Contract for order processing

between

Manufacturer

hereinafter referred to as the **Client**

and

Layer Software GmbH
Manteuffelstr 77
10999 Berlin

hereinafter referred to as the **Contractor**

§1 Subject of the Agreement

This contract regulates the processing of the personal data of the clients of the client, which the Contractor processes in the course of rendering the services for the client ("data").
Personal data is all the information which relates to an identified or identifiable natural individual. The client is solely responsible for determining whether any data processing is permissible and whether rights are adequately protected.

§ 2 Nature and purpose of the data processing of the client

(1) Nature and purpose of the processing
According to the statutory definition, these include in particular: "collecting, recording, organising, filing, storing, adapting or modifying, reading, retrieving, using, disclosing by transmission, dissemination or any other form of provision, matching or linking, restricting, deleting or destroying".

The processing serves the following purpose: The Contractor enables easier cooperation within the company. This includes the internal sharing of data as well as simplified processing. This is made possible by the specially developed tool.

(2) Nature of the data
The following data is processed:

- Personal data (salutation, name, address, delivery address, telephone, email)
- Order data: goods, quantity, price

(3) Categories of data subjects affected by the processing:

- Customers
- Employees

§ 3 Obligations of the Contractor

(1) The contractor undertakes to comply with the provisions of the relevant data protection laws and to observe the principles of proper data processing

(2) The contractor processes the data exclusively in the framework and for the purpose of providing the services for the client and according to its documented instructions. Copies and duplicates of data shall not be created without the knowledge and agreement of the client.

The instructions are initially determined by this agreement and may be subsequently amended, supplemented or replaced by the client by means of documented instructions.

Persons authorised by the Client to issue instructions are:
To be named

The individuals authorized by the Contractor to receive instructions:
Constantin Schünemann und Moritz Ten Eikelder

The Contractor does not process the personal data in any other way or for any other purpose unless he is legally obliged to do so.

(3) If personal data are to be corrected, deleted or blocked, the Contractor will do so within a reasonable time and will confirm this to the client in writing.

(4) The parties undertake to appoint a data protection officer, insofar as this is required by law, to provide their contact details and to cooperate with the data protection officer of the client.

Data Protection Officer of the Client: (fill out if available)

External Data Protection Officer of the Contractor:
heyData UG (limited liability), Daniel Deutsch, Milos Djurdjevic
Phone +49 89 41325320, Email: support@heydata.de

(5) The Contractor will familiarise its employees, who are responsible for the processing of personal data, with the relevant provisions of data protection and will oblige them in writing to maintain confidentiality and data secrecy.

(6) If the data of the client is unlawfully obtained, that is in violation of applicable data protection law, this contract or instructions of the client, to the knowledge of an unauthoriaed third party, the Contractor informs the Client about this immediately.

(7) Support and information obligation. If the client is only able to fulfil his obligations to the persons concerned (in particular the obligation to provide the affected person with information about the processing of his personal data) with the help of the Contractor, the Contractor will support the client on request. The client will compensate the Contractor according to the amount of time spent according to the assigned personnel in the usual local and appropriate amount.

Likewise, the Contractor, taking into account the nature of the processing and the information at his disposal, may order the Client to perform his obligations with regard to the security of personal data (processing security, notification of personal data breaches to the supervisory authority, Informing the person concerned about a personal data protection breach) and any necessary data protection impact assessment and prior consultations.

(8) The Contractor shall design its organisation in such a way that it meets the special requirements of data protection. He will take technical and organisational measures to adequately safeguard the personal data against misuse and loss that comply with the relevant data protection regulations. The contractor will implement and comply with the technical and organisational measures listed in **Annex 1** for this contract. The Contractor must prove the measures to the Client and any supervisory authorities upon request.

The technical and organisational measures are subject to technical progress and further development. In that regard, the Contractor is permitted to implement adequate alternative measures. In so doing, the security level must not fall below that of the previously agreed measures.

1. PHYSICAL ACCESS CONTROL
2. SYSTEM ACCESS CONTROL
3. NETWORK ACCESS CONTROL / SEPARATION
4. TRANSFER CONTROL
5. INPUT CHECK / MEMORY CHECK
6. JOB/ORDER CONTROL
7. AVAILABILITY CONTROL
8. PURPOSE
9. ORGANISATIONAL CONTROL
10. PSEUDONYMISATION

Likewise, the Contractor ensures that subordinated natural persons who have access to personal data process them only according to their purpose and at the instruction of the client, unless they are legally obliged to process them.

In the event that the security measures taken at the Contractor do not meet the requirements of the client, he notifies the client. The same shall apply to malfunctions and to suspected violations of data protection or to irregularities in the processing of personal data.

(9) The Contractor shall insure compliance with the obligation and shall provide appropriate insurance cover for liability damage during the term of this agreement and shall prove this to the Client upon request. The contractor also warrants that the data processed will be kept separate from other data in its possession.

(10) The Client shall be entitled to check the Contractor's compliance with the statutory provisions on data protection, the contractual agreements between the parties and the Client's instructions. The contractor will support and facilitate the Client for such controls. In particular, the support is provided by providing all information required to prove compliance with the data protection provisions.

(11) Authorisation of the Contractor to correct, erase and block
Legal or contractual deletion or storage periods of the data processed in the order are ensured by the Contractor at its own discretion. In addition, the Contractor may not correct, delete in accordance with data protection regulations or restrict the processing of data processed on behalf of the Client without authorisation, but only in accordance with documented instructions from the Client. If an affected person directly addresses the Contractor in this regard, the Contractor will forward this request to the Client.

(12) Your rights as a data subject
Deletion claim, right to be forgotten, rectification, data portability and information are ensured by the Contractor in its sole discretion and implemented in the individual case according to the corresponding documented instructions of the Client

(13) After completion of the contractual work, the Contractor shall, in accordance with the instructions of the Client,
hand over to the Client all documents in his possession and any processing or usage results created in connection with the contractual relationship.

§ 4 Subcontractors / subcontracting

(1) Subcontracting in terms of data processing on behalf
Subcontracting within the meaning of this provision include those services which relate directly to the provision of the main service. This does not include ancillary services which the Contractor uses such as telecommunication services, postal/transport services, maintenance, and user services, or data carrier disposal, or any other measures to ensure the confidentiality, availability, integrity, and resilience of the hardware and software of its data processing systems. However, the Contractor shall be obliged to enter into appropriate and legally binding contractual agreements and control measures to ensure the protection and security of the Client's data, especially when such services are outsourced.

(2) Involvement / commissioning of subcontractors
The Client shall only agree, with the prior consent of the Contractor, that the Contractor may use subcontractors for the performance of its contractual services under the condition of a contractual agreement in accordance with Art. 28 para. 2-4 of the GDPR. In the case of consent, the Contractor has to ensure by contract that the agreed regulations also apply to subcontractors. The contractor must regularly check compliance with the contractual obligations by the subcontractor.

(3) Transfer of the data to the subcontractor
The passing on of personal data of the client to the subcontractor and his first action are only permitted when all requirements for subcontracting according to § 3 para. 2 of the contract are met and when the subcontractor has fulfilled the obligation according to § 2 para. 9 of the contract.

§ 5 Confidentiality / Data secrecy

The contractor undertakes to maintain data secrecy and to obligate his employees accordingly when processing the personal data of the client in accordance with the order.

The special duty of confidentiality, in particular the relevant data protection regulations, especially in dealing with the personal data of clients of the client and the criminal liability for breach of confidentiality are known to the Contractor. For this purpose, the Contractor has to carry out record-breaking instructions and to oblige its employees in writing to maintain secrecy and to prove this declaration to the Client on request. The Contractor warrants that he will familiarise the employees employed in the performance of the work with the relevant provisions of data protection / confidentiality pursuant to § 203 StGB (German Criminal Code). The contractor monitors compliance with the aforementioned regulations and general data confidentiality.

The Contractor may only provide information to third parties with the prior written consent of the Client.

The activity of the Contractor is necessary so that customers of the Client are enabled to buy goods online and the purchase on account with attractive payment terms can be offered.

The Contractor and its vicarious agents are thereby contributors within the meaning of § 203 para. 4 of the German Criminal Code (StGB) and may be punished with imprisonment of up to one year or a fine if the customer data of the Client are disclosed to third parties.

The Contractor is aware of the special duty of confidentiality, particularly in dealing with the personal data of the Client's customers, and of the criminal nature of the breach of the duty of confidentiality.

§ 6 Contract Period

The contract has a term of one year from the date of signing. It will be extended for another year at the end of the term if it is not terminated before expiry of the respective term, subject to a notice period of three months to the end of the term.

The right to extraordinary termination of the contract for cause remains unaffected.

At the latest when the contract is terminated, the Contractor will delete the data of the client from his data carriers and destroy the corresponding documents with him, unless the Contractor is legally obliged to keep them or has a legitimate interest in data retention.

The above deletion obligations shall not apply to copies of data contained in periodic backup copies of the Contractor's comprehensive data sets, the isolated deletion of which would entail considerable expense for the Contractor and which would be incurred by the Contractor.

The obligations of the Contractor under this contract are valid for 3 years beyond the termination of the contract, the obligation of confidentiality unlimited.

§ 7 Liability

The contractor and his vicarious agents are not liable for material damage and expenses incurred by the client as a result of the execution of the contract, unless the contractor or his vicarious agents have caused the damage intentionally or through gross negligence. The liability for gross negligence is limited to the amount of the average damage typical for the contract and limited to the liability insurance sum of the customer's liability insurance.
Exclusion or limitation of liability for damages resulting from injury to life, limb or health, which are based on a negligent breach of duty by the client or a wilful or negligent breach of duty or vicarious agents, is not connected with this. The liability of the Contractor for lost profit of the client is excluded.

8 Final provisions

(1) Ancillary agreements and changes to the contract must be in writing in order to be valid, and this also applies to the change of the written form clause.

(2) This Agreement is governed by German law. The place of fulfilment is Berlin.

(3) Should individual provisions of this agreement be invalid or should a gap in this agreement become apparent, this shall not affect the validity of the remaining provisions. In place of the ineffective agreement provision or to fill the gap, a legally effective substitute regulation shall take effect, which takes

into account the intention of the parties recognisable from this agreement, the economic sense and purpose of the omitted regulation and the total agreement or comes as close as possible.

_____	_____
Place, Date	Place, Date
_____	_____
Client	Contractor

Annex 1: TECHNICAL AND ORGANISATIONAL MEASURES

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

a) Physical access control

The following measures implemented prevent unauthorised persons from gaining access to the data processing systems:

- Protection of building shafts
- Automatic access control system
- Chip card/transponder locking system
- Security locks
- Careful selection of cleaning personnel

b) System access control

The following measures implemented prevent unauthorised persons from having access to the data processing systems.

- Authentication with user + password
- Use of anti-virus software
- Use of firewalls
- Encryption of notebooks / tablets
- Manage user permissions
- Creating user profiles
- Central password allocation / password rules

c) Network access control

The following measures implemented ensure that unauthorised persons do not have access to personal data.

- Use of document shredders (crosscut)
- Logging the destruction of data
- Reduce the number of administrators to the "bare minimum
- Administration of user rights by system administrators

d) Separation control

The following measures ensure that personal data collected for different purposes is processed separately.

- Physically separate storage on separate systems or data carriers
- Separation of production and test system
- Definition of database rights
- Internal refusal to anonymize/pseudonymize personal data in case of disclosure or even after expiry of the legal deletion period

e) Pseudonymisation (Art. 32 para. 1 lit. a GDPR; Article 25 para. 1 GDPR)

The processing of personal data occurs in such a way that the data can no longer be assigned to a specific data subject without additional information being provided, given that such additional information is kept separate and subject to appropriate technical and organisational measures.

For this purpose, the data is linked to unique pseudonyms before further processing and further personal data is removed.

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

a) Delivery control

It is ensured that personal data can not be read, copied, altered or removed without authorisation during transmission or storage on data carriers and that it is possible to check which persons or bodies have received personal data. To ensure the following measures are implemented:

- Provision over encrypted connections like sftp, https

b) input control

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

- Clear responsibilities for deletions

3. Availability and dependability (Art. 32 para. 1 lit. b GDPR)

Availability control and resilience control

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

- Fire extinguishing equipment in server rooms
- Devices for monitoring temperature and humidity in server rooms
- Protective socket strips in server rooms
- Privacy safe
- Creation of a backup & recovery concept
- Storage of data backup in a secure, outsourced location
- No sanitary facilities in or above the server room
- Separate partitions for operating systems and data

4. Procedures for Regular Review, Assessment and Evaluation (Art. 32 para. 1(d) of the GDPR; Article 25 para. 1 GDPR)

a) Data protection management

The following measures are intended to ensure that an organisation satisfying basic data protection requirements is in place:

- Appointment of an external data protection officer
- Commitment of employees to data secrecy and banking secrecy
- Sufficient training of employees in privacy matters
- Keep an overview of processing activities (Art. 30 GDPR)
- Implementation of data protection impact assessments, if necessary (Art. 35 GDPR)

b) Incident response management

The following measures should ensure that reporting processes are triggered in the event of data breaches:

- Reporting process for data breaches according to Art. 4 No. 12 GDPR vis-à-vis the supervisory authorities (Art. 33 GDPR)
- Notification process for data protection violations according to Art. 4 No. 12 GDPR vis-à-vis the data subjects (Art. 34 GDPR)

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

The default settings are to be considered both for the standardised presettings of systems and apps as well as for the setup of the data processing methods. In this phase, functions and rights are concretely configured, the admissibility or inadmissibility of certain inputs or of input options (eg of free texts) is defined with regard to data minimisation and the availability of usage functions is decided (eg with regard to scope) the processing). Likewise, the type and scope of the personal reference or the anonymisation (eg in selection, export and evaluation functions, which can be specified and preset or freely designable) or the availability of certain processing functions, logging etc. established.

- Marking of optional input fields in online forms
- Pseudonymisation of data before further processing

d) Order control

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

- Identification of contact persons and / or responsible employees
- Commitment of employees to data secrecy
- Selection of the Contractor under care aspects (in particular with regards to data security)
- Ongoing review of the Contractor and its activities