# General Terms and Conditions Data Protection for Order Processing

the

**stratEDI Gesellschaft für Kommunikationskonzepte und -lösungen mbH**
Lusebrink 9
58285 Gevelsberg

- hereinafter referred to as **"Contractor"** -

- hereinafter jointly referred to as the **"Parties"** - the contractual partner and the contractor

## PREAMBLE

These terms and conditions describe the parties' obligations regarding data protection. The contractual partner - hereinafter referred to as the Client - wishes to commission the Contractor with the services specified in § 3. Part of the execution of the contract is the processing of personal data. In particular, Art. 28 GDPR places certain requirements on such commissioned processing. In order to comply with these requirements, the parties agree on the following provisions, the fulfilment of which is not remunerated separately, unless this is expressly agreed.

## § 1 DEFINITIONS

**(1)** Pursuant to Art. 4 (7) GDPR, the controller is the body which alone or jointly with other controllers determines the purposes and means of the processing of personal data.

**(2)** Processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller in accordance with Art. 4 (8) GDPR**.**

**(3)** Pursuant to Art. 4 (1) GDPR, personal data means any information relating to an identified or identifiable natural person (hereinafter referred to as "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.

**(4**) Particularly sensitive personal data are personal data pursuant to Art. 9 GDPR, which reveal the racial and ethnic origin, political opinions, religious or philosophical beliefs or trade union membership of data subjects, personal data pursuant to Art. 10 GDPR on criminal convictions and offences or related security measures as well as genetic data pursuant to Art. 4 para. 13 GDPR, biometric data pursuant to Art. 4 para. 14 GDPR, health data pursuant to Art. 4 para. 15 GDPR and data concerning a natural person's sex life or sexual orientation.

**(5)** 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, in accordance with Art. 4 (2) GDPR.

**(6)** Pursuant to Art. 4 (21) GDPR, the supervisory authority is an independent state body established by a Member State pursuant to Art. 51 GDPR**.**

## § 2 INDICATION OF THE COMPETENT DATA PROTECTION SUPERVISORY AUTHORITY

**(1)** The competent supervisory authority for the Contractor is the State Commissioner for Data Protection and Freedom of Information of North Rhine-Westphalia.

**(2)** The client and the contractor and, if applicable, their representatives shall cooperate with the supervisory authority in the fulfilment of their tasks upon request**.**

## § 3 OBJECT OF THE CONTRACT

**(1)** The Contractor shall provide services for the Client in the area of invoicing in electronic format. The basis for this service provision is the main contract.

In doing so, the contractor receives access to personal data and processes it exclusively on behalf of and in accordance with the instructions of the client. The scope and purpose of data processing by the Contractor are set out in the main contract (and the associated service description and the annexes to the main contract). The client is responsible for assessing the permissibility of the data processing.

**(2)** The parties conclude the present agreement in order to concretise the mutual rights and obligations under data protection law. In case of doubt, the provisions of this agreement shall take precedence over the provisions of the main contract.

**(3)** The provisions of this contract shall apply to all activities related to the main contract in which the Contractor and its employees or persons authorised by the Contractor come into contact with personal data originating from the Client or collected for the Client.

**(4)** The term of this contract is based on the term of the main contract, unless the following provisions provide for additional obligations or cancellation rights.

## § 4 RIGHT TO ISSUE INSTRUCTIONS

**(1)** The Contractor may only collect, process or use data within the scope of the main contract and in accordance with the Client's instructions; this applies in particular with regard to the transfer of personal data to a third country or to an international organisation. If the Contractor is obliged by the law of the European Union or the Member States to which it is subject to carry out further processing, it shall inform the Client of these legal requirements prior to processing.

(**2**) The client's instructions are initially set out in this contract and may subsequently be amended, supplemented or replaced by the client in writing by means of individual instructions (individual instructions). The client is authorised to issue corresponding instructions at any time. This includes instructions regarding the correction, deletion and blocking of data. The persons authorised to receive instructions are listed in **Appendix 5**. In the event of a change or long-term absence of the named persons, the Contractor shall immediately name a successor or representative to the Client in text form.

**(3)** All instructions issued must be documented by both the Client and the Contractor. Instructions that go beyond the service agreed in the main contract shall be treated as a request for a change in service.

**(4)** If the Contractor is of the opinion that an instruction from the Client violates data protection regulations, it must inform the Client of this immediately. Until clarification is obtained, the Contractor shall not be obliged to carry out the instruction. The Contractor may refuse to carry out an obviously unlawful instruction.

## § 5 TYPE OF DATA PROCESSED, GROUP OF DATA SUBJECTS

**(1)** As part of the performance of the main contract, the Contractor shall have access to the personal data specified in more detail in **Annex 1**.

**(2**) The group of data subjects affected by the data processing is shown in **Appendix 2.**

## § 6 PROTECTIVE MEASURES OF THE CONTRACTOR

**(1)** The Contractor is obliged to comply with the statutory provisions on data protection and not to disclose the information obtained from the Client's area to third parties or expose it to their access. Documents and data must be secured against unauthorised access, taking into account the state of the art.

**(2)** The Contractor shall design the internal organisation in its area of responsibility in such a way that it meets the special requirements of data protection. It shall take all necessary technical and organisational measures to adequately protect the Client's data in accordance with Art. 32 GDPR, in particular at least the measures listed in **Annex 3** of the

a) Access control

b) Access control

c) Access control

d) Transfer control

e) Input control

f) Order control

g) Availability control

h) Separation control

The contractor reserves the right to change the security measures taken, whereby he shall ensure that the contractually agreed level of protection is not fallen short of.

**(3**) The Contractor's company data protection officer/contact person for data protection is

**Mr Dipl. Inform. Olaf Tenti**

**GDI Gesellschaft für Datenschutz und Informationssicherheit mbH**

**as external data protection officer**

Körnerstr. 45

58095 Hagen

Phone: +49 (0) 2331 / 356832-0

E-mail: datenschutz@gdi-mbh.eu

Internet: http://gdi-mbh.eu/

appointed. The Contractor shall publish the contact details of the data protection officer on its website and notify them to the supervisory authority. The contractor shall provide suitable proof of publication and notification at the request of the client.

**(4**) The persons employed by the Contractor for data processing are prohibited from collecting, processing or using personal data without authorisation. The Contractor shall oblige all persons entrusted by it with the processing and fulfilment of this contract (hereinafter referred to as employees) accordingly (obligation of confidentiality, Art. 28 para. 3 lit. b GDPR) and ensure compliance with this obligation with due care.

## § 7 INFORMATION OBLIGATIONS OF THE CONTRACTOR

**(1**) In the event of disruptions, suspected data protection violations or breaches of contractual obligations of the Contractor, suspected security-related incidents or other irregularities in the processing of personal data by the Contractor, persons employed by the Contractor within the scope of the order or by third parties, the Contractor shall inform the Client immediately in text form. The same applies to audits of the Contractor by the data protection supervisory authority. The notification of a personal data breach shall contain at least the following information:

(a) a description of the nature of the personal data breach, including, where possible, the categories and number of data subjects concerned, the categories and number of personal data records concerned;

(b) a description of the measures taken or proposed to be taken by the contractor to remedy the breach and, where appropriate, measures to mitigate its possible adverse effects.

**(2)** The Contractor shall immediately take the necessary measures to secure the data and to minimise possible adverse consequences for the data subjects and shall inform the Client thereof.

**(3)** In addition, the Contractor shall be obliged to provide the Client with information at any time if the Client's data is affected by a breach in accordance with paragraph 1**.**

**(4)** Should the Client's data be jeopardised by seizure or confiscation, by insolvency or composition proceedings or by other events or measures by third parties, the Contractor shall inform the Client of this immediately, unless it is prohibited from doing so by court or official order. In this context, the Contractor shall immediately inform all competent bodies that the decision-making authority over the data lies exclusively with the Client as the "controller" within the meaning of the GDPR.

**(5)** The Contractor shall inform the Client immediately of any significant changes to the safety measures in accordance with § 6 (2).

**(6)** The client must be informed immediately of any change in the person of the company data protection officer/contact person for data protection.

**(7)** The contractor and, if applicable, its representative shall keep a list of all categories of processing activities carried out on behalf of the client, which shall contain all information pursuant to Art. 30 para. 2 GDPR. The list shall be made available to the client upon request.

(**8**) The Contractor shall co-operate to an appropriate extent in the preparation of the procedure directory by the Client. He shall provide the client with the necessary information in an appropriate manner.

## § 8 CONTROL RIGHTS OF THE CLIENT

**(1)** The Client shall satisfy itself of the Contractor's technical and organisational measures before commencing data processing and then regularly at appropriate intervals. For this purpose, it may, for example, obtain information from the Contractor, have existing certificates from experts, certifications or internal audits presented to it, or personally inspect the Contractor's technical and organisational measures after timely coordination during normal business hours or have them inspected by a competent third party, provided that the latter is not in a competitive relationship with the Contractor. The Client shall only carry out inspections to the extent necessary, at most once a year, and shall not disproportionately disrupt the Contractor's operational processes.

**(2)** The Contractor undertakes to provide the Client with all information and evidence required to carry out a check of the Contractor's technical and organisational measures within a reasonable period of time at the Client's written request.

**(3)** The Client shall document the results of the inspection and inform the Contractor thereof. In the event of errors or irregularities that the client discovers, in particular during the inspection of order results, it must inform the contractor immediately. If facts are discovered during the inspection that require changes to the ordered process flow in order to avoid them in the future, the client shall inform the contractor of the necessary procedural changes without delay.

**(4)** Upon request, the Contractor shall provide the Client with evidence of the obligation of the employees in accordance with Section 6 (4).

## § 9 USE OF SUBCONTRACTORS

**(1)** The Client hereby grants the Contractor general authorisation to involve further processors with regard to the processing of Client data. The other processors involved at the time of the conclusion of the contract are listed in **Annex 4** and, if applicable, in the main contract. In general, contractual relationships with service providers that involve the testing or maintenance of data processing procedures or systems by other bodies or other ancillary services are not subject to authorisation, even if access to Client Data cannot be ruled out, as long as the Contractor makes appropriate arrangements to protect the confidentiality of Client Data.

**(2)** The Contractor shall inform the Client of any intended changes with regard to the involvement or replacement of additional processors. In individual cases, the Client shall have the right to object to the commissioning of a potential additional processor. An objection may only be raised by the client for good cause to be proven to the contractor. If the client does not raise an objection within 14 days of receipt of the notification, its right of objection to the corresponding commissioning shall lapse. If the Client raises an objection, the Contractor shall be entitled to terminate the main contract and this contract with one month's notice.

**(3)** The contract between the Contractor and the additional processor must impose the same obligations on the additional processor as are imposed on the Contractor under this contract. The parties agree that this requirement is fulfilled if the contract has a level of protection corresponding to this contract or if the obligations set out in Art. 28 (3) GDPR are imposed on the additional processor.

**(4)** Subject to compliance with the requirements of this Agreement, the provisions in this Section 9 shall also apply if another processor in a third country is involved. If an additional processor in a third country is involved, the Contractor shall ensure that an adequate level of data protection is guaranteed with the respective additional processor (e.g. by concluding an agreement based on the applicable EU standard data protection clauses). The Client hereby authorises the Contractor, on behalf of the Client, to conclude such an agreement with another processor, including the EU standard data protection clauses for the transfer of personal data to processors in third countries in their respective valid form. Upon request, the Contractor shall provide the Client with evidence of the conclusion of the aforementioned agreements with its other processors. Insofar as the consent of the data subject pursuant to Art. 49 GDPR is required for certain transfer processes to third countries, the Client agrees to cooperate to the extent necessary in the fulfilment of the requirements of Art. 49 GDPR.

## § 10 ENQUIRIES AND RIGHTS OF DATA SUBJECTS

**(1)** The Contractor shall support the Client as far as possible with suitable technical and organisational measures in fulfilling its obligations under Art. 12 to 23 and 32 to 36 GDPR.

**(2)** If a data subject asserts rights, such as the right to information, correction or deletion of their data, directly against the contractor, the contractor shall not react independently but shall immediately refer the data subject to the client and await the client's instructions.

## § 11 LIABILITY

**(1**) In the external relationship, the client alone shall be responsible to the data subject for compensation for damages suffered by a data subject due to unauthorised or incorrect data processing or use within the scope of commissioned processing in accordance with data protection laws.

**(2)** The parties shall release each other from liability if one party proves that it is not responsible in any respect for the circumstance that caused the damage to an affected party.

## § 12 TERMINATION OF THE MAIN CONTRACT

**(1)** The Contractor shall return to the Client all documents, data and data carriers originating from the commissioned processing after termination of the main contract or at any time at the Client's request or - at the Client's request, unless there is an obligation to store the personal data under Union law or the law of the Federal Republic of Germany - delete or destroy them. This also applies to any data backups at the contractor. If there is an obligation to store data as described in the first sentence, all documents, data and data carriers that originate from the commissioned processing and are subject to the obligation must be returned, deleted or destroyed as soon as this obligation ceases to apply. The Contractor shall provide documented proof of the proper deletion of any data that still exists.

**(2)** The client has the right to check the complete and contractually compliant return or deletion of the data at the contractor in a suitable manner.

**(3)** As long as all personal data that was processed on behalf of the Client and was still in the possession of the Contractor after the cancellation of the main contract has not been deleted or destroyed by the Contractor or returned to the Client, this supplementary contract shall be deemed to continue, even after the cancellation of the main contract - for whatever legal reason. If the aforementioned condition is cancelled, the supplementary contract shall end without the need for a separate declaration by one of the parties.

## § 13 FINAL PROVISIONS

**(1)** The parties agree that the defence of the right of retention by the Contractor within the meaning of § 273 BGB with regard to the data to be processed and the associated data carriers is excluded.

**(2)** Amendments and supplements to this agreement must be made in writing. This also applies to the waiver of this formal requirement. The precedence of individual contractual agreements remains unaffected by this.

**(3)** Should individual provisions of this agreement be or become invalid or unenforceable in whole or in part, this shall not affect the validity of the remaining provisions.

**(4)** This agreement is subject to German law. The exclusive place of jurisdiction is Gevelsberg.

The following **PLANT** is the subject of the contract:

| | | |
|---|---|---|
| **ANNEX 1** | - | Type of data, type and purpose of data processing |
| **ANNEX 2** | - | Categories of data subjects |
| **ANNEX 3** | | - Technical and organisational measures of the contractor |
| **ANNEX 4** | - | Authorised subcontractors |
| **ANNEX 5** | - | Persons authorised to issue instructions |

## APPENDIX 1 - Type of data, type and purpose of data processing

| Type of data | Nature and purpose of data processing |
|---|---|
| • First name<br>• Surname<br>• address<br>• Tax number or VAT identification number<br>• Date of issue of the invoice<br>• Invoice number<br>• customary designation of the delivered goods or handling and type of other services<br>• Time of delivery or other service provision<br>• Date of receipt of the consideration or part of the consideration, if applicable<br>• remuneration broken down according to tax rates<br>• Applicable tax rate<br>• Tax amount attributable to the consideration | Receiving and issuing an invoice in electronic format within the meaning of Section 14 para. 1 sentence 2, para. 4 UStG (new version); transmission of the invoice to the client's customer |

**APPENDIX 2 - Categories of data subjects**

| **Categories of affected persons** |
|---|
| Customers of the client |

**ANNEX 3 - Technical and organisational measures (TOM) in accordance with Art. 32 GDPR**

The General Data Protection Regulation (GDPR) requires organisations or companies that collect, process or use personal data themselves or on their behalf to provide a level of protection appropriate to the risk to the rights and freedoms of natural persons.

The technical and organisational measures to ensure data protection and data security are defined below. The aim is to guarantee in particular the **confidentiality, integrity, resilience and availability** of the personal data processed on our behalf.

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

*Confidentiality within the meaning of Art. 32 para. 1 lit. b in conjunction with recitals. 39 and 83 GDPR is sufficiently guaranteed if unauthorised persons have no access to the data and cannot use the data or the devices with which it is processed and the data is also protected against unauthorised or unlawful processing and against accidental loss in accordance with Art. 5 para. 1 lit. f GDPR.*

### 1. access control:

*Measures to prevent unauthorised persons from gaining access to the data processing systems used to process personal data:*

In the Verizon data centre, the following measures in particular should be highlighted:

- Prior registration with prior order creation is required to enter the facility
- Only a defined group of people has access
- Several factors are used for authentication

Access control to the offices is particularly important:

- The building is secured by an alarm system
- There is a locking system with defined responsibilities and a tracking system for issuing and returning keys. If a key is lost, the locking system is replaced; keys are only reordered after separate authentication and authorisation
- People from outside the company (including tradesmen) are collected from the company's central reception and accompanied inside the company
- It is not possible for visitors to gain access to the rooms due to the locked areas of the company and the locked floors
- Responsibilities are defined for backup storage and access is severely restricted; the safe storage room for the backups is secured separately

### 2. access control

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

- Access control for the servers is subject to Verizon's specifications
- The contractor has a multi-level authorisation system for server administration
- Password guidelines exist for all passwords

### 3. access control

*Measures to ensure that those authorised to use the data processing procedures can only access the personal data subject to their access authorisation:*

- It is ensured that only persons from the EDI processing area have access to the
  Access the server infrastructure

- The different authorisation areas are separated by the assignment of different passwords

### 4. separation control

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

- The separation control is based on addressing according to customer specifications

## B. Integrity (Art. 32 para. 1 lit. b GDPR)

*Integrity within the meaning of Art. 32 para. 1 lit. b in conjunction with Art. 5 para. 1 lit. f GDPR is guaranteed if data is protected against accidental loss, accidental destruction or accidental damage, i.e. the data is complete, unchanged and intact.*

### 1. transfer control

*No unauthorised reading, copying, modification or removal during electronic transmission or transport*

- Incoming and outgoing connections are logged
- Transmission in automated procedures is encrypted

- In exceptional cases, processing by e-mail is only possible at the special request of the customer; no separate transmission of e-mails between the application and the server takes place on the part of the contractor
- Local backups are stored in the fireproof safe, responsibilities for accessing them are defined and access is severely restricted; the safe room is secured separately
- Transport of the backup to and from the safe without detours

**2. input control**

*Measures that ensure that it is possible to subsequently check and determine whether and by whom personal data has been entered, changed or removed from IT systems:*

- Incoming and outgoing data is logged as part of automated processing
- The logging functions of the operating systems are used for administration
- Due to the almost real-time processing, the manipulation options are very limited

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

*Availability within the meaning of Art. 32 para. 1 lit. b GDPR is guaranteed if the data can be used at any time in accordance with its purpose. In addition, in accordance with Art. 32 para. 1 lit. c GDPR, the ability to quickly restore availability and access to the data in the event of a physical or technical incident must exist.*

*Resilience must be ensured on a permanent basis in accordance with Art. 32 para. 1 lit. b GDPR and concerns systems and services in connection with the processing of personal data.*

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

1. hardware:

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

2. software:

- In-house development

## D. Rapid recoverability (Art. 32 para. 1 lit. c)

- Data is backed up locally and decentralised on a NAS system.
- the virtual systems are backed up in a data centre in Dortmund.
- In general, the systems are highly available and redundant

## E. Procedure for regular review, assessment and evaluation (Art. 32 para. 1 lit. d, Art. 25 para. 1, para. 2 GDPR)

*(e.g. data protection management system (DSMS), audit planning and implementation of internal and external audits, implementation of awareness-raising measures, action planning, reporting, risk management and analysis, process for handling data protection incidents, data protection-friendly default settings)*

- Audit planning and implementation of internal and external audits
- Implementation of sensitisation measures
- Action planning
- Reporting and reporting
- Risk management and analysis
- Process for handling data protection incidents
- Privacy-friendly default settings

### APPENDIX 4 - Authorised subcontractors

*The contractor has commissioned the following subcontractors with further services in connection with which personal data is processed:*

| Company | address | Order content |
|---|---|---|
| | | |
| Verizon Germany GmbH | Data centre services | Sebrathweg 20,<br>44149 Dortmund |
| Telekom Deutschland GmbH | BusinessMail X.400<br>EDI communication | Landgrabenweg 151,<br>53227 Bonn |
| | | |

## ANNEX 5 - Instruction recipient at the contractor

| Name | Contact details | Position |
|---|---|---|
| Dr Thorsten Georg | *info@stratedi.de* | Managing Director |
| Mr Marvin Karl | *Info@stratedi.de* | Managing Director |
| Mr Andreas Weng | *edi-support@stratedi.de* | EDI Project Manager |