Data Processing Agreement for SSI SCHAEFER Group companies

Last update: December 2021

This Data Processing Agreement ("**DPA**") specifies the data protection rights and obligations of the parties with regard to the processing of personal data within the framework of the main contract concluded between the parties, which refers to this agreement ("**main contract**"), by the legal entity of the SSI SCHAEFER Group concluding the main contract (hereinafter "**Contractor**") for the customer (hereinafter "**Customer**").

1. Scope of application

By providing the services in accordance with the main contract, the Contractor processes personal data provided by the Customer for the performance of the agreed services and for which the Customer acts as controller in the legal sense of the data protection regulation ("**Customer data**"). In case of discrepancies between this DPA and regulations from other agreements, in particular from the main contract, the regulations defined in this DPA have priority.

2. Subject and scope of the processing/instruction authority of the Customer

2.1 The Contractor will process the Customer data exclusively on behalf of the Customer and in accordance with the instructions of the Customer, provided that the Contractor is not obliged to process the data by law of the European Union or a Member State thereof. In such case, the Contractor informs the Customer about these legal requirements prior to processing, unless the respective law prohibits such information for reasons of important public interest.

Unless agreed otherwise in the main contract or in writing during the project, processing of Customer data is exclusively carried out by the Contractor in the defined nature and scope, as well as for the defined purpose and means specified in **Annex 1**, and only concerns the specified types of personal data and categories of data subjects.

2.2 The duration of the processing corresponds to the term of the main contract.

2.3 Instructions result from the main contract. The Customer is entitled to give further instructions concerning the nature, scope, purpose and means of the processing of Customer data. Instructions should be given in written form. Oral instructions are confirmed by the Customer in writing or via e-mail.

2.4 If the Customer gives instructions exceeding the services agreed upon in the main contract or in this DPA, the Customer bears the costs for the execution of instructions. The Contractor will inform the Customer about the expected costs prior to the execution of the instructions and will wait until the Customer confirms the costs. This does not apply to instructions to refrain from processing data as a whole or to erase individual or all Customer data, or to hand them over to the Customer.

2.5 If the Contractor is of the opinion that an instruction of the Customer contradicts this DPA, the GDPR or other data protection provisions of the Union or of the Member States, it will immediately inform the Customer of this in writing. The Contractor is entitled to refrain from the execution of such an instruction, until the Customer confirms the instruction in writing. If the Customer insists on the execution of an instruction despite the concerns expressed by the Contractor, the Customer indemnifies the Contractor from all damages and costs caused by executing the Customer's instruction. The Contractor will inform the Customer of any damages asserted against it and of any costs incurring to it and will not acknowledge claims of third parties without the Customer's consent and will, by the choice of the Contractor, conduct the defense in agreement with the Customer or leave it to the Customer.

3. Personnel requirements

3.1 The Contractor must oblige all persons, who process Customer data, to commit themselves to confidentiality, unless they are subject to an appropriate statutory obligation of confidentiality.

3.2 The Contractor ensures that persons subordinate to it, who have access to Customer data, only process these data according to this DPA and according to the instructions of the Customer; unless they are obliged to processing by the law of the European Union or of the Member States.

4. Sub-processors

4.1 For the processing of Customer data, the Contractor uses, unless otherwise agreed in the main contract, the sub-processors listed in **Annex 2**. They are considered approved upon conclusion of the DPA. The Contractor is also entitled to use all other affiliated enterprises of the SSI SCHAEFER Group in accordance with § 15 *deutsches AktG* (German Stock Corporation Act) as sub-processors.

4.2 The Contractor is entitled to make use of sub-processors for processing Customer data, subject to the following: The Contractor informs the Customer in writing before engaging a sub-processor. Provided that the Customer does not object within 14 days, the claim is considered approved.

4.3 If the Customer objects to the use of a sub-processor without valid reason, the Contractor is entitled, at its choice, to continue its services without the respective sub-processor or to terminate the main contract as well as this DPA in accordance with the terms of the main contract.

4.4 The Contractor must oblige every sub-processor in the same way as the Contractor is obliged to the Customer due to this DPA.

4.5 The Contractor is obliged to only choose and make use of sub-processors who sufficiently guarantee that the appropriate technical and organizational measures will be implemented in a way that allows the processing of Customer data to be carried out in accordance with the requirements of the GDPR and this DPA. Upon request, the Contractor will provide the Customer with proof on the compliance with the requirements of the GDPR and this DPA by sub-processors.

4.6 Subject to the compliance with the provisions of this DPA, the Contractor is also entitled to process Customer data outside the European Economic Area ("**EEA**") or to have Customer data processed by sub-processors in accordance with section 4 of this DPA, if the requirements of Art. 44 to 48 of the GDPR are met or if there is an exception in accordance with Art. 49 of the GDPR.

4.7 If the Contractor uses sub-processors, who process personal data outside Member States of the European Union or the EEA, and unless the requirements in Art. 44 to 48 of the GDPR are met in any way or there is an exception in accordance with Art. 49 GDPR, the Contractor will agree the Standard Contractual Clauses (Module 3) listed under https://www.ssi-schaefer.com/en-de/data-processing-agreements in their latest version with these sub-processors as data exporter.

5. Security of processing

5.1 The Contractor implements appropriate technical and organizational measures required to ensure a level of security appropriate to the risk for the Customer data, taking into account the state of the art, the costs of implementation and – as far as known to the Contractor – the nature, scope, context and purposes of processing the Customer data as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects.

5.2 The Contractor must implement the technical and organizational measures, in particular those listed in **Annex 3** of this DPA, prior to the processing of Customer data and maintain them for the duration of the main contract and ensure that the processing of Customer data is carried out in accordance with these measures.

5.3 As the technical and organizational measures are subject to technical progress, the Contractor is entitled and obliged to implement the technical and organizational measures listed in Annex 3 adequately and by taking into consideration the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects to ensure the security of processing.

5.4 It is the responsibility of the Customer to examine the technical and organizational measures implemented by the Contractor, in particular whether these measures are sufficient with regard to the context of the data processing, unknown to the Contractor.

6. Rights of data subjects

6.1 The Contractor will implement all reasonable technical and organizational measures to assist the Customer in the fulfillment of its obligation to respond to requests for exercising the data subject's rights.

6.2 In particular, the Contractor will within the scope of its possibilities:

a) inform the Customer if a data subject directly contacts the Contractor with a request to exercise the data subject's rights with regard to Customer data;

b) provide the Customer with information on processing of Customer data upon request, which the Customer needs in order to answer the request of a data subject and which are not in the possession of the Customer itself;

c) promptly rectify, erase or limit the processing of Customer data upon instruction of the Customer, provided that the Customer cannot do this on its own and provided that this is technically feasible for the Contractor;

d) support the Customer, as far as necessary, to obtain the Customer data processed within the scope of the Contractor's responsibility – insofar as this is technically feasible for the Contractor – in a structured, commonly used and machine-readable format in case that a data subject exercises the right of Customer data portability.

7. Other support obligations of the Contractor

7.1 The Contractor reports any Customer data breach to the Customer, immediately after it was informed of such, in particular events that have led to, and with a sufficient degree of probability, will lead to destruction, loss, alteration or unauthorized disclosure of and unauthorized access to Customer data.

7.2 In case of any Customer data breach, the Contractor is obliged to promptly take any required and commercially reasonable measures to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

7.3 If the Customer is obliged to inform a public authority or a person about the processing of Customer data or to cooperate with them in any other way, the Contractor is obliged within the scope of its possibilities to support the Customer in providing this information and in fulfilling other obligations for cooperation.

7.4 In the event that the Customer is obliged to inform the supervisory authority and/or data subjects in accordance with Art. 33, 34 of the GDPR, the Contractor will support the Customer upon the Customer's request and within the scope of its possibilities to fulfill these obligations. The Contractor is particularly obliged to document any Customer data breaches including all facts relating to this Customer data breach in a way that enables the Customer to prove compliance with any relevant statutory notification obligation.

7.5 The Contractor will support the Customer with information available to it and within reason in possible data protection impact assessments to be carried out by it and, if necessary, in subsequent consultations with the supervisory authorities in accordance with Art. 35, 36 of the GDPR.

7.6 The Contractor will support the controller, taking into account the information available to it, in complying with the obligations stated in Art. 32 of the GDPR.

8. Erasure and return of data

8.1 At the instruction of the Customer, the Contractor will, upon termination of the main contract, completely erase all Customer data or return them to the Customer, unless the Contractor is obliged by law of the European Union or a Member State to continue storing Customer data.

8.2 However, the Contractor is entitled to keep safety copies of the Customer data for a period of 60 days, provided that the erasure of Customer data from these safety copies is not required for technical reasons or Art. 32 of the GDPR. During this period, the rights and obligations of the parties from this DPA with regard to the safety copies continue to apply, by way of derogation from clause 2.2.

8.3 Documentation used for proof of the orderly and proper processing of the Customer data must be kept by the Contractor in accordance with the statutory retention periods beyond the contract termination of this DPA.

9. Proof and inspections

9.1 The Contractor must ensure and check on a regular basis that the processing of Customer data complies with this DPA, the main contract as well as the Customer's instructions.

9.2 The Contractor will appropriately document the implementation of the obligations according to this DPA and will provide the Customer with all necessary proof showing the Contractor's compliance with the obligations stated in the GDPR and this DPA upon request of the Customer.

9.3 The Customer is entitled to review the Contractor prior to the start of the processing of Customer data and regularly during the term of the main contract regarding the compliance with regulations of this DPA, in particular the implementation of suitable technical and organizational measures, either by itself or by a qualified auditor obliged to confidentiality; this includes inspections. The Contractor enables such reviews and contributes to such reviews by taking all appropriate and reasonable measures, in particular by granting the necessary access rights and by providing all relevant information. The costs for these reviews and inspections are borne by the Customer.

9.4 The reviews and inspections should not, if possible, impede the Contractor in its normal business operations and should not impose an undue burden on it. In particular, inspections at the Contractor's site without concrete reason should not be carried out more than once per calendar year and only during the normal operating hours of the Contractor. The Customer must inform the Contractor about inspections in due time in advance and in writing.

9.5 In accordance with the provisions of the GDPR, the Customer and the Contractor are subject to public controls by the competent supervisory authority. Upon request by the Customer, the Contractor will provide the supervisory authority with the required information and will grant the supervisory authority the opportunity for reviews, this includes inspections at the Contractor's site by the supervisory authority or by persons assigned by the supervisory authority. Within this context, the Contractor grants the competent supervisory authority the necessary rights of access, information and inspection.

10. Liability

The limitations of liability agreed in the main contract apply accordingly.

11. Other

11.1 Amendments and subsidiary agreements to this DPA must be made in writing. The same applies to this clause.

11.2 Provided that this contract stipulates the written form, communication via e-mail is sufficient to meet the written form requirement.

11.3 Choice of law and place of jurisdiction for this DPA are determined in accordance with the main contract.

Annex 1 – Purpose, nature and scope of the data processing, type of data and group of data subjects

Purpose of the data processing	Planning, delivery, installation, commissioning or extension of an intralogistics system or intralogistics software Services regarding the operation or the extension of an intralogistics system or intralogistics software
Nature and scope of the data processing	Access to data stored in the customer system for the implementation and integration of software and customer IT systems on site or via remote access. Access to data stored in the customer system to render services (bug fixing, updates, monitoring of hardware, operating system, data base and application). Creation of (database)analyses and reports for the Customer made from data stored in customer systems. Hosting of data is carried out in the IT landscape of the customer.
Type of data	• Name • Contact details (address, e-mail, phone) • Sex • Payment information (e.g. bank account details, credit card number) • Date and place of birth • Job details • Order data • Other data stored in the system by the Customer
Group of data subjects	• Employees of the Customer • Customers of the Customer • Contract partners of the Customer (in particular suppliers, service providers or sub-companies) • Contract partners and communication partners of the Customer's customers

Annex 2 – Sub-processors

Particularly, the following legal entities of the SSI SCHAEFER Group can act as sub-processors, unless one of the legal entities listed below is already contractual partner, and as such, processor in accordance with this Agreement:

Name	Address
Fritz Schäfer GmbH & Co KG	Fritz-Schäfer-Straße 20, 57290, Neunkirchen/Siegerland, Germany
Fritz Schäfer GmbH	Fritz-Schäfer-Straße 20, 57290, Neunkirchen/Siegerland, Germany
SSI Schäfer Automation GmbH AT	Fischeraustraße 27, 8051 Graz, Austria
SSI Schäfer Automation GmbH DE	i_Park Klingholz 6, 97232 Giebelstadt, Germany
SSI Schäfer IT Solutions GmbH AT	Friesachstraße 15, 8114 Friesach bei Graz, Austria
SSI Schäfer IT Solutions GmbH DE	i_Park Klingholz 18/19, 97232 Giebelstadt, Germany
SSI Schäfer SRL	B-dul Industriei nr. 6, 300714 Timisoara, Romania
SSI Schäfer Sistemas Internacional, S.L.	C/Can Pi No 17, Pol. Ind. Gran Vía Sur, Antigua Ctra del Prat 17, 08908 L'Hospitalet de Llobregat, Bcn, Spain
SSI Schäfer A/S	Ved Stranden 1, 9560 Hadsund, Denmark

Annex 3 – Technical and organizational measures

1. The processor ensures appropriate technical and organizational measures, based on the state of the art, the costs of implementation and the precise risks, which are suitable to ensure an appropriate level of protection for the rights of the data subject.

2. State of the art refers to advanced processes, infrastructure and operating modes, which, according to the prevailing opinion of leading experts, seem to ensure the achievement of the defined statutory goal in data protection. Processes, infrastructure and operating modes or comparable procedures, infrastructure and operating modes must have proven their worth in practice or – if this is not already the case – should have been tested successfully at the company.

3. The following measures are taken in particular:

3.1 Confidentiality (Art. 32 (1)(a) and (b) GDPR)

3.1.1 Entrance control

Access to facilities where personal data is processed is prohibited for unauthorized persons.

3.1.2 User control

The use of automated data processing systems via facilities for data transfer (e.g. via remote access) by unauthorized persons is prevented.

3.1.3 Access control

The access of authorized persons is limited to the personal data required for the fulfillment of their tasks.

Facilities for data transfer are checked and it is determined, to whom personal data was transferred or provided or to whom personal data can be transferred and provided. Data recipients, to whom personal data is enclosed via facilities for data transfer (e.g. via remote access) can be identified.

3.1.4 Separation control

By different departments with various tasks and authorizations.

3.1.5 Pseudonymization

The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.

3.2 Integrity (Art. 32 (1)(b) and (c) GDPR)

3.2.1 Transfer control

When disclosing personal data and transporting data carriers, it is prevented that data can be read, copied, modified or removed without authorization.

3.2.2 Input control

Unauthorized storing as well as unauthorized inspection, modification or erasure of stored, personal data is prevented accordingly.

In automated systems it can be subsequently checked which personal data were entered when and by whom (protocol data).

It is ensured that, depending on the protection needs, all functions of the system are available (availability, resilience), occurring malfunctions are reported (reliability) and stored personal data cannot be damaged or disclosed through malfunctions of the system (integrity, confidentiality).

3.3 Availability (Art. 32 (1)(c) GDPR)

3.3.1 Availability control

Unauthorized persons are prevented from reading, copying, modifying or removing data carriers.

3.3.2 Recoverability

Depending on the protection needs, it is ensured that the applied systems can be restored as fast as possible and without delay in case of malfunctions → various backups.

3.4 Process for regular testing (Art. 32 (1)(d) DSGVO)

3.4.1 Order control

Measures are taken to ensure timely recognition and transparency of unauthorized access and unauthorized disclosure of personal data as well as of any events that may lead to a breach of personal data.

4. As a result, the processor provides sufficient guarantees that appropriate technical and organizational measures are implemented in a way that all requirements of data protection and data security are met and thus ensure a suitable level of protection for the rights of the data subject.