract. The contractor shall conclude agreements with these third parties to the extent necessary to ensure appropriate data protection and information security measures.

The contractually agreed services or the partial services described below shall be performed with the involvement of the following subcontractors:

Name and address of the subcontractor	Description of partial services
DATEN_PARTNER Gesellschaft für Direktmarketing und Informations-Technologie mbH Feldheider Str. 39 – 45 40699 Erkrath Deutschland (EU)	Printing and shipping of personalized advertising materials
STRATO AG Pascalstraße 10 10587 Berlin Deutschland (EU)	The customer-specific advertising materials (including the above-mentioned customer data of the client) are calculated in data centers of STRATO AG.
QualityHosting AG Uferweg 40-42 63571 Gelnhausen Deutschland (EU) **Microsoft Ireland Operations Limited** Leopardstown, Dublin 18, D18 P521, Irland (EU)	Use of Microsoft Office 365: • Exchange (communication with the client) • Teams (conference calls, web telephony) • SharePoint, OneDrive (file storage and versioning)
SoftwareONE Deutschland GmbH Blochstraße 1 04329 Leipzig Deutschland (EU)	Leveraging Azure through SoftwareONE as an end-to-end software and cloud technology solution provider.
HubSpot, Inc. 25 1st Street Cambridge MA 0214 USA	Storage of the client's billing address for invoicing purposes

Before calling in further subcontractors or replacing listed subcontractors, the contractor shall obtain the consent of the client, which may not be refused without an important reason under data protection law.

7.2. If the contractor places orders with subcontractors, it shall be incumbent upon the contractor to transfer its obligations under data protection law from this agreement to the subcontractor.

8. Information obligations, written form clause, choice of law

8.1. If the customer's data at the contractor is endangered by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the contractor shall inform the

customer thereof without undue delay. The contractor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lie exclusively with the client as the "responsible person" within the meaning of the general data protection regulation.

8.2. Amendments and supplements to this annex and all its components - including any assurances of the contractor - shall require a written agreement, which may also be in an electronic format (text form), and the express indication that it is an amendment or supplement to these terms and conditions. This shall also apply to the waiver of this formal requirement.

8.3. In the event of any contradictions, the provisions of this annex on data protection shall take precedence over the provisions of the agreement. Should individual parts of this annex be invalid, this shall not affect the validity of the rest of the annex.

8.4. German law shall apply.

9. Liability and compensation

The client and the contractor shall be liable vis-à-vis data subjects in accordance with the provision set out in article 82 of the GDPR.

10. Costs and expenses

10.1. Insofar as data protection obligations incumbent upon the client are fulfilled by the contractor on the client's instructions, the client shall remunerate these services.

10.2. The contractor may also demand reimbursement from the client for costs and expenses incurred for checks or inspections by the client, in particular costs for checks not related to the cause. The above provision in sentence 1 shall not apply to inspections carried out by the client in the course of fulfilling its statutory inspection obligations.

10.3. The amount of the remuneration and the settlement modalities result from the price list sent with the offer.

TECHNICAL AND ORGANIZATIONAL MEASURES

In case of differences between the German and English version of this Agreement, only the German version shall be decisive and applicable.

1. Introduction

1.1. Responsible

The responsible party pursuant to article 4 (7) of the EU General Data Protection Regulation (GDPR) is AutLay - Automatisches Layout GmbH, Unter Käster 14-16, 50667 Cologne, Germany, e-mail: mail@autlay.com. We are legally represented by Dr. David Schölgens, Sven Müller.

1.2. Data protection officer

Our data protection officer is heyData GmbH, Gormannstr. 14, 10119 Berlin, www.heydata.eu, e-mail: info@heydata.de.

1.3. Subject of the document

This document summarizes the technical and organizational measures taken by the controller within the meaning of article 32 (1) of the GDPR. These are measures with which the controller protects personal data. The purpose of the document is to support the controller in fulfilling its accountability obligations under article 5 (2) of the GDPR.

2. Confidentiality (Art. 32 para. 1 lit. b GDPR)

2.1. Entry control

The following implemented measures prevent unauthorized persons from gaining access to the data processing facilities:

- Manual locking system (e.g., key)
- Security locks
- Key regulation / key book
- Careful selection of cleaning personnel.

2.2. Access control

The following implemented measures prevent unauthorized persons from accessing the data processing systems:

- Authentication with user and password
- Authentication with biometric data
- Use of mobile device management
- Encryption of data carriers
- Encryption of notebooks / tablets
- Management of user authorizations
- Creation of user profiles
- Central password rules
- Use of 2-factor authentication
- Key regulation / key book

2.3. Control of data retrieval

The following implemented measures ensure that unauthorized persons do not have access to personal data:

- Use of document shredders (with cross cut function).
- Logging of accesses to applications (especially when entering, changing, and deleting data)
- Use of an authorization concept
- Number of administrators is kept as small as possible
- Management of user rights by system administrators.

2.4. Separation control

The following measures ensure that personal data collected for different purposes are processed separately:

- Separation of productive and test system
- Logical client separation (on the software side)
- Creation of an authorization concept
- Definition of database rights

3. Integrity (Art. 32 para. 1 lit. b GDPR)

3.1. Transfer control

It is ensured that personal data cannot be read, copied, changed or removed without authorization during transfer or storage on data carriers and that it is possible to check which persons or bodies have received personal data. The following measures have been implemented to ensure this:

- WLAN encryption (WPA2 with strong password)

3.2. Input control

The following measures ensure that it is possible to check who has processed personal data in data processing systems and at what time:

- Logging of the entry, modification, and deletion of data
- Traceability of data entry, modification, and deletion through individual usernames (not user groups)
- Allocation of rights for entering, changing, and deleting data based on an authorization concept.

4. Availability and resilience (Art. 32 para. 1 lit. b GDPR)

The following measures ensure that personal data is protected against accidental destruction or loss and is always available to the client:

- Hosting (at least of the most important data) with a professional hoster

5. Procedures for regular review, assessment, and evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

5.1. Data protection management

The following measures are intended to ensure that an organization that meets the basic requirements of data protection law is in place:

- Use of the heyData platform for data protection management
- Designation of the data protection officer heyData
- Obligation of employees to maintain data secrecy
- Regular training of employees in data protection

- Maintaining an overview of processing activities (Art. 30 GDPR).
- Conducting data protection impact assessments, if required (Art. 35 GDPR).

5.2. Incident-Response-Management

The following measures are intended to ensure that notification processes are triggered in the event of data protection breaches:

- Notification process for data protection breaches pursuant to Art. 4 No. 12 GDPR towards supervisory authorities (Art. 33 GDPR)
- Notification process for data protection breaches pursuant to Art. 4 No. 12 of the GDPR towards the data subjects (Art. 34 of the GDPR)
- Involvement of the data protection officer in security incidents and data breaches

5.3. Privacy-friendly default settings (Art. 25 (2) GDPR)

The following implemented measures consider the requirements of the "Privacy by de-sign" and "Privacy by default" principles:

- Training of employees in "Privacy by design" and "Privacy by default".
- No more personal data is collected than is necessary for the respective purpose.

5.4. Order control

The following measures ensure that personal data can only be processed in accordance with instructions:

- Written instructions to the contractor or instructions in text form (e.g., by order processing contract).
- Ensuring the destruction of data after completion of the order, e.g., by requesting corresponding confirmations.
- Confirmation by contractors that they obligate their own employees to maintain data secrecy (typically in the order processing contract)
- Careful selection of contractors (especially regarding data security).