

Standard Contractual Clauses

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Data exporter is the “Auftraggeber” according to this agreement.

And

The according data importer with whom these SCCs will be agreed upon.

each a ‘party’; together ‘the parties’.

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

1. Definitions

For the purposes of the Clauses:

- 1.1.1 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- 1.1.2 'the data exporter' means the controller who transfers the personal data;
- 1.1.3 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- 1.1.4 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- 1.1.5 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- 1.1.6 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3. Third-party beneficiary clause

- 3.1 The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
- 3.2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the

entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

- 3.3 The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
- 3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Obligations of the data exporter

The data exporter agrees and warrants:

- 4.1.1 that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- 4.1.2 that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- 4.1.3 that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- 4.1.4 that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- 4.1.5 that it will ensure compliance with the security measures;
- 4.1.6 that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

- 4.1.7 to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- 4.1.8 to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- 4.1.9 that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- 4.1.10 that it will ensure compliance with Clause 4(a) to (i).

5. Obligations of the data importer

The data importer agrees and warrants:

- 5.1.1 to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- 5.1.2 that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- 5.1.3 that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- 5.1.4 that it will promptly notify the data exporter about:
 - 5.1.4.1 any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
 - 5.1.4.2 any accidental or unauthorised access; and
 - 5.1.4.3 any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

- 5.1.5 to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- 5.1.6 the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- 5.1.7 to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- 5.1.8 that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- 5.1.9 that the processing services by the sub-processor will be carried out in accordance with Clause 11;
- 5.1.10 send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6. Liability

- 6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
- 6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

- 6.3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

7.1.1 to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

7.1.2 to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Cooperation with supervisory authorities

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

9. Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely Germany.

10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

11. Sub-processing

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

- 11.2 The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
- 11.3 The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely Germany.
- 11.4 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data-processing services

- 12.1 The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
- 12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order
for the contract to be binding
(if any):

Stamp:

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for
the contract to be binding (if
any):

Stamp:

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

The data exporter is the Customer, who uses the services defined in the DPA and the main contract.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

The data importer is planning, delivering, installing, commissioning or extend an intralogistics system or intralogistics software.

The data importer also provides services regarding the operation or the extension of an intralogistics system or intralogistics software

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

- 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

Categories of data

The personal data transferred concern the following categories of data (please specify):

- 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

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

- Special categories of data which are stored in the system by the Customer

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

- 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.

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

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.

Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

- 1.1.1 the data exporter promptly notifying the data importer of a claim; and
- 1.1.2 the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim.