General Order Processing Terms and Conditions

of the

stratEDI GmbH, Lusebrink 9, 58285 Gevelsberg, Germany

-Contractor-

Preamble

These Terms and Conditions describe the contract parties' data protection obligations that follow from the respective contracts of the parties. These Terms and Conditions apply to all activities related to the contracts and for which employees of the Contractor or parties commissioned by the Contractor process personal data (»data«) of the Client.

§ 1 Area of Applicability and Responsibility

The Contractor shall process personal data on behalf of the Client. This shall include activities specified by the respective contract and, if applicable, in the service description. The duration of this contract corresponds with the duration of the main contract. For each contract, the Client shall be solely responsible for adherence to legal data protection regulations, especially for the legitimacy of data transfers to the Contractor and for the legitimacy of data processing (»controller« in the sense of Art. 4 No. 7 of the GDPR).

The Contractor's obligations under data protection law shall be specified by the contract and may subsequently be changed, supplemented or replaced by the Client in written form or electronic format (text form) through individual directives (individual directives). Oral directives must be confirmed in writing or in text form without delay.

The type and purpose of the processing, the type of data to be processed and the data subject categories shall follow the service description (name, address, email address, telephone number).

§ 2 Duties of the Contractor

The Contractor may only process data of data subjects as part of the order or directive of the Client, unless an exception under Art. 28(3a) of the General Data Protection Regulation (GDPR) applies. The Contractor must notify the Client without delay if he believes that the Client's directives violate applicable laws. The Contractor may suspend the execution of the directive until the directive is confirmed or changed by the Client.

1.The Client shall name the persons with the authority to issue directives. Changes must be reported beforehand in writing and in a timely manner.

Directive recipients of the Contractor shall be:

- Dr. Thorsten Georg, CEO, 02332 66600-0
- Andreas Weng, EDI Project Manager, 02332 66600-0
- Markus Martini, EDI Project Manager, 02332 66600-0

2. The Contractor shall structure his internal company organization within his area of applicability to account for the special requirements of data protection. The Contractor shall implement technical and organizational measures that meet the requirements of the General Data Protection Regulation to provide proper protection of the Client's data (Art. 32 of the GDPR). The Contractor must implement technical and organizational measures that ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. The Client shall be aware of these technical and organizational measures and shall be responsible for ensuring that these measures provide an adequate level of protection against the risks of the data to be processed.

Changes to implemented security measures shall remain reserved to the Contractor, though the contractually agreed level of protection must be maintained.

A description of the technical-organizational measures of the Contractor shall be provided after these General Terms and Conditions.

3. The Contractor shall, to the best of his ability, support the Client with the fulfillment of requests and demands of data subjects in accordance with Chapter III of the GDPR and with adherence to the duties under Art. 33 to 36 of the GDPR. The Client shall compensate the Contractor for these efforts at the Contractor's respectively applicable hourly rates.

4. The Contractor shall guarantee that his employees and other persons serving the Contractor shall be prohibited from processing data contrary to the respective directive. Furthermore, the Contractor must guarantee that the persons authorized to process personal data have committed to maintain confidentiality or are subject to appropriate legal confidentiality obligations. Such confidentiality obligations shall continue to apply even after the completion of the order.

5. The Contractor shall notify the Client without delay upon learning of any violations of the protection of the Client's personal data.

The Contractor must take any measures required for ensuring the security of the data and reducing possible disadvantages to the data subjects and shall coordinate such measures with the Client without delay.

6. The Contractor shall state his internal data protection officer for any data protection questions under this Contract to the Client.

7. The Contractor must guarantee that he will fulfill his obligations under Art. 32(1) Letter d of the GDPR for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

8. The Contractor shall correct or delete the Contractual data on the Client's orders. If data cannot be deleted or if its processing cannot be limited in accordance with applicable data protection regulations, the Contractor shall, in accordance with data protection regulations, destroy data carriers and other materials due to individual orders by the Client or shall return these data carriers to the Client unless agreed otherwise in the contract.

In special cases to be determined by the Client, storage or handover shall be performed for which the according remuneration and protective measures must be concluded separately unless already agreed to in the contract.

9. Data, data carriers and any other material must be returned or deleted on the Client's request upon the completion of the order.

10. Should claims under Art. 82 of the GDPR be asserted against the Client by a data subject, the Contractor must, to the best of his ability, support the Client with the defense against such claims free of charge.

11. The Client shall compensate the Contractor for these efforts at the Contractor's respectively applicable hourly rates.

§ 3 Duties of the Client

1. The Client must notify the Contractor completely and without delay about any data protection regulation errors or irregularities discovered in the order results.

2. In the event of a recourse of the contractor by an affected person in terms of possible claims under Art. 82 of the GDPR §2 Abs. 10 shall apply accordingly.

3. The Client shall state his contact person for any data protection questions under this contract to the Contractor.

§ 4 Requests of Data Subjects

If a data subject submits a deletion or information request to the Contractor, the Contractor shall refer the data subject to the Client if the request can be assigned to the Client based on the information of the data subject. The Contractor shall forward the data subject's request to the Client without delay. The Contractor must, to the best of his ability, support the Client in accordance with any respective directives insofar as agreed. The Contractor shall not be liable if the Client fails to respond to the data subject's request or does not respond correctly or in time.

§ 5 Possible Proof

1. The Contractor shall prove his adherence to his duties under this contract to the Client through suitable means.

2. Should inspections by the Client or by an auditor commissioned by the Client be required in individual cases, such inspections shall be performed during regular business hours without disrupting the Client's business operations and with an appropriate lead time following registration. The Contractor may make this conditional on prior registration with an appropriate lead time and the signing of a confidentiality agreement for the data of other customers and the established technical and organizational measures. Should the auditor commissioned by the Client be in competition with the Contractor, the Contractor may object to his commissioning.

The Client shall compensate the Contractor for his support with the performance of an audit at the Contractor's respectively applicable hourly rates.

3. Should data protection regulatory authorities or other sovereign authorities of the Client perform audits, Subsection 2 shall apply accordingly. The signing of a confidentiality agreement shall not be required if the regulatory authorities are subject to legal or professional confidentiality requirements whose violations constitute offenses under the German Criminal Code [Strafgesetzbuch, StGB].

§ 6 Subcontractors (Other Order Processors)

1.To fulfill his contractual obligations, the Contractor makes use of the services of the subcontractors mentioned in attachment 2.[…]

2. Such a subcontractor relationship shall be present if the Contractor commissions other contractors for all or part of the Contractually agreed services. The Contractor must conclude agreements with these third parties to the extent required for ensuring appropriate data and information security measures.

3. The Client shall allow the Contractor to include subcontractors. The Contractor shall notify the Client about the inclusion or replacement of any subcontractors with a notice period of three weeks. The Client may object to the changes—within an appropriate period—for a compelling reason. If no objection is raised within the stated period, approval of the change shall be deemed to have been granted.

4. If the Contractor awards orders to subcontractors, the Contractor shall be responsible for transferring his data protection obligations under this Contract to the subcontractors.

§ 7 Obligation to Provide Information, Written Form Clause, Applicable Law

1. Should the Client's data be threatened by seizure or confiscation, insolvency or settlement proceedings or other events or measures by third parties at the Contractor's office, the Contractor must notify the Client of this without delay. The Contractor must inform all persons responsible without delay that sovereignty and ownership of the data belongs solely to the Client as the »responsible person« in the sense of the General Data Protection Regulation.

2. Changes or additions to these General Terms and Conditions and any of their parts—including any assurances of the Contractor—shall require a written agreement that may also be issued in electronic format (text form). An express notice that changes or additions to these conditions are being made shall also be required. The same shall apply to any waiver of this written form requirement.

In case of contradictions, this Annex on order processing shall take precedence over the contract. Should individual parts of this Annex prove to be invalid, the validity of the Annex shall remain.

3. German law shall apply.

Annex 1: Technical and Organizational Measures Under Art. 32 of the GDPR

A. Confidentiality (Art. 32 No 1 lit. b of the GDPR)

1. Access Control:

Measures for preventing unauthorized access to the data processing systems that process personal data:

Among other things, the following measures must especially be emphasized at the Verizon data center:

- Access to the system requires prior registration and a prior order
- Access is only granted to a defined circle of persons
- Several factors are used for authentication

Office access controls to be especially emphasized:

- The building is secured by an alarm system
- A locking system with defined responsibilities and that traces key issuance and returns. If keys are lost, the locking system will be replaced; new keys will only be ordered following separate authentication and authorization
- Non-company persons (including craftsmen) are picked up from the company's central reception and accompanied inside the company building
- Visitors cannot access rooms through locked areas and floors of the company building
- Responsibilities for backup storage are defined and access is severely restricted; the room housing the backup safe is secured separately

2. Usage Controls

Measures to prevent unauthorized persons from using the data processing systems and procedures:

- Access control to the servers is subject to measures by Verizon
- The Contractor employs a multi-step authorization system for the administration of the servers
- All passwords are subject to password guidelines

3. Access Controls

Measures to ensure that persons authorized to use the data processing procedures can only access the personal data for which they received authorization:

- Only persons from the EDI processing division may access the server infrastructure
- Areas requiring permission are separated by different passwords

4. Separation Controls

Measures to ensure that data collected for different purposes can be processed separately:

- Separation controls are based on addressing according to customer specifications

B. Integrity (Art. 32 No 1 lit. c of the GDPR)

1. Transfer Controls

Measures that ensure that personal data cannot be read, copied, changed or removed without authorization during electronic transfers or transportation and that allow the recipients of personal data through data transfer facilities to be reviewed and determined:

- Protocols of incoming and outgoing connections
- Encrypted transfers for automated processes
- In exceptions, processing by email is only made possible on the customer's request; the Contractor will not send separate emails between the application and server
- Local backups are stored in a fire-proof safe, responsibilities for access to the safe are defined and access is severely restricted; the safe room is secured separately
- Backups are transported from and to the safe without detours

2. Entry Controls

Measures that allow whether and by whom personal data has been entered, changed or removed from the DP systems to be subsequently reviewed and determined:

- Protocols of incoming and outgoing data as part of automated processing
- Logging functions of the operating systems are used for administration
- Possibilities for manipulation are extremely limited due to near-real time processing

C. Availability and loading capacity (Art. 32 No. 1 lit. b of the GDPR)

1. Availability Controls

The Contractor uses the following facilities to process personal data in accordance with the order:

Hardware:

- Highly-available server infrastructure at Verizon with Raid
- Highly-available server in-house with Raid

Software:

- Own developments

D. Rapid recoverability (Art. 32 No 1 lit. c of the GDPR)

Measures to protect personal data against destruction or loss:

- Data is secured according to a defined QM system in accordance with ISO 9001
- Local backups are stored in a fire-proof safe, responsibilities for access to the safe are defined and access is severely restricted; the safe room is secured separately
- Systems are generally highly-available and structured redundantly

E. Procedure for regular review, validation and evaluation (Art. 32 No 1 lit. C; Art. 25 No. 1 of the GDPR)

- Audit scheduling and processing of internal and external audits
- Processing of sensitising measures
- Arrangement of measures
- Reporting
- Risk management and analysis
- Process for handling of protection of privacy events
- Protection of privacy friendly presets

Annex 2: Approved subcontractors

Hereafter the list of subcontractors who render services for the contractor:

Name	**Field of operation**	**Place of business**
Verizon Deutschland GmbH	Data center services	Sebrathweg 20 44149 Dortmund
Telekom Deutschland GmbH	BusinessMail X.400 EDI communication	Landgrabenweg 151 53227 Bonn