# Data Processing and Transfer Agreements to comply with the General Data Protection Regulation (GDPR), UK Data Protection Law (United Kingdom), FDPA (Switzerland), CCPA/CPRA (California), PDPL (UAE), PIPL (China) and other data protection laws, and Confidentiality of Trade Secrets

The Data Processing and Transfer Agreements contained herein shall automatically become essential part to any contractual arrangement or agreement (in the following "Main-Agreement" or similar) that is concluded between our company (in the following "Provider", "Exporter", "Business", "Personal Information Handler", "Us", "Our" or similar), as specified in the imprint of this or one of our website(s) or email(s) and/or in the Main-Agreement, and your company (in the following "Business Partner" "Contractor", „Overseas Recipient", "Vendor", "Client", "Importer", "You" or mentioned with a similar term) as specified in the Main-Agreement, or in case the Main-Agreement is concluded verbally, by implicit acts or otherwise, the natural or legal person, agency or other body that is our contractual partner, but only in case processing or transfer of personal data (in the following "Data") is part of or essential to the Main-Agreement and if data subjects that are subject to processing are based in a country that we implemented agreements for in this Set of Agreements, or otherwise protected under the respective laws and if trade and business secrets are processed or exchanged between you and us.

Based on the individual business relationship between you and us, if you agree to or are notified of this Set of Agreements, which may be by email or by means of a link, or if it is incorporated into the Main-Agreement, the following shall automatically apply (1) the "EU Standard Contractual Clauses 2021/915 BETWEEN CONTROLLERS AND PROCESSORS" if a processing relationship exists or is to be established between the parties and both parties are located within the European Union or the EEA, and/or (2) the "EU Standard Contractual Clauses 2021/914 MODULE ONE: Transfer Controller to Controller" if one of the parties is established outside the European Union or the EEA and receives Data as a Controller from the other party, and the other party is also a Controller and is established in the European Union or the EEA, or Data of Data Subjects from the European Union or the EEA are transferred, and/or (3) the "EU Standard Contractual Clauses 2021/914 MODULE TWO: Transfer Controller to Processor" if the Processor is established outside the European Union or the EEA and Data is transferred by the other party as a Controller which is established in the European Union or the EEA, or Data of Data Subjects from the European Union or


© All rights reserved by Heiko Maniero.

the EEA are transferred, and/or (4) the "EU Standard Contractual Clauses 2021/914 MODULE THREE: Transfer Processor to Processor" if the Data Transferer acts as a Processor for another Controller or a Processor from the European Union or the EEA, and transfers Data to the other party as another Processor, or Data of Data Subjects from the European Union or the EEA are transferred, and/or (5) the "EU Standard Contractual Clauses 2021/914 MODULE FOUR: Transfer Processor to Controller" if the Data Transferer acts as a Processor for another Controller or a Processor from the European Union or the EEA, and transfers Data to the other party as a Controller outside the European Union or the EEA, or Data of Data Subjects from the European Union or the EEA are transferred, and/or (6) the "International Data Transfer Agreement (United Kingdom)" if the Data Transferer is based in the United Kingdom and transfers Data to the other party outside the United Kingdom, or Data of Data Subjects from the United Kingdom are transferred, and/or (7) the "International Data Transfer Addendum to the European Commission's Standard Contractual Clauses for International Data Transfers (United Kingdom)", if the Data Transferer is based in the United Kingdom and transfers Data to the other party outside the United Kingdom, and the EU Standard Contractual Clauses have already been concluded without using this Set of Agreements, and/or (8) the "Data Processing Agreement for the United Kingdom", if a processing relationship exists or is to be established between the parties and both parties are located within the United Kingdom, and/or (9) the "CCPA-CPRA CONTRACTOR AGREEMENT" if Consumer Data from California, or Data previously transferred to California, is being (back)transferred, and/or (10) the "Confidentiality and Data Protection Agreement for Vendors" if your company is a vendor but not a Processor of our company, and/or (11) based on separately executed declarations of intent by both parties, the "Confidentiality and Data Protection Agreement for Customers" if your company is a customer of ours, and no Standard Contractual Clauses or other agreement contained in this Set of Agreements is applicable to our business relationship, and/or (12) the "Data Processing Agreement, Joint Controllership Agreement and Cross-Border Personal Data Transfer and Sharing Agreement for the United Arab Emirates", if Data from the United Arab Emirates, or Data previously transferred to the United Arab Emirates, is being (back)transferred, and/or (13) the "Standard Contract for Outbound Cross-border Transfer of Personal Information (People's Republic of China) (Contract Language: Chinese)", if Personal Information is transferred from the People's Republic of China to an Overseas Recipient, or Personal Information of Personal Information Subjects from the People's Republic of China are transferred, and/or (14) the "Data Processing Agreement and National Joint Controllership Agreement to


© All rights reserved by Heiko Maniero.

comply with PIPL (People's Republic of China) (Contract Language: Chinese)", if a processing relationship exists or is to be established between the parties and both parties are located within the People's Republic of China.

The following contracts and appendixes are included in this Set of Agreements:

**APPENDIX 1 – SCCs 2021/915 BETWEEN CONTROLLERS AND PROCESSORS**

**APPENDIX 2 – SCCs 2021/914 MODULE ONE: Transfer Controller to Controller**

**APPENDIX 3 – SCCs 2021/914 MODULE TWO: Transfer Controller to Processor**

**APPENDIX 4 – SCCs 2021/914 MODULE THREE: Transfer Processor to Processor**

**APPENDIX 5 – SCCs 2021/914 MODULE FOUR: Transfer Processor to Controller**

**APPENDIX 6 – SUB-PROCESSORS**

**APPENDIX 7 – LIST OF PARTIES**

**APPENDIX 8 – DESCRIPTION OF THE PROCESSING OR THE TRANSFER**

**APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES**

**APPENDIX 10 – COMPETENT SUPERVISORY AUTHORITY**

**APPENDIX 11 – Confidentiality and Data Protection Agreement for Vendors**

**APPENDIX 12 – Confidentiality and Data Protection Agreement for Customers**

**APPENDIX 13 – International Data Transfer Agreement (United Kingdom)**

**APPENDIX 14 – International Data Transfer Addendum to the European Commission's Standard Contractual Clauses for International Data Transfers (United Kingdom)**

**APPENDIX 15 – Data Processing Agreement for the United Kingdom**

**APPENDIX 16 – CCPA-CPRA CONTRACTOR AGREEMENT**

**APPENDIX 17 – Data Processing Agreement, Joint Controllership Agreement and Cross-Border Personal Data Transfer and Sharing Agreement for the United Arab Emirates**

**APPENDIX 18 – Standard Contract for Outbound Cross-border Transfer of Personal Information (People's Republic of China)**

**APPENDIX 19 – Standard Contract for Outbound Cross-border Transfer of Personal Information (People's Republic of China) (Contract Language: Chinese)**

**APPENDIX 20 – Data Processing Agreement and National Joint Controllership Agreement to comply with PIPL (People's Republic of China) (Contract Language: English)**

The applicable Standard Contractual Clauses or Agreements contained herein shall govern the relationship between you and us in regards to the processing of any Personal Data from Data Subjects that are based or resident in countries or regions where the GDPR, UK


© All rights reserved by Heiko Maniero.

Data Protection Law, FDPA, CCPA/CPRA or other laws contained in this Set of Agreements are applicable ("Personal Data Processing"), and shall prevail over any conflicting or inconsistent provisions pertaining to Personal Data Processing in any commitment, obligation, arrangement, contract or agreement between you and us, unless and until the Standard Contractual Clauses or other agreements contained herein are superseded by any new laws or regulations enacted by the competent legislators (collectively, the "New Laws"), wherein such New Laws shall, from the date of their applicability, apply automatically in place of the respective Contractual Clauses to Personal Data Processing between you and us, unless either party notifies the other party in writing of its objection thereto within 30 days from the official publication date of the New Laws.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

# STANDARD CONTRACTUAL CLAUSES 2021/915 BETWEEN CONTROLLERS AND PROCESSORS

## Clause 1

## Purpose and scope

a) The purpose of these Standard Contractual Clauses (the "**Clauses**") is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in **Annex I** have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in **Annex II**.

(d) **Annexes I to IV** are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

## Clause 2

## Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

## Clause 3

## Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.


© All rights reserved by Heiko Maniero.

## Clause 4

## Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

## Clause 5

## Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing **Annex I**.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in **Annex I**.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

## Clause 6

## Description of the processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in **Annex II**.

## Clause 7

## Obligations of the Parties

### 7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

### 7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in **Annex II**, unless it receives further instructions from the controller.

### 7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in **Annex II**.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

### 7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in **Annex III** to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

### 7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

### 7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

### 7.7. Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.


© All rights reserved by Heiko Maniero.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub- processor to fulfill its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

### 7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfill a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with **Clause 7.7.** for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

## Clause 8

## Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to **Clause 8(b)**, the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:


© All rights reserved by Heiko Maniero.

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in **Annex III** the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

## Clause 9

## Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

### 9.1. Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679 shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679 with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

### 9.2. Data breach concerning data processed by the processor


© All rights reserved by Heiko Maniero.

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

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

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in **Annex III** all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

## Clause 10

## Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.


© All rights reserved by Heiko Maniero.

## ANNEX I
## List of parties

**SEE APPENDIX 7**


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## ANNEX II
## Description of the processing

**SEE APPENDIX 8**


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## ANNEX III

**Technical and organisational measures including technical and organisational measures to ensure the security of the data**

**EXPLANATORY NOTE:**

**The technical and organisational measures need to be described concretely and not in a generic manner.**

**Description of the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. Examples of possible measures:**

**SEE APPENDIX 9**


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## ANNEX IV
## List of sub-processors

**EXPLANATORY NOTE:**

**This Annex needs to be completed in case of specific authorisation of sub-processors (Clause 7.7(a), Option 1).**

The controller has authorised the use of the following sub-processors:

**SEE APPENDIX 6**


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

# STANDARD CONTRACTUAL CLAUSES 2021/914
# MODULE ONE: Transfer Controller to Controller

## Clause 1
## Purpose and scope

(a) The purpose of these contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "**entity/ies**") transferring the personal data, as listed in **Annex I.A** (hereinafter each "**data exporter**"), and

ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in **Annex I.A** (hereinafter each "**data importer**") have agreed to these contractual clauses ("**Clauses**").

(c) These Clauses apply with respect to the transfer of personal data as specified in **Annex I.B**.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

## Clause 2
## Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

## Clause 3
## Third-party beneficiaries

(a) The data subjects can enforce against the data exporter and/or data importer these Clauses, with the following exceptions:

 © All rights reserved by Heiko Maniero.

i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

ii) Clause 8.5 (e) and Clause 8.9 (b)

*[iii) not applicable]*

iv) Clause 12 (a) and (d);

v) Clause 13;

vi) Clause 15.1 (c), (d) and (e);

vii) Clause 16 (e);

viii) Clause 18 (a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

**Clause 4**

**Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

**Clause 5**

**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of other related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

**Clause 6**

**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in **Annex I.B** hereunder.

**Clause 7**

**Docking clause**

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing **Annex I.A**.

(b) Once it has completed the Appendix and signed **Annex I.A**, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in **Annex I.A.**

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**Clause 8**


© All rights reserved by Heiko Maniero.

**Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

### 8.1. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in **Annex I. B**. It may only process the personal data for another purpose:

i) where it has obtained the data subject's prior consent;

ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

### 8.2. Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to **Clause 10**, the data importer shall inform them, either directly or through the data exporter:

i) of its identity and contact details;

ii) of the categories of personal data processed;

iii) of the right to obtain a copy of these Clauses;

iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to **Clause 8.7**.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

### 8.3. Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

### 8.4. Storage limitation


© All rights reserved by Heiko Maniero.

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

### 8.5. Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in **Annex II.** The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to **Clause 13**. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

### 8.6. Sensitive data


© All rights reserved by Heiko Maniero.

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

### 8.7. Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### 8.8. Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

### 8.9. Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.


© All rights reserved by Heiko Maniero.

***[Clause 9 not applicable]***

**Clause 10**

**Data subject rights**

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in **Annex I**; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to **Clause 8.7**; and provide information on the right to lodge a complaint with a supervisory authority in accordance with **Clause 12(c)(i)**;

ii) rectify inaccurate or incomplete data concerning the data subject;

iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.


© All rights reserved by Heiko Maniero.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

## Clause 11

## Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to **Clause 3**, the data importer shall accept the decision of the data subject to:

i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to **Clause 13**;

ii) refer the dispute to the competent courts within the meaning of **Clause 18**.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

## Clause 12

## Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

## Clause 13


© All rights reserved by Heiko Maniero.

**Supervision**

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in **Annex I.C**, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in **Annex I.C**, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in **Annex I.C**, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

**Clause 14**

**Local laws and practices affecting compliance with the Clauses**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, **Clause 16(d) and (e)** shall apply.

## Clause 15

## Obligations of the data importer in case of access by public authorities

### 15.1. Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.


© All rights reserved by Heiko Maniero.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to **Clause 14(e)** and **Clause 16** to inform the data exporter promptly where it is unable to comply with these Clauses.

### 15.2. Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under **Clause 14(e)**.

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## Clause 16

## Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to **Clause 14(f)**.

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

ii) the data importer is in substantial or persistent breach of these Clauses; or

iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.


© All rights reserved by Heiko Maniero.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

**Clause 17**

**Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of Germany.

**Clause 18**

**Choice of forum and jurisdiction**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Germany.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.


© All rights reserved by Heiko Maniero.

# ANNEX I

## A. LIST OF PARTIES

## SEE APPENDIX 7


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## B. DESCRIPTION OF TRANSFER

## SEE APPENDIX 8


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## C. COMPETENT SUPERVISORY AUTHORITY

## SEE APPENDIX 10


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## ANNEX II

## TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

**SEE APPENDIX 9**


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

# STANDARD CONTRACTUAL CLAUSES 2021/914
# MODULE TWO: Transfer Controller to Processor

## Clause 1
## Purpose and scope

(a) The purpose of these contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "**entity/ies**") transferring the personal data, as listed in **Annex I.A** (hereinafter each "**data exporter**"), and

ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in **Annex I.A** (hereinafter each "**data importer**")

have agreed to these contractual clauses ("**Clauses**").

(c) These Clauses apply with respect to the transfer of personal data as specified in **Annex I.B**.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

## Clause 2
## Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

## Clause 3
## Third-party beneficiaries


© All rights reserved by Heiko Maniero.

(a) The data subjects can enforce against the data exporter and/or data importer these Clauses, with the following exceptions:

i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

iii) Clause 9(a), (c), (d) and (e);

iv) Clause 12(a), (d) and (f);

v) Clause 13;

vi) Clause 15.1 (c), (d) and (e);

vii) Clause 16 (e);

viii) Clause 18 (a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

**Clause 4**

**Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

**Clause 5**

**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of other related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

**Clause 6**

**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in **Annex I.B** hereunder.

**Clause 7**

**Docking clause**

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing **Annex I.A.**

(b) Once it has completed the Appendix and signed **Annex I.A**, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in **Annex I.A**.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.


© All rights reserved by Heiko Maniero.

## Clause 8

### Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

### 8.1. Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

### 8.2. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in **Annex I. B**, unless on further instructions from the data exporter.

### 8.3. Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in **Annex II** and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

### 8.4. Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

### 8.5. Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in **Annex I.B**. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to **Clause 14**, in particular the requirement for the data importer under **Clause**


© All rights reserved by Heiko Maniero.

**14(e)** to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under **Clause 14(a)**.

### 8.6. Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in **Annex II**. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

### 8.7. Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in **Annex I.B**.

### 8.8. Onward transfers


© All rights reserved by Heiko Maniero.

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### 8.9. Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

## Clause 9

## Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION: The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these

 © All rights reserved by Heiko Maniero.

Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under **Clause 8.8.** The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

## Clause 10

## Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in **Annex II** the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

## Clause 11

## Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to **Clause 3**, the data importer shall accept the decision of the data subject to:

i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to **Clause 13**;

ii) refer the dispute to the competent courts within the meaning of **Clause 18**.


© All rights reserved by Heiko Maniero.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

**Clause 12**

**Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

**Clause 13**

**Supervision**

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in **Annex I.C**, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in **Annex I.C**, shall act as competent supervisory authority.


© All rights reserved by Heiko Maniero.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in **Annex I.C**, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

## Clause 14

## Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a


© All rights reserved by Heiko Maniero.

change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g., technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, **Clause 16(d) and (e)** shall apply.

## Clause 15

## Obligations of the data importer in case of access by public authorities

### 15.1. Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to **Clause 14(e)** and **Clause 16** to inform the data exporter promptly where it is unable to comply with these Clauses.

### 15.2. Review of legality and data minimisation


© All rights reserved by Heiko Maniero.

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under **Clause 14(e).**

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## Clause 16

## Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to **Clause 14(f)**.

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

ii) the data importer is in substantial or persistent breach of these Clauses; or

iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers


© All rights reserved by Heiko Maniero.

the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

**Clause 17**

**Governing law**

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

**Clause 18**

**Choice of forum and jurisdiction**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Germany.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.


© All rights reserved by Heiko Maniero.

# ANNEX I

## A. LIST OF PARTIES

## SEE APPENDIX 7


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## B. DESCRIPTION OF TRANSFER

## SEE APPENDIX 8


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## C. COMPETENT SUPERVISORY AUTHORITY

## SEE APPENDIX 10


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## ANNEX II

## TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

**SEE APPENDIX 9**


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## ANNEX III
## LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

**SEE APPENDIX 6**


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

# STANDARD CONTRACTUAL CLAUSES 2021/914
# MODULE THREE: Transfer Processor to Processor

## Clause 1
## Purpose and scope

(a) The purpose of these contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "**entity/ies**") transferring the personal data, as listed in **Annex I.A** (hereinafter each "**data exporter**"), and

ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in **Annex I.A** (hereinafter each "**data importer**")

have agreed to these standard contractual clauses (hereinafter: "**Clauses**").

(c) These Clauses apply with respect to the transfer of personal data between the Parties as specified in **Annex I.B**.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

## Clause 2
## Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

## Clause 3
## Third-party beneficiaries


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

(a) The data subjects can enforce against the data exporter and/or data importer these Clauses, with the following exceptions:

i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

ii) Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

iii) Clause 9(a), (c), (d) and (e);

iv) Clause 12(a), (d) and (f);

v) Clause 13;

vi) Clause 15.1 (c), (d) and (e);

vii) Clause 16 (e);

viii) Clause 18 (a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

**Clause 4**

**Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

**Clause 5**

**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of other related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

**Clause 6**

**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in **Annex I.B**.

**Clause 7**

**Docking clause**

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing **Annex I.A**.

(b) Once it has completed the Appendix and signed **Annex I.A**, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in **Annex I.A**.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.


© All rights reserved by Heiko Maniero.

## Clause 8

### Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

### 8.1. Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

### 8.2. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in **Annex I.B.**, unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

### 8.3. Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

### 8.4. Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

### 8.5. Duration of processing and erasure or return of data


© All rights reserved by Heiko Maniero.

Processing by the data importer shall only take place for the duration specified in **Annex I.B**. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to **Clause 14**, in particular the requirement for the data importer under **Clause 14(e)** to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under **Clause 14(a)**.

### 8.6. Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in **Annex II**. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

### 8.7. Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in **Annex I.B**.

### 8.8. Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679;

iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### 8.9. Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.


© All rights reserved by Heiko Maniero.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

**Clause 9**

**Use of sub-processors**

(a) GENERAL WRITTEN AUTHORISATION: The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under **Clause 8.8**. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

**Clause 10**

**Data subject rights**

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in **Annex II** the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## Clause 11

## Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to **Clause 3**, the data importer shall accept the decision of the data subject to:

i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to **Clause 13**;

ii) refer the dispute to the competent courts within the meaning of **Clause 18**.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

## Clause 12

## Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.


© All rights reserved by Heiko Maniero.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

**Clause 13**

**Supervision**

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in **Annex I.C**, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in **Annex I.C**, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in **Annex I.C**, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

**Clause 14**

**Local laws and practices affecting compliance with the Clauses**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in

 © All rights reserved by Heiko Maniero.

light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, **Clause 16(d) and (e)** shall apply.

## Clause 15

## Obligations of the data importer in case of access by public authorities

### 15.1. Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller.


© All rights reserved by Heiko Maniero.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to **Clause 14(e)** and **Clause 16** to inform the data exporter promptly where it is unable to comply with these Clauses.

### 15.2. Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under **Clause 14(e)**.

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## Clause 16

## Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to **Clause 14(f)**.

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:


© All rights reserved by Heiko Maniero.

i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

ii) the data importer is in substantial or persistent breach of these Clauses; or

iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

## Clause 17

## Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

## Clause 18

## Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Germany.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.


© All rights reserved by Heiko Maniero.

# ANNEX I

## A. LIST OF PARTIES

## SEE APPENDIX 7


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## B. DESCRIPTION OF TRANSFER

## SEE APPENDIX 8


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## C. COMPETENT SUPERVISORY AUTHORITY

## SEE APPENDIX 10


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## ANNEX II

## TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

**SEE APPENDIX 9**


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## ANNEX III
## LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

**SEE APPENDIX 6**


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

# STANDARD CONTRACTUAL CLAUSES 2021/914
# MODULE FOUR: Transfer Processor to Controller

## Clause 1

## Purpose and scope

(a) The purpose of these contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "**entity/ies**") transferring the personal data, as listed in **Annex I.A** (hereinafter each "**data exporter**"), and

ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in **Annex I.A** (hereinafter each "**data importer**")

have agreed to these standard contractual clauses (hereinafter: "**Clauses**").

(c) These Clauses apply with respect to the transfer of personal data between the Parties as specified in **Annex I.B**.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

## Clause 2

## Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.


© All rights reserved by Heiko Maniero.

**Clause 3**

**Third-party beneficiaries**

(a) The data subjects can enforce against the data exporter and/or data importer these Clauses, with the following exceptions:

i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

ii) Clause 8.1 (b) and Clause 8.3(b);

*[iii) and iv) not applicable]*

v) Clause 13;

vi) Clause 15.1 (c), (d) and (e);

vii) Clause 16 (e);

viii) Clause 18;

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

**Clause 4**

**Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

**Clause 5**

**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of other related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

**Clause 6**

**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in **Annex I.B** hereunder.

**Clause 7**

**Docking clause**

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing **Annex I.A**.

(b) Once it has completed the Appendix and signed **Annex I.A**, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in **Annex I.A**.


© All rights reserved by Heiko Maniero.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.


© All rights reserved by Heiko Maniero.

## Clause 8

### Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

### 8.1. Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

### 8.2. Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

### 8.3. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.


© All rights reserved by Heiko Maniero.

***[Clause 9 not applicable]***

**Clause 10**

**Data subject rights**

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

**Clause 11**

**Redress**

The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

**Clause 12**

**Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

***[Clause 13 not applicable]***

**Clause 14**

**Local laws and practices affecting compliance with the Clauses**

Where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU):

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is


© All rights reserved by Heiko Maniero.

based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, **Clause 16(d) and (e)** shall apply.

## Clause 15

## Obligations of the data importer in case of access by public authorities

Where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU:


© All rights reserved by Heiko Maniero.

### 15.1. Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to **Clause 14(e)** and **Clause 16** to inform the data exporter promptly where it is unable to comply with these Clauses.

### 15.2. Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under **Clause 14(e)**.

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.


© All rights reserved by Heiko Maniero.

**Clause 16**

**Non-compliance with the Clauses and termination**

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to **Clause 14(f).**

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

ii) the data importer is in substantial or persistent breach of these Clauses; or

iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

**Clause 17**

**Governing law**

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

**Clause 18**

**Choice of forum and jurisdiction**

Any dispute arising from these Clauses shall be resolved by the courts of Germany.


© All rights reserved by Heiko Maniero.

# ANNEX I

## A. LIST OF PARTIES

## SEE APPENDIX 7


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## B. DESCRIPTION OF TRANSFER

## SEE APPENDIX 8


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## APPENDIX 6 – SUB-PROCESSORS

**A CURRENT LIST OF OUR PROCESSORS CAN BE FOUND ON OUR WEBSITE OR CAN BE REQUESTED SEPARATELY.**

**Our list contains the following information on all processors:**

**Company name, Link to website, Service or transmission details, Country of processing, Subject matter of (sub-) processing, Nature of (sub-) processing, Duration of (sub-) processing, Concluded contract or appropriate safeguards according to Art. 44ff GDPR.**

**IF YOU USE OTHER PROCESSORS NOT MENTIONED IN OUR LIST AND / OR APPROVED BY US, PLEASE SEND US A LIST OF THEIR PROCESSORS FOR VERIFICATION AND / OR APPROVAL.**


© All rights reserved by Heiko Maniero.

## APPENDIX 7 – LIST OF PARTIES

**Party Number 1:**

Name: Provider name, see Main-Agreement

Address: Provider address, see Main-Agreement

Contact person's name, position and contact details: Provider contact person, see Main-Agreement

Activities relevant to the data transferred under these Clauses: All activities in which personal data are processed or transmitted

If applicable, the controller's data protection officer: If applicable, see website of Provider

If applicable, the representative in the European Union: If applicable, see website of Provider

Accession date/date: See date of Main-Agreement

Role: Controller and/or Processor, based on the applicable SCCs or other contract, or Overseas Recipient

**Party Number 2:**

Name: Business Partner name, see Main-Agreement

Address: Business Partner address, see Main-Agreement

Contact person's name, position and contact details: Business Partner contact person, see Main-Agreement

Activities relevant to the data transferred under these Clauses: All activities in which personal data are processed or transmitted

If applicable, the controller's data protection officer: If applicable, see website of Business Partner

If applicable, the representative in the European Union: If applicable, see website of Business Partner

Accession date/date: See date of Main-Agreement

Role: Controller and/or Processor, based on the applicable SCCs or other contract, or Overseas Recipient


© All rights reserved by Heiko Maniero.

## APPENDIX 8 – DESCRIPTION OF THE PROCESSING OR THE TRANSFER

**Categories of data subjects / personal information subjects whose personal data is processed or transferred:**

Customers, potential customers, employees, business partners, suppliers.

**Categories of personal data / personal information processed or transferred:**

Customer data, data of potential customers, employee data, data of business partners, supplier data.

**Sensitive data processed or transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.**

**Sensitive data / sensitive personal information processed or transferred:**

None.

**Applied restrictions or safeguards:**

None, because no sensitive data is processed or transferred.

**Frequency of transfer:**

The data is transferred on a continuous basis as long as the Main-Agreement is in force.

**Nature of the processing:**

See Main-Agreement, the following processing could occur: collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, otherwise making available, alignment, combination, restriction, erasure, destruction.

**Purpose(s) for which the personal data / personal information is processed on behalf of the controller or Purpose(s) of the data transfer and further processing:**

See Main-Agreement.

**Duration of the processing:**


© All rights reserved by Heiko Maniero.

Duration of the Main-Agreement.

**The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period**

The criteria for determining the retention period is resulting from the main contract and statutory retention periods.

**For processing by or transfer to (sub-) processors, also specify subject matter, nature and duration of the processing**

**Subject matter of (sub-) processing: SEE APPENDIX 6**

**Nature of (sub-) processing: SEE APPENDIX 6**

**Duration of (sub-) processing: SEE APPENDIX 6**


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES

**The technical and organizational security measures mentioned as follows are the minimum required from you, and are also fulfilled by us. If you have not implemented these technical and organizational security measures, please inform us immediately. Furthermore, you shall send us a list of all additional technical and organizational security measures taken by you, if any.**

1. **Measures of pseudonymization and encryption of personal data**

Pseudonymisation of personal data that are no longer needed in plain text
Encryption of websites (SSL)
Encryption of e-mail (TLS 1.2 or 1.3)

2. **Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services**

Confidentiality agreements with employees
NDAs with third parties
Data Protection agreements with employees
Firewall
Anti-Virus
Regular backups

3. **Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident**

Regular backups of the whole system
Regular test of backup and recovery
Regular training of IT staff

4. **Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing**

In-house checks
Regular review of processes by IT
Regular audits (e.g. by the DPO)

5. **Measures for user identification and authorisation**


© All rights reserved by Heiko Maniero.

Authentication with username / password
Regular checks of authorisations
Password guideline
Limitation of the number of administrators
Management of rights by system administrator

### 6. Measures for the protection of data during transmission

Use of encryption technologies
Logging of activities and events
Encryption of email (TIS 1.2 or 1.3)
Use of company internal / restricted drives

### 7. Measures for the protection of data during storage

Logging of actions and events
Limitation of the number of administrator's
Firewall

### 8. Measures for ensuring physical security of locations at which personal data are processed

Manual locking system
Security locks
Key control

### 9. Measures for ensuring events logging

Logging activated on application level
Regular manual checks of logs

### 10. Measures for ensuring system configuration, including default configuration

Configuration change control process
Data protection by default is observed
Configuration only by system administrator
Regular training of IT staff


© All rights reserved by Heiko Maniero.

## 11. Measures for internal IT and IT security governance and management

IT security policy
Training of employees on data security
IT team with clear roles and responsibilities

## 12. Measures for certification/assurance of processes and products

Clear overview of the provisions applicable to the provided products/services/processes
Regular internal and/or external audits
Assignment of audit responsibilities to certified experts

## 13. Measures for ensuring data minimization

Identification of the purpose of processing
Assessment of a link between processing and purpose
Identification of the applicable retention periods for each data category
Secure erasure of the data after expiration of the retention period

## 14. Measures for ensuring data quality

Logging of entry and modification of data
Assignment of rights for data entry
Traceability of entry, modification of data by individual user names (not user groups)

## 15. Measures for ensuring limited data retention

Regular training on retention periods
Regular audit and assessment of retained data

## 16. Measures for ensuring accountability

Provision of training / awareness rising
Regular controls and checks
Appropriate policies on data protection
Conclusion of SCCs

## 17. Measures for allowing data portability and ensuring erasure


© All rights reserved by Heiko Maniero.

Personal data is stored in a structured format
Monitoring of legal deadline ensured
Observation of retention periods
Establishment of data portability process
Proper handling of data subject requests
Secure data erasure and data carrier destruction ensured by contracting with Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Germany, email: info@notebook12.com

18. **For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter**

Standard Contractual Clauses (SCCs) are signed or agreed on
Contractually agreed on effective control rights
Contractually agreed on provision of assistance to the controller


© All rights reserved by Heiko Maniero.

## APPENDIX 10 – COMPETENT SUPERVISORY AUTHORITY

The supervisory authority responsible for the first controller is responsible. If the first controller is located outside the European Union or the EEA, the parties hereby irrevocably declare the competence of the following supervisory authority:

BayLDA - Das Bayerische Landesamt für Datenschutzaufsicht

Promenade 18

91522 Ansbach

Deutschland


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

# Confidentiality and Data Protection Agreement for Vendors

Between our company

- Principal -

and your company

- Contractor -

the following is agreed on:

1. The Contractor is obliged to keep business and trade secrets as well as operational matters of a confidential nature, which are designated as such by the Principal in written or oral form, or are obviously to be recognized as such information, confidential and not make them available to any third party without explicit approval of Principal. The obligation to maintain secrecy shall also apply to employees of Client and Contractor, third parties and other contractual partners of Client and Contractor and their employees, provided that they are not directly involved in the matter in question.

   Business and trade secret is any information that

   a) neither in general nor in their precise arrangement or composition is generally known or otherwise available to the persons in circles, who usually handle such type of information and is therefore of economic value and

   b) subject in appropriate circumstances to reasonable confidentiality measures by its lawful owner and

   c) where there is a legitimate interest in secrecy.

   Trade secret, according to global Trade Secrets Acts and thereby confidential, is particularly information related to prices, target figures, turnover / profit / income figures, economical figures, current and planned projects, technological and conceptual structures, analytical work, software architectures and interfaces, datasets and their usage, passwords, authorities, duties, suppliers and customers data, data of relevant business partners as well as particularly all confidential information related to customers and suppliers of Principal, to which the Contractor got access when preparing or executing an order or regarding to customers and suppliers of Principal, as for example information on relevant customers or suppliers of Principal, business processes, infrastructure, business plans and products, software, programming or any information, that Contractor processed during usage of confidential information. The information is not subject of the nondisclosure obligation, if it is to everyone accessible or is generally known. In case of doubts Contractor shall obtain an instruction from Principal regarding confidentiality of certain facts.


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

2. The Contractor is obliged to keep bank secrecy, secrecy of telecommunications, communication confidentiality, postal secrecy, secrecy of social data, and privacy of correspondence and abide all other secrecy regulations and laws.

3. Nondisclosure obligation is not applicable to third parties, insofar as there is a lawful disclosure obligation. It is also not applicable to persons who are professionally obliged to secrecy, insofar as disclosure of facts to be kept in secret is necessary to ensure legitimate interest of Contractor.

4. The nondisclosure obligation also extends to matters of other companies, with which the Principal is economically or organizationally associated.

5. The nondisclosure obligation will continue to exist also after the termination of the contractual relationship. If any post contractual nondisclosure obligations of Contractor put an obstacles to its professional development, it has the right to be exempted from these obligations by Principal.

6. Contractor is notified, that disclosure of secrets may be punishable in accordance with applicable Trade Secret Acts.

7. The Contractor is obliged to keep personal data, to which it gets access to or becomes aware of within a framework of its activities, confidential. The Contractor is prohibited from unauthorized accessing or processing, in particular to collect, record, organize, structure, store, adapt or alter, retrieve, consult, use, disclose by transmission, dissemination or otherwise make available, align or combine, restrict, erase or destruct personal data, which means all information related to identified or identifiable natural persons; 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.

   Personal data can only be processed, when consent or another legal basis permits processing of such data.

   Personal data shall be at all times

   a) processed lawfully and in a comprehensive manner for the data subject;
   b) collected with the defined, explicit and legitimate purpose and shall not be processed in other way, that is not associated with those purposes;
   c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimization’);
   d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
   e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;


© All rights reserved by Heiko Maniero.

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’).

8. The obligation to maintain data secrecy continues to exist after termination of the contractual relationship.

9. Contractor has been informed that the violation of the protection of personal data may be punishable according to applicable data protection laws.

10. The Contractor will consider requirements of Principal’s customers on how to deal with confidential matters and personal data and their protection.

11. Defects in data protection or data protection system shall be unrequested and immediately reported to the top management or Data Protection Officer of the Principal.

12. Special nondisclosure agreements or requirements (for example, project or customer-oriented agreements) remain unaffected and are applicable besides the obligations of this nondisclosure agreement.

13. The Contractor recognizes that the Principal is obliged to the comprehensive secrecy in relationship with its customers and is threatened with severe sanctions (loss of contract, penalty payments, compensation etc.), if these obligations will be infringed by Principal or Contractor.

14. Infringement of abovementioned obligations can entitle the Principal to the extraordinary and when appropriate without previous notice termination of contractual relationship and cause Contractor’s obligation to compensation.

This document contains general terms and conditions. They become effective by publication and after written inclusion in the main contract (e.g., inclusion by sending a link via e-mail).


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

# Confidentiality and Data Protection Agreement for Customers

Between our company

- Provider -

and your company

- Client -

jointly, the - Parties -

the following is agreed on:

1. The Parties are obliged to keep business and trade secrets as well as operational matters of a confidential nature, which are designated as such by the other party in written or oral form, or are obviously to be recognized as such information, confidential and not make them available to any third party without explicit approval of the other party. The obligation to maintain secrecy shall also apply to employees of the parties, third parties and other contractual partners of the parties and their employees, provided that they are not directly involved in the matter in question.

   Business and trade secret is any information that

   d) neither in general nor in their precise arrangement or composition is generally known or otherwise available to the persons in circles, who usually handle such type of information and is therefore of economic value and

   e) subject in appropriate circumstances to reasonable confidentiality measures by its lawful owner and

   f) where there is a legitimate interest in secrecy.

   Trade secret, according to global Trade Secrets Acts and thereby confidential, is particularly information related to prices, target figures, turnover / profit / income figures, economical figures, current and planned projects, technological and conceptual structures, analytical work, software architectures and interfaces, datasets and their usage, passwords, authorities, duties, suppliers and customers data, data of relevant business partners as well as particularly all confidential information related to customers and suppliers of one party, to which the other party got access when preparing or executing an order or regarding to customers and suppliers of the other party, as for example information on relevant customers or suppliers of one party, business processes, infrastructure, business plans and products, software, programming or any information, that the other party processed during usage of confidential information. The information is not subject of the nondisclosure obligation, if it is to everyone accessible or is


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

generally known. In case of doubts one party shall obtain an instruction from the other party regarding confidentiality of certain facts.

2. Both parties are obliged to keep bank secrecy, secrecy of telecommunications, communication confidentiality, postal secrecy, secrecy of social data, and privacy of correspondence and to abide all other secrecy regulations and laws.

3. Nondisclosure obligation is not applicable to third parties, insofar as there is a lawful disclosure obligation. It is also not applicable to persons who are professionally obliged to secrecy, insofar as disclosure of facts to be kept in secret is necessary to ensure legitimate interest of the party.

4. The nondisclosure obligation also extends to matters of other companies, with which the other party is economically or organizationally associated.

5. The nondisclosure obligation will continue to exist also after the termination of the contractual relationship. If any post contractual nondisclosure obligations of one party put an obstacles to the professional development of the other party, the second party has the right to be exempted from these obligations by the first party.

6. Both parties understand that disclosure of secrets may be punishable in accordance with applicable Trade Secret Acts.

7. Both parties are obliged to keep personal data, to which they get access to or become aware of within the framework of their activities, confidential. Both parties are prohibited from unauthorized accessing or processing, in particular to collect, record, organize, structure, store, adapt or alter, retrieve, consult, use, disclose by transmission, disseminate or otherwise make available, align or combine, restrict, erase or destruct personal data, which means all information related to identified or identifiable natural persons; 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.

   Personal data can only be processed, when consent or another legal basis permits processing of such data.

   Personal data shall be at all times

   g) processed lawfully and in a comprehensive manner for the data subject;
   h) collected with the defined, explicit and legitimate purpose and shall not be processed in other way, that is not associated with those purposes;
   i) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimization’);
   j) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
   k) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;


© All rights reserved by Heiko Maniero.

l) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

8. The obligation to maintain data secrecy continues to exist after termination of the contractual relationship.

9. Both parties are informed that the violation of the protection of personal data may be punishable according to applicable data protection laws.

10. Both parties will consider requirements of the other parties' customers on how to deal with confidential matters and personal data and their protection.

11. Defects in data protection or data protection system shall be unrequested and immediately reported to the top management or Data Protection Officer of the other party.

12. Special nondisclosure agreements or requirements (for example, project or customer-oriented agreements) remain unaffected and are applicable besides the obligations of this nondisclosure agreement.

13. The parties recognize that the other party may be obliged to comprehensive secrecy in relationship with its customers and is threatened with severe sanctions (loss of contract, penalty payments, compensation etc.), if these obligations will be infringed by one of the parties.

14. Infringement of abovementioned obligations can entitle the other party to the extraordinary and when appropriate without previous notice termination of contractual relationship and cause an obligation to compensation.

This document contains general terms and conditions. They become effective by publication and after written inclusion in the main contract (e.g. inclusion by sending a link via e-mail).


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

# Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

## International Data Transfer Agreement

VERSION A1.0, in force 21 March 2022

This IDTA has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

## Part 1: Tables

### Table 1: Parties and signatures

| | | |
|---|---|---|
| **Start date** | see Main-Agreement | |
| **The Parties** | **Exporter (who sends the Restricted Transfer)** | **Importer (who receives the Restricted Transfer)** |
| **Parties' details** | Full legal name:<br>see Main-Agreement<br>Trading name (if different):<br>if applicable, see Main-Agreement<br>Main address (if a company registered address):<br>see Main-Agreement | Full legal name:<br>see Main-Agreement<br>Trading name (if different):<br>if applicable, see Main-Agreement<br>Main address (if a company registered address):<br>see Main-Agreement |


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

| | | |
|---|---|---|
| | Official registration number (if any) (company number or similar identifier):<br>if applicable, see Main-Agreement | Official registration number (if any) (company number or similar identifier):<br>if applicable, see Main-Agreement |
| **Key Contact** | Full Name (optional):<br>if applicable, see Main-Agreement<br>Job Title:<br>if applicable, see Main-Agreement<br>Contact details including email:<br>if applicable, see Main-Agreement | Full Name (optional):<br>if applicable, see Main-Agreement<br>Job Title:<br>if applicable, see Main-Agreement<br>Contact details including email:<br>if applicable, see Main-Agreement |
| **Importer Data Subject Contact** | | Job Title: see Main-Agreement<br>Contact details including email: see Main-Agreement |
| **Signatures confirming each Party agrees to be bound by this IDTA** | Signed for and on behalf of the **Exporter** set out above<br>Signed:<br>see Main-Agreement<br>Date of signature:<br>see Main-Agreement<br>Full name:<br>see Main-Agreement<br>Job title:<br>see Main-Agreement | Signed for and on behalf of the **Importer** set out above<br>Signed:<br>see Main-Agreement<br>Date of signature:<br>see Main-Agreement<br>Full name:<br>see Main-Agreement<br>Job title:<br>see Main-Agreement |


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

Table 2: Transfer Details

| | |
|---|---|
| **UK country's law that governs the IDTA:** | England and Wales, Northern Ireland, or Scotland<br>see Main-Agreement, or alternatively, place on the main establishment of the Exporter, or alternatively, based on the place of residence of the majority of data subjects |
| **Primary place for legal claims to be made by the Parties** | England and Wales, Northern Ireland, or Scotland<br>see Main-Agreement, or alternatively, place on the main establishment of the Exporter, or alternatively, based on the place of residence of the majority of data subjects |
| **The status of the Exporter** | In relation to the Processing of the Transferred Data:<br>Exporter is a Controller / or / Exporter is a Processor or Sub-Processor – based on the nature of the Main-Agreement, and the Agreement with another Controller |
| **The status of the Importer** | In relation to the Processing of the Transferred Data:<br>Importer is a Controller / or / Importer is the Exporter's Processor or Sub-Processor / or / Importer is not the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller) - based on the nature of the Main-Agreement, and the Agreement with another Controller or Third Party |
| **Whether UK GDPR applies to the Importer** | UK GDPR applies to the Importer's Processing of the Transferred Data |
| **Linked Agreement** | **If the Importer is the Exporter's Processor or Sub-Processor** – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data:<br>Name of agreement: if any, see Main-Agreement<br>Date of agreement: if any, see Main-Agreement |


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

| | |
|---|---|
| | Parties to the agreement: if any, see Main-Agreement<br>Reference (if any): if any, see Main-Agreement<br>**Other agreements** – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement:<br>Name of agreement: if any, see Main-Agreement<br>Date of agreement: if any, see Main-Agreement<br>Parties to the agreement: if any, see Main-Agreement<br>Reference (if any): if any, see Main-Agreement<br>**If the Exporter is a Processor or Sub-Processor** – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data:<br>Name of agreement: if any, see Main-Agreement<br>Date of agreement: if any, see Main-Agreement<br>Parties to the agreement: if any, see Main-Agreement<br>Reference (if any): if any, see Main-Agreement |
| **Term** | The Importer may Process the Transferred Data for the following time period:<br>the period for which the Linked Agreement is in force |
| **Ending the IDTA before the end of the Term** | The Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing. |
| **Ending the IDTA when the Approved IDTA changes** | Which Parties may end the IDTA as set out in Section 29.2:<br>neither Party |


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

| | |
|---|---|
| **Can the Importer make further transfers of the Transferred Data?** | The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data). |
| **Specific restrictions when the Importer may transfer on the Transferred Data** | The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1:<br>there are no specific restrictions. |
| **Review Dates** | Each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment. |

Table 3: Transferred Data

| | |
|---|---|
| **Transferred Data** | The personal data to be sent to the Importer under this IDTA consists of:<br>The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to. |
| **Special Categories of Personal Data and criminal convictions and offences** | The Transferred Data includes data relating to:<br>none |
| **Relevant Data Subjects** | The Data Subjects of the Transferred Data are: |


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

| | |
|---|---|
| | The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to. |
| **Purpose** | The Importer may Process the Transferred Data for the following purposes: To fulfil the Main-Agreement. |

Table 4: Security Requirements

| | |
|---|---|
| **Security of Transmission** | See APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES |
| **Security of Storage** | See APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES |
| **Security of Processing** | See APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES |
| **Organisational security measures** | See APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES |
| **Technical security minimum requirements** | See APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES |
| **Updates to the Security Requirements** | The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to. |

Part 2: Extra Protection Clauses

| | |
|---|---|
| **Extra Protection Clauses:** | None |


© All rights reserved by Heiko Maniero.

| | |
|---|---|
| **(i) Extra technical security protections** | See APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES |
| **(ii) Extra organisational protections** | None |
| **(iii) Extra contractual protections** | None |

## Part 3: Commercial Clauses

| | |
|---|---|
| **Commercial Clauses** | see Main-Agreement |

## Part 4: Mandatory Clauses

### Information that helps you to understand this IDTA

### 1. This IDTA and Linked Agreements

1.1 Each Party agrees to be bound by the terms and conditions set out in the IDTA, in exchange for the other Party also agreeing to be bound by the IDTA.

1.2 This IDTA is made up of:

1.2.1 Part one: Tables;

1.2.2 Part two: Extra Protection Clauses;

1.2.3 Part three: Commercial Clauses; and

1.2.4 Part four: Mandatory Clauses.

1.3 The IDTA starts on the Start Date and ends as set out in Sections 29 or 30.

1.4 If the Importer is a Processor or Sub-Processor instructed by the Exporter: the Exporter must ensure that, on or before the Start Date and during the Term, there is a Linked Agreement which is enforceable between the Parties


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

and which complies with Article 28 UK GDPR (and which they will ensure continues to comply with Article 28 UK GDPR).

1.5 References to the Linked Agreement or to the Commercial Clauses are to that Linked Agreement or to those Commercial Clauses only in so far as they are consistent with the Mandatory Clauses.

## 2. Legal Meaning of Words

2.1 If a word starts with a capital letter it has the specific meaning set out in the Legal Glossary in Section 36.

2.2 To make it easier to read and understand, this IDTA contains headings and guidance notes. Those are not part of the binding contract which forms the IDTA.

## 3. You have provided all the information required

3.1 The Parties must ensure that the information contained in Part one: Tables is correct and complete at the Start Date and during the Term.

3.2 In Table 2: Transfer Details, if the selection that the Parties are Controllers, Processors or Sub-Processors is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws) then:

3.2.1 the terms and conditions of the Approved IDTA which apply to the correct option which was not selected will apply; and

3.2.2 the Parties and any Relevant Data Subjects are entitled to enforce the terms and conditions of the Approved IDTA which apply to that correct option.

3.3 In Table 2: Transfer Details, if the selection that the UK GDPR applies is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws), then the terms and conditions of the IDTA will still apply to the greatest extent possible.

## 4. How to sign the IDTA

4.1 The Parties may choose to each sign (or execute):

4.1.1 the same copy of this IDTA;

4.1.2 two copies of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement;


© All rights reserved by Heiko Maniero.

4.1.3 a separate, identical copy of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement,

unless signing (or executing) in this way would mean that the IDTA would not be binding on the Parties under Local Laws.

## 5. Changing this IDTA

5.1 Each Party must not change the Mandatory Clauses as set out in the Approved IDTA, except only:

5.1.1 to ensure correct cross-referencing: cross-references to Part one: Tables (or any Table), Part two: Extra Protections, and/or Part three: Commercial Clauses can be changed where the Parties have set out the information in a different format, so that the cross-reference is to the correct location of the same information, or where clauses have been removed as they do not apply, as set out below;

5.1.2 to remove those Sections which are expressly stated not to apply to the selections made by the Parties in Table 2: Transfer Details, that the Parties are Controllers, Processors or Sub-Processors and/or that the Importer is subject to, or not subject to, the UK GDPR. The Exporter and Importer understand and acknowledge that any removed Sections may still apply and form a part of this IDTA if they have been removed incorrectly, including because the wrong selection is made in Table 2: Transfer Details;

5.1.3 so the IDTA operates as a multi-party agreement if there are more than two Parties to the IDTA. This may include nominating a lead Party or lead Parties which can make decisions on behalf of some or all of the other Parties which relate to this IDTA (including reviewing Table 4: Security Requirements and Part two: Extra Protection Clauses, and making updates to Part one: Tables (or any Table), Part two: Extra Protection Clauses, and/or Part three: Commercial Clauses); and/or

5.1.4 to update the IDTA to set out in writing any changes made to the Approved IDTA under Section 5.4, if the Parties want to. The changes will apply automatically without updating them as described in Section 5.4;

provided that the changes do not reduce the Appropriate Safeguards.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

5.2 If the Parties wish to change the format of the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of the Approved IDTA, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

5.3 If the Parties wish to change the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of this IDTA (or the equivalent information), they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

5.4 From time to time, the ICO may publish a revised Approved IDTA which:

5.4.1 makes reasonable and proportionate changes to the Approved IDTA, including correcting errors in the Approved IDTA; and/or

5.4.2 reflects changes to UK Data Protection Laws.

The revised Approved IDTA will specify the start date from which the changes to the Approved IDTA are effective and whether an additional Review Date is required as a result of the changes. This IDTA is automatically amended as set out in the revised Approved IDTA from the start date specified.

## 6. Understanding this IDTA

6.1 This IDTA must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

6.2 If there is any inconsistency or conflict between UK Data Protection Laws and this IDTA, the UK Data Protection Laws apply.

6.3 If the meaning of the IDTA is unclear or there is more than one meaning, the meaning which most closely aligns with the UK Data Protection Laws applies.

6.4 Nothing in the IDTA (including the Commercial Clauses or the Linked Agreement) limits or excludes either Party's liability to Relevant Data Subjects or to the ICO under this IDTA or under UK Data Protection Laws.

6.5 If any wording in Parts one, two or three contradicts the Mandatory Clauses, and/or seeks to limit or exclude any liability to Relevant Data Subjects or to the ICO, then that wording will not apply.


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

6.6 The Parties may include provisions in the Linked Agreement which provide the Parties with enhanced rights otherwise covered by this IDTA. These enhanced rights may be subject to commercial terms, including payment, under the Linked Agreement, but this will not affect the rights granted under this IDTA.

6.7 If there is any inconsistency or conflict between this IDTA and a Linked Agreement or any other agreement, this IDTA overrides that Linked Agreement or any other agreements, even if those agreements have been negotiated by the Parties. The exceptions to this are where (and in so far as):

6.7.1 the inconsistent or conflicting terms of the Linked Agreement or other agreement provide greater protection for the Relevant Data Subject's rights, in which case those terms will override the IDTA; and

6.7.2 a Party acts as Processor and the inconsistent or conflicting terms of the Linked Agreement are obligations on that Party expressly required by Article 28 UK GDPR, in which case those terms will override the inconsistent or conflicting terms of the IDTA in relation to Processing by that Party as Processor.

6.8 The words "include", "includes", "including", "in particular" are used to set out examples and not to set out a finite list.

6.9 References to:

6.9.1 singular or plural words or people, also includes the plural or singular of those words or people;

6.9.2 legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this IDTA has been signed; and

6.9.3 any obligation not to do something, includes an obligation not to allow or cause that thing to be done by anyone else.

## 7. Which laws apply to this IDTA

7.1 This IDTA is governed by the laws of the UK country set out in Table 2: Transfer Details. If no selection has been made, it is the laws of England


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

and Wales. This does not apply to Section 35 which is always governed by the laws of England and Wales.

How this IDTA provides Appropriate Safeguards

## 8. The Appropriate Safeguards

8.1 The purpose of this IDTA is to ensure that the Transferred Data has Appropriate Safeguards when Processed by the Importer during the Term. This standard is met when and for so long as:

8.1.1 both Parties comply with the IDTA, including the Security Requirements and any Extra Protection Clauses; and

8.1.2 the Security Requirements and any Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach, including considering any Special Category Data within the Transferred Data.

8.2 The Exporter must:

8.2.1 ensure and demonstrate that this IDTA (including any Security Requirements and Extra Protection Clauses) provides Appropriate Safeguards; and

8.2.2 (if the Importer reasonably requests) provide it with a copy of any TRA.

8.3 The Importer must:

8.3.1 before receiving any Transferred Data, provide the Exporter with all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including any information which may reasonably be required for the Exporter to carry out any TRA (the "Importer Information");

8.3.2 co-operate with the Exporter to ensure compliance with the Exporter's obligations under the UK Data Protection Laws;

8.3.3 review whether any Importer Information has changed, and whether any Local Laws contradict its obligations in this IDTA and take reasonable steps to verify this, on a regular basis. These reviews must be at least as frequent as the Review Dates; and


© All rights reserved by Heiko Maniero.

8.3.4 inform the Exporter as soon as it becomes aware of any Importer Information changing, and/or any Local Laws which may prevent or limit the Importer complying with its obligations in this IDTA. This information then forms part of the Importer Information.

8.4 The Importer must ensure that at the Start Date and during the Term:

8.4.1 the Importer Information is accurate;

8.4.2 it has taken reasonable steps to verify whether there are any Local Laws which contradict its obligations in this IDTA or any additional information regarding Local Laws which may be relevant to this IDTA.

8.5 Each Party must ensure that the Security Requirements and Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

## 9. Reviews to ensure the Appropriate Safeguards continue

9.1 Each Party must:

9.1.1 review this IDTA (including the Security Requirements and Extra Protection Clauses and the Importer Information) at regular intervals, to ensure that the IDTA remains accurate and up to date and continues to provide the Appropriate Safeguards. Each Party will carry out these reviews as frequently as the relevant Review Dates or sooner; and

9.1.2 inform the other party in writing as soon as it becomes aware if any information contained in either this IDTA, any TRA or Importer Information is no longer accurate and up to date.

9.2 If, at any time, the IDTA no longer provides Appropriate Safeguards the Parties must Without Undue Delay:

9.2.1 pause transfers and Processing of Transferred Data whilst a change to the Tables is agreed. The Importer may retain a copy of the Transferred Data during this pause, in which case the Importer must carry out any Processing required to maintain, so far as possible, the measures it was taking to achieve the Appropriate Safeguards prior to the time the IDTA no longer provided Appropriate Safeguards, but no other Processing;


© All rights reserved by Heiko Maniero.

9.2.2 agree a change to Part one: Tables or Part two: Extra Protection Clauses which will maintain the Appropriate Safeguards (in accordance with Section 5); and

9.2.3 where a change to Part one: Tables or Part two: Extra Protection Clauses which maintains the Appropriate Safeguards cannot be agreed, the Exporter must end this IDTA by written notice on the Importer.

## 10. The ICO

10.1 Each Party agrees to comply with any reasonable requests made by the ICO in relation to this IDTA or its Processing of the Transferred Data.

10.2 The Exporter will provide a copy of any TRA, the Importer Information and this IDTA to the ICO, if the ICO requests.

10.3 The Importer will provide a copy of any Importer Information and this IDTA to the ICO, if the ICO requests.

### The Exporter

## 11. Exporter's obligations

11.1 The Exporter agrees that UK Data Protection Laws apply to its Processing of the Transferred Data, including transferring it to the Importer.

11.2 The Exporter must:

11.2.1 comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;

11.2.2 comply with the Linked Agreement as it relates to its transferring the Transferred Data to the Importer; and

11.2.3 carry out reasonable checks on the Importer's ability to comply with this IDTA, and take appropriate action including under Section 9.2, Section 29 or Section 30, if at any time it no longer considers that the Importer is able to comply with this IDTA or to provide Appropriate Safeguards.

11.3 The Exporter must comply with all its obligations in the IDTA, including any in the Security Requirements, and any Extra Protection Clauses and any Commercial Clauses.

11.4 The Exporter must co-operate with reasonable requests of the Importer to pass on notices or other information to and from Relevant Data Subjects


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

or any Third Party Controller where it is not reasonably practical for the Importer to do so. The Exporter may pass these on via a third party if it is reasonable to do so.

11.5 The Exporter must co-operate with and provide reasonable assistance to the Importer, so that the Importer is able to comply with its obligations to the Relevant Data Subjects under Local Law and this IDTA.

The Importer

## 12. General Importer obligations

12.1 The Importer must:

12.1.1 only Process the Transferred Data for the Purpose;

12.1.2 comply with all its obligations in the IDTA, including in the Security Requirements, any Extra Protection Clauses and any Commercial Clauses;

12.1.3 comply with all its obligations in the Linked Agreement which relate to its Processing of the Transferred Data;

12.1.4 keep a written record of its Processing of the Transferred Data, which demonstrate its compliance with this IDTA, and provide this written record if asked to do so by the Exporter;

12.1.5 if the Linked Agreement includes rights for the Exporter to obtain information or carry out an audit, provide the Exporter with the same rights in relation to this IDTA; and

12.1.6 if the ICO requests, provide the ICO with the information it would be required on request to provide to the Exporter under this Section 12.1 (including the written record of its Processing, and the results of audits and inspections).

12.2 The Importer must co-operate with and provide reasonable assistance to the Exporter and any Third Party Controller, so that the Exporter and any Third Party Controller are able to comply with their obligations under UK Data Protection Laws and this IDTA.

## 13. Importer's obligations if it is subject to the UK Data Protection Laws

13.1 If the Importer's Processing of the Transferred Data is subject to UK Data Protection Laws, it agrees that:


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

13.1.1 UK Data Protection Laws apply to its Processing of the Transferred Data, and the ICO has jurisdiction over it in that respect; and

13.1.2 it has and will comply with the UK Data Protection Laws in relation to the Processing of the Transferred Data.

13.2 If Section 13.1 applies and the Importer complies with Section 13.1, it does not need to comply with:

- Section 14 (Importer's obligations to comply with key data protection principles);
- Section 15 (What happens if there is an Importer Personal Data Breach);
- Section 15 (How Relevant Data Subjects can exercise their data subject rights); and
- Section 21 (How Relevant Data Subjects can exercise their data subject rights – if the Importer is the Exporter's Processor or Sub-Processor).

## 14. Importer's obligations to comply with key data protection principles

14.1 The Importer does not need to comply with this Section 14 if it is the Exporter's Processor or Sub-Processor.

14.2 The Importer must:

14.2.1 ensure that the Transferred Data it Processes is adequate, relevant and limited to what is necessary for the Purpose;

14.2.2 ensure that the Transferred Data it Processes is accurate and (where necessary) kept up to date, and (where appropriate considering the Purposes) correct or delete any inaccurate Transferred Data it becomes aware of Without Undue Delay; and

14.2.3 ensure that it Processes the Transferred Data for no longer than is reasonably necessary for the Purpose.

## 15. What happens if there is an Importer Personal Data Breach

15.1 If there is an Importer Personal Data Breach, the Importer must:

15.1.1 take reasonable steps to fix it, including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again. If the Importer is the Exporter's Processor or Sub-Processor: these steps must comply with the Exporter's instructions and the Linked Agreement and be in co-operation with the Exporter and any Third Party Controller; and


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

15.1.2 ensure that the Security Requirements continue to provide (or are changed in accordance with this IDTA so they do provide) a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

15.2 If the Importer is a Processor or Sub-Processor: if there is an Importer Personal Data Breach, the Importer must:

15.2.1 notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

15.2.1.1 a description of the nature of the Importer Personal Data Breach;

15.2.1.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;

15.2.1.3 likely consequences of the Importer Personal Data Breach;

15.2.1.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;

15.2.1.5 contact point for more information; and

15.2.1.6 any other information reasonably requested by the Exporter,

15.2.2 if it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay; and

15.2.3 assist the Exporter (and any Third Party Controller) so the Exporter (or any Third Party Controller) can inform Relevant Data Subjects or the ICO or any other relevant regulator or authority about the Importer Personal Data Breach Without Undue Delay.

15.3 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a risk to the rights or freedoms of any Relevant Data


© All rights reserved by Heiko Maniero.

Subject the Importer must notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

15.3.1 a description of the nature of the Importer Personal Data Breach;

15.3.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;

15.3.3 likely consequences of the Importer Personal Data Breach;

15.3.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;

15.3.5 contact point for more information; and

15.3.6 any other information reasonably requested by the Exporter.

If it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay.

15.4 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a high risk to the rights or freedoms of any Relevant Data Subject, the Importer must inform those Relevant Data Subjects Without Undue Delay, except in so far as it requires disproportionate effort, and provided the Importer ensures that there is a public communication or similar measures whereby Relevant Data Subjects are informed in an equally effective manner.

15.5 The Importer must keep a written record of all relevant facts relating to the Importer Personal Data Breach, which it will provide to the Exporter and the ICO on request.

This record must include the steps it takes to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Security Requirements continue to provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

## 16. Transferring on the Transferred Data

16.1 The Importer may only transfer on the Transferred Data to a third party if it is permitted to do so in Table 2: Transfer Details Table, the transfer is


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

for the Purpose, the transfer does not breach the Linked Agreement, and one or more of the following apply:

16.1.1 the third party has entered into a written contract with the Importer containing the same level of protection for Data Subjects as contained in this IDTA (based on the role of the recipient as controller or processor), and the Importer has conducted a risk assessment to ensure that the Appropriate Safeguards will be protected by that contract; or

16.1.2 the third party has been added to this IDTA as a Party; or

16.1.3 if the Importer was in the UK, transferring on the Transferred Data would comply with Article 46 UK GDPR; or

16.1.4 if the Importer was in the UK transferring on the Transferred Data would comply with one of the exceptions in Article 49 UK GDPR; or

16.1.5 the transfer is to the UK or an Adequate Country.

16.2 The Importer does not need to comply with Section 16.1 if it is transferring on Transferred Data and/or allowing access to the Transferred Data in accordance with Section 23 (Access Requests and Direct Access).

## 17. Importer's responsibility if it authorises others to perform its obligations

17.1 The Importer may sub-contract its obligations in this IDTA to a Processor or Sub-Processor (provided it complies with Section 16).

17.2 If the Importer is the Exporter's Processor or Sub-Processor: it must also comply with the Linked Agreement or be with the written consent of the Exporter.

17.3 The Importer must ensure that any person or third party acting under its authority, including a Processor or Sub-Processor, must only Process the Transferred Data on its instructions.

17.4 The Importer remains fully liable to the Exporter, the ICO and Relevant Data Subjects for its obligations under this IDTA where it has sub-contracted any obligations to its Processors and Sub-Processors, or authorised an employee or other person to perform them (and references to the Importer in this context will include references to its Processors, Sub-Processors or authorised persons).


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## 18. The right to a copy of the IDTA

18.1 If a Party receives a request from a Relevant Data Subject for a copy of this IDTA:

18.1.1 it will provide the IDTA to the Relevant Data Subject and inform the other Party, as soon as reasonably possible;

18.1.2 it does not need to provide copies of the Linked Agreement, but it must provide all the information from those Linked Agreements referenced in the Tables;

18.1.3 it may redact information in the Tables or the information provided from the Linked Agreement if it is reasonably necessary to protect business secrets or confidential information, so long as it provides the Relevant Data Subject with a summary of those redactions so that the Relevant Data Subject can understand the content of the Tables or the information provided from the Linked Agreement.

## 19. The right to Information about the Importer and its Processing

19.1 The Importer does not need to comply with this Section 19 if it is the Exporter's Processor or Sub-Processor.

19.2 The Importer must ensure that each Relevant Data Subject is provided with details of:

- the Importer (including contact details and the Importer Data Subject Contact);
- the Purposes; and
- any recipients (or categories of recipients) of the Transferred Data;

The Importer can demonstrate it has complied with this Section 19.2 if the information is given (or has already been given) to the Relevant Data Subjects by the Exporter or another party.

The Importer does not need to comply with this Section 19.2 in so far as to do so would be impossible or involve a disproportionate effort, in which case, the Importer must make the information publicly available.

19.3 The Importer must keep the details of the Importer Data Subject Contact up to date and publicly available. This includes notifying the Exporter in writing of any such changes.


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

19.4 The Importer must make sure those contact details are always easy to access for all Relevant Data Subjects and be able to easily communicate with Data Subjects in the English language Without Undue Delay.

## 20. How Relevant Data Subjects can exercise their data subject rights

20.1 The Importer does not need to comply with this Section 20 if it is the Exporter's Processor or Sub-Processor.

20.2 If an individual requests, the Importer must confirm whether it is Processing their Personal Data as part of the Transferred Data.

20.3 The following Sections of this Section 20, relate to a Relevant Data Subject's Personal Data which forms part of the Transferred Data the Importer is Processing.

20.4 If the Relevant Data Subject requests, the Importer must provide them with a copy of their Transferred Data:

20.4.1 Without Undue Delay (and in any event within one month);

20.4.2 at no greater cost to the Relevant Data Subject than it would be able to charge if it were subject to the UK Data Protection Laws;

20.4.3 in clear and plain English that is easy to understand; and

20.4.4 in an easily accessible form

together with

20.4.5 (if needed) a clear and plain English explanation of the Transferred Data so that it is understandable to the Relevant Data Subject; and

20.4.6 information that the Relevant Data Subject has the right to bring a claim for compensation under this IDTA.

20.5 If a Relevant Data Subject requests, the Importer must:

20.5.1 rectify inaccurate or incomplete Transferred Data;

20.5.2 erase Transferred Data if it is being Processed in breach of this IDTA;

20.5.3 cease using it for direct marketing purposes; and


© All rights reserved by Heiko Maniero.

20.5.4 comply with any other reasonable request of the Relevant Data Subject, which the Importer would be required to comply with if it were subject to the UK Data Protection Laws.

20.6 The Importer must not use the Transferred Data to make decisions about the Relevant Data Subject based solely on automated processing, including profiling (the "Decision-Making"), which produce legal effects concerning the Relevant Data Subject or similarly significantly affects them, except if it is permitted by Local Law and:

20.6.1 the Relevant Data Subject has given their explicit consent to such Decision-Making; or

20.6.2 Local Law has safeguards which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK; or

20.6.3 the Extra Protection Clauses provide safeguards for the Decision-Making which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK.

## 21. How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor

21.1 Where the Importer is the Exporter's Processor or Sub-Processor: If the Importer receives a request directly from an individual which relates to the Transferred Data it must pass that request on to the Exporter Without Undue Delay. The Importer must only respond to that individual as authorised by the Exporter or any Third Party Controller.

## 22. Rights of Relevant Data Subjects are subject to the exemptions in the UK Data Protection Laws

22.1 The Importer is not required to respond to requests or provide information or notifications under Sections 18, 19, 20, 21 and 23 if:

22.1.1 it is unable to reasonably verify the identity of an individual making the request; or

22.1.2 the requests are manifestly unfounded or excessive, including where requests are repetitive. In that case the Importer may


© All rights reserved by Heiko Maniero.

refuse the request or may charge the Relevant Data Subject a reasonable fee; or

22.1.3 a relevant exemption would be available under UK Data Protection Laws, were the Importer subject to the UK Data Protection Laws.

If the Importer refuses an individual's request or charges a fee under Section 22.1.2 it will set out in writing the reasons for its refusal or charge, and inform the Relevant Data Subject that they are entitled to bring a claim for compensation under this IDTA in the case of any breach of this IDTA.

How to give third parties access to Transferred Data under Local Laws

## 23. Access requests and direct access

23.1 In this Section 23 an "Access Request" is a legally binding request (except for requests only binding by contract law) to access any Transferred Data and "Direct Access" means direct access to any Transferred Data by public authorities of which the Importer is aware.

23.2 The Importer may disclose any requested Transferred Data in so far as it receives an Access Request, unless in the circumstances it is reasonable for it to challenge that Access Request on the basis there are significant grounds to believe that it is unlawful.

23.3 In so far as Local Laws allow and it is reasonable to do so, the Importer will Without Undue Delay provide the following with relevant information about any Access Request or Direct Access: the Exporter; any Third Party Controller; and where the Importer is a Controller, any Relevant Data Subjects.

23.4 In so far as Local Laws allow, the Importer must:

23.4.1 make and keep a written record of Access Requests and Direct Access, including (if known): the dates, the identity of the requestor/accessor, the purpose of the Access Request or Direct Access, the type of data requested or accessed, whether it was challenged or appealed, and the outcome; and the Transferred Data which was provided or accessed; and

23.4.2 provide a copy of this written record to the Exporter on each Review Date and any time the Exporter or the ICO reasonably requests.


© All rights reserved by Heiko Maniero.

## 24. Giving notice

24.1 If a Party is required to notify any other Party in this IDTA it will be marked for the attention of the relevant Key Contact and sent by e-mail to the e-mail address given for the Key Contact.

24.2 If the notice is sent in accordance with Section 24.1, it will be deemed to have been delivered at the time the e-mail was sent, or if that time is outside of the receiving Party's normal business hours, the receiving Party's next normal business day, and provided no notice of non-delivery or bounceback is received.

24.3 The Parties agree that any Party can update their Key Contact details by giving 14 days' (or more) notice in writing to the other Party.

## 25. General clauses

25.1 In relation to the transfer of the Transferred Data to the Importer and the Importer's Processing of the Transferred Data, this IDTA and any Linked Agreement:

25.1.1 contain all the terms and conditions agreed by the Parties; and

25.1.2 override all previous contacts and arrangements, whether oral or in writing.

25.2 If one Party made any oral or written statements to the other before entering into this IDTA (which are not written in this IDTA) the other Party confirms that it has not relied on those statements and that it will not have a legal remedy if those statements are untrue or incorrect, unless the statement was made fraudulently.

25.3 Neither Party may novate, assign or obtain a legal charge over this IDTA (in whole or in part) without the written consent of the other Party, which may be set out in the Linked Agreement.

25.4 Except as set out in Section 17.1, neither Party may sub contract its obligations under this IDTA without the written consent of the other Party, which may be set out in the Linked Agreement.

25.5 This IDTA does not make the Parties a partnership, nor appoint one Party to act as the agent of the other Party.

25.6 If any Section (or part of a Section) of this IDTA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity and


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

enforceability of any other Section (or the rest of that Section) of this IDTA.

25.7 If a Party does not enforce, or delays enforcing, its rights or remedies under or in relation to this IDTA, this will not be a waiver of those rights or remedies. In addition, it will not restrict that Party's ability to enforce those or any other right or remedy in future.

25.8 If a Party chooses to waive enforcing a right or remedy under or in relation to this IDTA, then this waiver will only be effective if it is made in writing. Where a Party provides such a written waiver:

25.8.1 it only applies in so far as it explicitly waives specific rights or remedies;

25.8.2 it shall not prevent that Party from exercising those rights or remedies in the future (unless it has explicitly waived its ability to do so); and

25.8.3 it will not prevent that Party from enforcing any other right or remedy in future.

What happens if there is a breach of this IDTA?

## 26. Breaches of this IDTA

26.1 Each Party must notify the other Party in writing (and with all relevant details) if it:

26.1.1 has breached this IDTA; or

26.1.2 it should reasonably anticipate that it may breach this IDTA, and provide any information about this which the other Party reasonably requests.

26.2 In this IDTA "Significant Harmful Impact" means that there is more than a minimal risk of a breach of the IDTA causing (directly or indirectly) significant damage to any Relevant Data Subject or the other Party.

## 27. Breaches of this IDTA by the Importer

27.1 If the Importer has breached this IDTA, and this has a Significant Harmful Impact, the Importer must take steps Without Undue Delay to end the Significant Harmful Impact, and if that is not possible to reduce the Significant Harmful Impact as much as possible.


© All rights reserved by Heiko Maniero.

27.2 Until there is no ongoing Significant Harmful Impact on Relevant Data Subjects:

27.2.1 the Exporter must suspend sending Transferred Data to the Importer;

27.2.2 If the Importer is the Exporter's Processor or Sub-Processor: if the Exporter requests, the importer must securely delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter); and

27.2.3 if the Importer has transferred on the Transferred Data to a third party receiver under Section 16, and the breach has a Significant Harmful Impact on Relevant Data Subject when it is Processed by or on behalf of that third party receiver, the Importer must:

27.2.3.1 notify the third party receiver of the breach and suspend sending it Transferred Data; and

27.2.3.2 if the third party receiver is the Importer's Processor or Sub-Processor: make the third party receiver securely delete all Transferred Data being Processed by it or on its behalf, or securely return it to the Importer (or a third party named by the Importer).

27.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Exporter must end this IDTA under Section 30.1.

## 28. Breaches of this IDTA by the Exporter

28.1 If the Exporter has breached this IDTA, and this has a Significant Harmful Impact, the Exporter must take steps Without Undue Delay to end the Significant Harmful Impact and if that is not possible to reduce the Significant Harmful Impact as much as possible.

28.2 Until there is no ongoing risk of a Significant Harmful Impact on Relevant Data Subjects, the Exporter must suspend sending Transferred Data to the Importer.

28.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Importer must end this IDTA under Section 30.1.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## 29. How to end this IDTA without there being a breach

29.1 The IDTA will end:

29.1.1 at the end of the Term stated in Table 2: Transfer Details; or

29.1.2 if in Table 2: Transfer Details, the Parties can end this IDTA by providing written notice to the other: at the end of the notice period stated;

29.1.3 at any time that the Parties agree in writing that it will end; or

29.1.4 at the time set out in Section 29.2.

29.2 If the ICO issues a revised Approved IDTA under Section 5.4, if any Party selected in Table 2 "Ending the IDTA when the Approved IDTA changes", will as a direct result of the changes in the Approved IDTA have a substantial, disproportionate and demonstrable increase in:

29.2.1 its direct costs of performing its obligations under the IDTA; and/or

29.2.2 its risk under the IDTA,

and in either case it has first taken reasonable steps to reduce that cost or risk so that it is not substantial and disproportionate, that Party may end the IDTA at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved IDTA.

## 30. How to end this IDTA if there is a breach

30.1 A Party may end this IDTA immediately by giving the other Party written notice if:

30.1.1 the other Party has breached this IDTA and this has a Significant Harmful Impact. This includes repeated minor breaches which taken together have a Significant Harmful Impact, and

30.1.1.1 the breach can be corrected so there is no Significant Harmful Impact, and the other Party has failed to do so Without Undue Delay (which cannot be more than 14 days of being required to do so in writing); or


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

30.1.1.2 the breach and its Significant Harmful Impact cannot be corrected;

30.1.2 the Importer can no longer comply with Section 8.3, as there are Local Laws which mean it cannot comply with this IDTA and this has a Significant Harmful Impact.

## 31. What must the Parties do when the IDTA ends?

31.1 If the parties wish to bring this IDTA to an end or this IDTA ends in accordance with any provision in this IDTA, but the Importer must comply with a Local Law which requires it to continue to keep any Transferred Data then this IDTA will remain in force in respect of any retained Transferred Data for as long as the retained Transferred Data is retained, and the Importer must:

31.1.1 notify the Exporter Without Undue Delay, including details of the relevant Local Law and the required retention period;

31.1.2 retain only the minimum amount of Transferred Data it needs to comply with that Local Law, and the Parties must ensure they maintain the Appropriate Safeguards, and change the Tables and Extra Protection Clauses, together with any TRA to reflect this; and

31.1.3 stop Processing the Transferred Data as soon as permitted by that Local Law and the IDTA will then end and the rest of this Section 29 will apply.

31.2 When this IDTA ends (no matter what the reason is):

31.2.1 the Exporter must stop sending Transferred Data to the Importer; and

31.2.2 if the Importer is the Exporter's Processor or Sub-Processor: the Importer must delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter), as instructed by the Exporter;

31.2.3 if the Importer is a Controller and/or not the Exporter's Processor or Sub-Processor: the Importer must securely delete all Transferred Data.

31.2.4 the following provisions will continue in force after this IDTA ends (no matter what the reason is):


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

- **Section 1** (This IDTA and Linked Agreements);
- **Section 2** (Legal Meaning of Words);
- **Section 6** (Understanding this IDTA);
- **Section 7** (Which laws apply to this IDTA);
- **Section 10** (The ICO);
- Sections 11.1 and 11.4 (Exporter's obligations);
- Sections 12.1.2, 12.1.3, 12.1.4, 12.1.5 and 12.1.6 (General Importer obligations);
- Section 13.1 (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 17** (Importer's responsibility if it authorised others to perform its obligations);
- **Section 24** (Giving notice);
- **Section 25** (General clauses);
- **Section 31** (What must the Parties do when the IDTA ends);
- **Section 32** (Your liability);
- **Section 33** (How Relevant Data Subjects and the ICO may bring legal claims);
- **Section 34** (Courts legal claims can be brought in);
- **Section 35** (Arbitration); and
- **Section 36** (Legal Glossary).

How to bring a legal claim under this IDTA

## 32. Your liability

32.1 The Parties remain fully liable to Relevant Data Subjects for fulfilling their obligations under this IDTA and (if they apply) under UK Data Protection Laws.

32.2 Each Party (in this Section, "Party One") agrees to be fully liable to Relevant Data Subjects for the entire damage suffered by the Relevant Data Subject, caused directly or indirectly by:

32.2.1 Party One's breach of this IDTA; and/or


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

32.2.2 where Party One is a Processor, Party One's breach of any provisions regarding its Processing of the Transferred Data in the Linked Agreement;

32.2.3 where Party One is a Controller, a breach of this IDTA by the other Party if it involves Party One's Processing of the Transferred Data (no matter how minimal)

in each case unless Party One can prove it is not in any way responsible for the event giving rise to the damage.

32.3 If one Party has paid compensation to a Relevant Data Subject under Section 32.2, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party's responsibility for the damage, so that the compensation is fairly divided between the Parties.

32.4 The Parties do not exclude or restrict their liability under this IDTA or UK Data Protection Laws, on the basis that they have authorised anyone who is not a Party (including a Processor) to perform any of their obligations, and they will remain responsible for performing those obligations.

## 33. How Relevant Data Subjects and the ICO may bring legal claims

33.1 The Relevant Data Subjects are entitled to bring claims against the Exporter and/or Importer for breach of the following (including where their Processing of the Transferred Data is involved in a breach of the following by either Party):

- **Section 1** (This IDTA and Linked Agreements);
- **Section 3** (You have provided all the information required by Part one: Tables and Part two: Extra Protection Clauses);
- **Section 8** (The Appropriate Safeguards);
- **Section 9** (Reviews to ensure the Appropriate Safeguards continue);
- **Section 11** (Exporter's obligations);
- **Section 12** (General Importer Obligations);
- **Section 13** (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 14** (Importer's obligations to comply with key data protection laws);
- **Section 15** (What happens if there is an Importer Personal Data Breach);


© All rights reserved by Heiko Maniero.

- **Section 16** (Transferring on the Transferred Data);
- **Section 17** (Importer's responsibility if it authorises others to perform its obligations);
- **Section 18** (The right to a copy of the IDTA);
- **Section 19** (The Importer's contact details for the Relevant Data Subjects);
- **Section 20** (How Relevant Data Subjects can exercise their data subject rights);
- **Section 21** (How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor);
- **Section 23** (Access Requests and Direct Access);
- **Section 26** (Breaches of this IDTA);
- **Section 27** (Breaches of this IDTA by the Importer);
- **Section 28** (Breaches of this IDTA by the Exporter);
- **Section 30** (How to end this IDTA if there is a breach);
- **Section 31** (What must the Parties do when the IDTA ends); and
- any other provision of the IDTA which expressly or by implication benefits the Relevant Data Subjects.

33.2 The ICO is entitled to bring claims against the Exporter and/or Importer for breach of the following Sections: Section 10 (The ICO), Sections 11.1 and 11.2 (Exporter's obligations), Section 12.1.6 (General Importer obligations) and Section 13 (Importer's obligations if it is subject to UK Data Protection Laws).

33.3 No one else (who is not a Party) can enforce any part of this IDTA (including under the Contracts (Rights of Third Parties) Act 1999).

33.4 The Parties do not need the consent of any Relevant Data Subject or the ICO to make changes to this IDTA, but any changes must be made in accordance with its terms.

33.5 In bringing a claim under this IDTA, a Relevant Data Subject may be represented by a not-for-profit body, organisation or association under the same conditions set out in Article 80(1) UK GDPR and sections 187 to 190 of the Data Protection Act 2018.


© All rights reserved by Heiko Maniero.

## 34. Courts legal claims can be brought in

34.1 The courts of the UK country set out in Table 2: Transfer Details have non-exclusive jurisdiction over any claim in connection with this IDTA (including non-contractual claims).

34.2 The Exporter may bring a claim against the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.

34.3 The Importer may only bring a claim against the Exporter in connection with this IDTA (including non-contractual claims) in the courts of the UK country set out in the Table 2: Transfer Details

34.4 Relevant Data Subjects and the ICO may bring a claim against the Exporter and/or the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.

34.5 Each Party agrees to provide to the other Party reasonable updates about any claims or complaints brought against it by a Relevant Data Subject or the ICO in connection with the Transferred Data (including claims in arbitration).

## 35. Arbitration

35.1 Instead of bringing a claim in a court under Section 34, any Party, or a Relevant Data Subject may elect to refer any dispute arising out of or in connection with this IDTA (including non-contractual claims) to final resolution by arbitration under the Rules of the London Court of International Arbitration, and those Rules are deemed to be incorporated by reference into this Section 35.

35.2 The Parties agree to submit to any arbitration started by another Party or by a Relevant Data Subject in accordance with this Section 35.

35.3 There must be only one arbitrator. The arbitrator (1) must be a lawyer qualified to practice law in one or more of England and Wales, or Scotland, or Northern Ireland and (2) must have experience of acting or advising on disputes relating to UK Data Protection Laws.

35.4 London shall be the seat or legal place of arbitration. It does not matter if the Parties selected a different UK country as the 'primary place for legal claims to be made' in Table 2: Transfer Details.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

35.5 The English language must be used in the arbitral proceedings.

35.6 English law governs this Section 35. This applies regardless of whether or not the parties selected a different UK country's law as the 'UK country's law that governs the IDTA' in Table 2: Transfer Details.

## 36. Legal Glossary

| Word or Phrase | Legal definition (this is how this word or phrase must be interpreted in the IDTA) |
|---|---|
| Access Request | As defined in Section 23, as a legally binding request (except for requests only binding by contract law) to access any Transferred Data. |
| Adequate Country | A third country, or:<br>• a territory;<br>• one or more sectors or organisations within a third country;<br>• an international organisation;<br>which the Secretary of State has specified by regulations provides an adequate level of protection of Personal Data in accordance with Section 17A of the Data Protection Act 2018. |
| Appropriate Safeguards | The standard of protection over the Transferred Data and of the Relevant Data Subject's rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR. |
| Approved IDTA | The template IDTA A1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4. |


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

| Word or Phrase | Legal definition (this is how this word or phrase must be interpreted in the IDTA) |
|---|---|
| Commercial Clauses | The commercial clauses set out in Part three. |
| Controller | As defined in the UK GDPR. |
| Damage | All material and non-material loss and damage. |
| Data Subject | As defined in the UK GDPR. |
| Decision-Making | As defined in Section 20.6, as decisions about the Relevant Data Subjects based solely on automated processing, including profiling, using the Transferred Data. |
| Direct Access | As defined in Section 23 as direct access to any Transferred Data by public authorities of which the Importer is aware. |
| Exporter | The exporter identified in Table 1: Parties & Signature. |
| Extra Protection Clauses | The clauses set out in Part two: Extra Protection Clauses. |
| ICO | The Information Commissioner. |
| Importer | The importer identified in Table 1: Parties & Signature. |
| Importer Data Subject Contact | The Importer Data Subject Contact identified in Table 1: Parties & Signature, which may be updated in accordance with Section 19. |


© All rights reserved by Heiko Maniero.

| Word or Phrase | Legal definition (this is how this word or phrase must be interpreted in the IDTA) |
|---|---|
| Importer Information | As defined in Section 8.3.1, as all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including for the Exporter to carry out any TRA. |
| Importer Personal Data Breach | A 'personal data breach' as defined in UK GDPR, in relation to the Transferred Data when Processed by the Importer. |
| Linked Agreement | The linked agreements set out in Table 2: Transfer Details (if any). |
| Local Laws | Laws which are not the laws of the UK and which bind the Importer. |
| Mandatory Clauses | Part four: Mandatory Clauses of this IDTA. |
| Notice Period | As set out in Table 2: Transfer Details. |
| Party/Parties | The parties to this IDTA as set out in Table 1: Parties & Signature. |
| Personal Data | As defined in the UK GDPR. |
| Personal Data Breach | As defined in the UK GDPR. |
| Processing | As defined in the UK GDPR. |


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

| Word or Phrase | Legal definition (this is how this word or phrase must be interpreted in the IDTA) |
|---|---|
| | When the IDTA refers to Processing by the Importer, this includes where a third party Sub-Processor of the Importer is Processing on the Importer's behalf. |
| Processor | As defined in the UK GDPR. |
| Purpose | The 'Purpose' set out in Table 2: Transfer Details, including any purposes which are not incompatible with the purposes stated or referred to. |
| Relevant Data Subject | A Data Subject of the Transferred Data. |
| Restricted Transfer | A transfer which is covered by Chapter V of the UK GDPR |
| Review Dates | The review dates or period for the Security Requirements set out in Table 2: Transfer Details, and any review dates set out in any revised Approved IDTA. |
| Significant Harmful Impact | As defined in Section 26.2 as where there is more than a minimal risk of the breach causing (directly or indirectly) significant harm to any Relevant Data Subject or the other Party. |
| Special Category Data | As described in the UK GDPR, together with criminal conviction or criminal offence data. |
| Start Date | As set out in Table 1: Parties and signature. |


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

| Word or Phrase | Legal definition (this is how this word or phrase must be interpreted in the IDTA) |
|---|---|
| Sub-Processor | A Processor appointed by another Processor to Process Personal Data on its behalf.<br>This includes Sub-Processors of any level, for example a Sub-Sub-Processor. |
| Tables | The Tables set out in Part one of this IDTA. |
| Term | As set out in Table 2: Transfer Details. |
| Third Party Controller | The Controller of the Transferred Data where the Exporter is a Processor or Sub-Processor<br>If there is not a Third Party Controller this can be disregarded. |
| Transfer Risk Assessment or TRA | A risk assessment in so far as it is required by UK Data Protection Laws to demonstrate that the IDTA provides the Appropriate Safeguards |
| Transferred Data | Any Personal Data which the Parties transfer, or intend to transfer under this IDTA, as described in Table 2: Transfer Details |
| UK Data Protection Laws | All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018. |
| UK GDPR | As defined in Section 3 of the Data Protection Act 2018. |
| Without Undue Delay | Without undue delay, as that phase is interpreted in the UK GDPR. |


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

Information Commissioner's Office

# Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

## International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

**VERSION B1.0, in force 21 March 2022**

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

## Part 1: Tables

### Table 1: Parties

| | | |
|---|---|---|
| **Start date** | see Main-Agreement | |
| **The Parties** | **Exporter (who sends the Restricted Transfer)** | **Importer (who receives the Restricted Transfer)** |
| **Parties' details** | Full legal name:<br>see Main-Agreement<br>Trading name (if different):<br>if applicable, see Main-Agreement<br>Main address (if a company registered address): | Full legal name:<br>see Main-Agreement<br>Trading name (if different):<br>if applicable, see Main-Agreement<br>Main address (if a company registered address): |


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

| | | |
|---|---|---|
| | see Main-Agreement<br><br>Official registration number (if any) (company number or similar identifier):<br>if applicable, see Main-Agreement | see Main-Agreement<br><br>Official registration number (if any) (company number or similar identifier):<br>if applicable, see Main-Agreement |
| **Key Contact** | Full Name (optional):<br>if applicable, see Main-Agreement<br>Job Title:<br>if applicable, see Main-Agreement<br>Contact details including email:<br>if applicable, see Main-Agreement | Full Name (optional):<br>if applicable, see Main-Agreement<br>Job Title:<br>if applicable, see Main-Agreement<br>Contact details including email:<br>if applicable, see Main-Agreement |
| **Signature (if required for the purposes of Section 2)** | if applicable, see Main-Agreement | if applicable, see Main-Agreement |

Table 2: Selected SCCs, Modules and Selected Clauses

| | |
|---|---|
| **Addendum EU SCCs** | The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:<br>Date: see above, Additional conditions for compliance with the General Data Protection Regulation (GDPR), UK-GDPR and Confidentiality of Trade Secrets<br>Reference (if any): if applicable, see Main-Agreement<br>Other identifier (if any): if applicable, see Main-Agreement |


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

### Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

| |
|---|
| Annex 1A: List of Parties: see APPENDIX 7 – LIST OF PARTIES |
| Annex 1B: Description of Transfer: see APPENDIX 8 – DESCRIPTION OF THE PROCESSING OR THE TRANSFER |
| Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES |
| Annex III: List of Sub processors (Modules 2 and 3 only): if applicable, separate list of our sub-processors must be requested separately |

### Table 4: Ending this Addendum when the Approved Addendum Changes

| | |
|---|---|
| **Ending this Addendum when the Approved Addendum changes** | Which Parties may end this Addendum as set out in Section 19:<br>neither Party |

## Part 2: Mandatory Clauses

### Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

### Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

| | |
|---|---|
| Addendum | This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs. |
| Addendum EU SCCs | The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information. |
| Appendix Information | As set out in Table 3. |
| Appropriate Safeguards | The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR. |
| Approved Addendum | The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18. |
| Approved EU SCCs | The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021. |
| ICO | The Information Commissioner. |
| Restricted Transfer | A transfer which is covered by Chapter V of the UK GDPR. |
| UK | The United Kingdom of Great Britain and Northern Ireland. |


© All rights reserved by Heiko Maniero.

| | |
|---|---|
| UK Data Protection Laws | All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018. |
| UK GDPR | As defined in section 3 of the Data Protection Act 2018. |

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

### Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.


© All rights reserved by Heiko Maniero.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

### Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";


© All rights reserved by Heiko Maniero.

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

## Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may


© All rights reserved by Heiko Maniero.

end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

# Data Processing Agreement for the United Kingdom

This Data Processing Agreement is concluded on the same date as the Services Agreement (as defined below) and is concluded by and between

(1) the **Controller**, named with its Company details as a Party in the Services Agreement; and

(2) the **Processor**, named with its Company details as a Party in the Services Agreement.

(each a **Party** and together the **Parties**)

## 1. Preamble

The Processor is a provider of professional services (**Services**). The Parties entered into an Agreement which describes the Services provided by the Processor to or on behalf of the Controller in more detail (**Services Agreement**).

The Parties have agreed to enter into this Agreement in relation to the Processing of Personal Data by the Processor in the course of providing the Services. The terms of this Agreement are intended to apply in addition to and not in substitution of the terms of the Services Agreement.

## 2. Definitions and interpretation

2.1. In this Agreement the terms **Controller**, **Processor**, **Personal Data**, **Special Categories Of Personal Data**, **Processing**, **Pseudonymisation, Encryption, Personal Data Breach**, **Supervisory Authority, Categories of Data Subject, Types of Personal Data, Scope,** and **Purpose** shall have the meanings given to them by Data Protection Legislation (as defined below).

2.2. In addition to those terms, the following definitions shall apply:

**Affiliates** means in relation to the Controller, each and any business entity or undertaking under the Controller's direction and in relation to either Party, any entity that directly or indirectly controls, is controlled by or is under common control with that Party (where control is defined as the direct or indirect ownership or control of more than 50% of the shares or other equity securities, of an entity or of the power to direct or significantly influence the direction of the management, policies and voting interests of an entity whether by contract or otherwise).

**Authorised Person** means the Person(s) be nominated by the Controller from time to time in writing.

**Business Day** means a day other than a Saturday, Sunday or public holiday in England when banks in the City of London are generally open for business.

**Data Protection Legislation** means the UK-GDPR and any national laws, regulations and secondary legislation in the UK; all applicable laws and regulations relating to the Processing of Personal Data and privacy; and where applicable, the guidance and codes of practice issued

 © All rights reserved by Heiko Maniero.

by the UK Information Commissioner's Office (ICO) or any other Supervisory Authority (and the equivalent of any of the foregoing in any relevant jurisdiction).

**EEA** means the European Economic Area including, for the Purposes of this Agreement, the UK.

**Personnel** means in relation to a Party, those of its employees, workers, agents, consultants, contractors, sub-contractors, representatives or other Persons employed or engaged by that Party on whatever terms.

**Sub-Processor** means any entity (whether or not an Affiliate of the Processor, but excluding the Processor's Personnel) appointed by or on behalf of the Processor to process Personal Data on behalf of the Controller under this Agreement.

2.3. Clause, schedule and paragraph headings shall not affect the interpretation of this Agreement.

2.4. A **Person** includes a natural Person, corporate or unincorporated body (whether or not having separate legal personality). A reference to a **Company** shall include any Company, corporation or other body corporate, wherever and however incorporated or established.

2.5. Unless the context otherwise requires, any reference to a Party shall be deemed to include that Party's Affiliates and where an obligation is imposed on a Party under this Agreement, it will be required to procure compliance with such obligation by that Party's Affiliates where appropriate.

2.6. Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular and a reference to one gender shall include a reference to the other genders.

2.7. A reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time and shall include all subordinate legislation made from time to time under that statute or statutory provision.

2.8. Unless the context otherwise requires, a reference to writing or written includes email but not fax.

2.9. Any words following the terms **including**, **include**, **in particular** or **for example** or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.

2.10. In the event of any ambiguity or inconsistency between the terms of this Agreement (including its Schedules) and the terms of the Services Agreement, the terms of this Agreement shall take precedence.

## 3. Roles and responsibilities

**Schedule 1** sets out the Scope and Purpose of the Processing of Personal Data by the Processor, the duration of the Processing and the Types of Personal Data and Categories of Data Subject concerned.

## 4. Compliance with Data Protection Legislation


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

4.1. Each Party shall comply with all applicable requirements of the Data Protection Legislation. This clause is in addition to, and does not relieve any Party from complying with, a Party's obligations under the Data Protection Legislation.

4.2. Without prejudice to the generality of this clause, the Controller will ensure that it has all necessary appropriate consents and notices in place to enable the lawful transfer to and Processing of the Personal Data by the Processor in connection with the performance by the Processor of its obligations under the Services Agreement and this Agreement.

4.3. To the extent within the Controller's control having regard to the Processor's obligations under the Services Agreement and this Agreement, the Controller shall be responsible for the accuracy and quality of the Personal Data processed by the Processor under this Agreement.

4.4. The Processor shall have an ongoing obligation throughout the duration of the Services Agreement to identify and report to the Controller:

4.4.1. best practice techniques relating to the Processing of Personal Data under this Agreement; and

4.4.2. the emergence of new and evolving technologies which could improve the availability, confidentiality and/or integrity of the Processing of Personal Data under this Agreement.

## 5. Processing of Personal Data by the Processor

5.1. The Processor shall only process Personal Data:

5.1.1. for the Purposes expressly specified in the Services Agreement;

5.1.2. otherwise in accordance with the Controller's documented instructions as given by an Authorised Person,

unless the Processor is required by any applicable law to which the Processor is subject, to process Personal Data for any other Purposes (in which case the Processor shall, to the extent permitted by such applicable law, inform the Controller of such legal requirement before undertaking such Processing).

5.2. The Controller shall ensure that any Authorised Person is fully aware of the terms of the Services Agreement and this Agreement such that the Processor shall be entitled to assume that any instruction given by any Authorised Person to the Processor shall be given with the Controller's full authority. The Controller further acknowledges and agrees that the Processor shall not be under any duty to investigate the completeness, accuracy or sufficiency of any instructions given to it by any Authorised Person.

## 6. Processor's Personnel

6.1. The Processor shall take reasonable steps to ensure the reliability of those of its Personnel who may have access to any Personal Data.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

6.2. The Processor shall ensure that those of its Personnel authorised to process Personal Data under this Agreement:

6.2.1. are aware of the confidential nature of the Personal Data;
6.2.2. are bound by obligations of confidentiality by virtue of a written Agreement between the Processor and such Persons; and
6.2.3. have received appropriate training on the handling of Personal Data and on their responsibilities in relation to the Processing of Personal Data.

6.3. The Processor shall implement appropriate technical and organisational measures to ensure that those of its Personnel only have access to such part or parts of the Personal Data as is strictly necessary for the performance of their duties and obligations.

## 7. Security of the Processing

7.1. Taking into account the state of the art, the costs of implementation and 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 the data subjects the Processor shall, in relation to the Processing of Personal Data under this Agreement, implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate:

7.1.1. the Pseudonymisation and Encryption of Personal Data;
7.1.2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
7.1.3. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
7.1.4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

7.2. In assessing the appropriate level of security, the Processor shall take into account any risks that are presented by the Processing, in particular, from a Personal Data Breach.

7.3. The Processor shall implement the specific security measures set out in **Schedule 2**. The Processor may add to, amend, or replace the specific security measures for security reasons and shall notify the Controller in writing where it has done so.

## 8. Sub-Processors

8.1. The Controller hereby authorises the Processor to appoint Sub-Processors (**General Written Authorisation**). The Processor shall name all its Sub-Processors to the Controller prior to initiation of Processing.

8.2. With respect to each Sub-Processor appointed by the Processor under General Written Authorisation, the Processor shall:

8.2.1. undertake appropriate due diligence prior to the Processing of Personal Data by such Sub-Processor to ensure that it is capable of providing the level of protection for Personal Data required by the terms of the Services Agreement and this Agreement;


© All rights reserved by Heiko Maniero.

8.2.2. enter into a written Agreement with the Sub-Processor incorporating terms which are substantially similar (and no less onerous) than those set out in this Agreement and which meets the requirements stipulated in article 28(3) of the UK-GDPR; and

8.2.3. as between the Controller and the Processor, remain fully liable to the Controller for all acts or omissions of such Sub-Processor as though they were its own.

8.3. To the extent that the Processor has already appointed any Sub-Processors prior to the Processing of any Personal Data under this Agreement, the Processor shall ensure that its obligations under clause 8.2 are met as soon as practicable.

8.4. Where the Processor proposes any changes concerning the addition or replacement of any Sub-Processor, it shall notify the Controller in writing as soon as reasonably practicable prior to implementing such change specifying:

8.4.1. the name of any Sub-Processor which it proposes to add or replace;
8.4.2. the Processing activity or activities affected by the proposed change;
8.4.3. the reasons for the proposed change; and
8.4.4. the proposed date for implementation of the change.

8.5. If within thirty (30) days of receipt of a notice under clause 8.4 the Controller (acting reasonably and in good faith) notifies the Processor in writing of any objections to the proposed change, the Parties shall use their respective reasonable endeavours to resolve the Controller's objections. Where such resolution cannot be agreed within thirty (30) days of the Processor's receipt of the Controller's objections (or such longer period as the Parties may agree in writing) the Controller may, notwithstanding the terms of the Services Agreement, serve written notice on the Processor to terminate the Services Agreement (to the extent that the provision of the Services is or would be affected by the proposed change).

8.6. The Processor shall, upon the Controller's request, provide the Controller with copies of any Agreements between the Processor and its Sub-Processors (which may be redacted to remove information which is confidential to the Processor and/or its Sub-Processors and which is not relevant to the terms of this Agreement).

## 9. Rights of data subjects

9.1. Taking into account the nature of the Processing, the Processor shall assist the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights under the Data Protection Legislation.

9.2. Without prejudice to the generality of clause 9.1, the Processor shall implement measures intended to uphold the rights of data subjects.

9.3. The Processor shall:

9.3.1. promptly and in any case within one (1) Business Day] notify the Controller if it (or any of its Sub-Processors) receives a request from a data subject under the Data


© All rights reserved by Heiko Maniero.

Protection Legislation in respect of any Personal Data processed by the Processor under the terms of the Services Agreement or this Agreement; and

9.3.2. give to the Controller its full co-operation and assistance in relation to any request made by a data subject to have access to their Personal Data.

## 10. Notification of Personal Data Breaches

10.1. The Processor shall notify the Controller without undue delay after becoming aware of any Personal Data Breach affecting the Personal Data processed by the Processor under this Agreement, providing sufficient information to enable the Controller to evaluate the impact of such Personal Data Breach and to meet any obligations on the Controller to report the Personal Data Breach to a Supervisory Authority and/or notify the affected data subjects in accordance with the Data Protection Legislation.

10.2. The Processor shall provide the Controller with such assistance as the Controller may reasonably request and take such reasonable commercial steps as the Controller may request in order to evaluate, investigate, mitigate and remediate any Personal Data Breach (including, where applicable, communicating any Personal Data Breach to affected data subjects).

## 11. Data Protection Impact Assessments and Prior Consultation

The Processor shall provide the Controller with such assistance as the Controller may reasonably request with any data protection (or privacy) impact assessments and prior consultation with any Supervisory Authority or other competent authorities which the Controller considers necessary pursuant to Articles 35 and 36 of the UK-GDPR respectively. The Processor's assistance shall, in each case, be limited to the Processing of Personal Data under this Agreement.

## 12. Obligations upon expiry or termination of the Services Agreement

12.1. Notwithstanding the Processor's obligations under the Services Agreement following its expiry or termination, the Processor shall promptly and in any event within thirty (30) days of the expiry or termination of the Services Agreement, at the Controller's option (given by any Authorised Person) either delete or return (in such format and on such media or by such means as the Parties shall agree in writing) all copies of the Personal Data processed by the Processor and/or its Sub-Processors on behalf of the Controller under this Agreement.

12.2. Where the Controller has instructed the Processor to delete the Personal Data under clause 12.1, the Processor shall do so in accordance with best industry practice for the reliable and secure deletion of data for the secure destruction of confidential material.

12.3. The Processor (and those of its Sub-Processors, as appropriate) may retain a copy of the Personal Data processed by it under this Agreement to the extent required by any applicable law to which the Processor (or any Sub-Processor) is subject and only for such period as shall be required by such applicable law. Where applicable, the Processor shall notify the Controller of such requirement and shall ensure that such Personal Data are kept confidential and not processed for any other Purpose.


© All rights reserved by Heiko Maniero.

12.4. The Controller may require the Processor to provide a written certificate confirming that it has complied with its obligations under this clause 12.

## 13. Record-keeping requirements and audit rights

13.1. The Processor shall maintain a record of all categories of processing activities carried out by it on behalf of the Controller under this Agreement in accordance with Data Protection Legislation (**Processing Records**).

13.2. The Processor shall permit the Controller, any Authorised Person or any other auditor mandated by the Controller, on reasonable notice and during the Processor's normal business hours (but without notice, in the case of any reasonably suspected breach of this clause 13) to:

13.2.1. gain access to, and take copies of, the Processing Records and any other information held at the Processor's premises; and
13.2.2. inspect all Processing Records, documents and electronic data and the Processor's systems, facilities and equipment,

for the Purpose of auditing and certifying the Processor's compliance with its obligations under this Agreement. Such audit rights may be exercised only once in any calendar year during the term of the Services Agreement and for a period of three years following the expiry or termination of the Services Agreement.

13.3. The Processor shall give all necessary assistance to the conduct of any audits under clause 13.2.

13.4. The Processor further agrees that it shall provide the Controller with such assistance as it may reasonably request in connection with any compulsory or voluntary audit or inspection by a Supervisory Authority or other competent authority.

13.5. The Processor shall immediately inform the Controller if, in its opinion, any instruction infringes the Data Protection Legislation.

## 14. Transfers of Personal Data outside of the EEA

14.1. For the Purposes of this clause 14, the **Transfer of any Personal Data** shall include:

14.1.1. storing Personal Data on servers located or co-located outside the EEA;
14.1.2. appointing any Sub-Processor which is located outside the EEA (in accordance with clause 8; or
14.1.3. granting access rights to any of the Processor's Personnel who are located outside the EEA.

14.2. The Processor shall not transfer any Personal Data processed under this Agreement outside of the EEA except with the Controller's prior written consent and provided that the Controller is satisfied that the following conditions have been met:


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

14.2.1. the Controller, the Processor and/or any Sub-Processor (as appropriate) have (1) the International Data Transfer Agreement (published by the ICO) or (2) the International Data Transfer Addendum to the European Commission's Standard Contractual Clauses for International Data Transfers (published by the ICO) and the Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council or Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council) in place;

14.2.2. the data subject has enforceable rights and effective legal remedies in relation to the Processing of Personal Data relating to them; and

14.2.3. the Processor and/or Sub-Processor (as appropriate) complies with its obligations under the Data Protection Legislation by providing an adequate level of protection for any Personal Data that are transferred.

## 15. General provisions

15.1. Term and termination: Except in respect of any provision of this Agreement that expressly or by implication is intended come into or continue in force on or after the expiry or termination of the Services Agreement, this Agreement shall be coterminous with the Services Agreement.

15.2. Third Party rights: A Person who is not a Party to this Agreement shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any terms of this Agreement.

15.3. Severance

15.3.1. If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this clause shall not affect the validity and enforceability of the rest of this Agreement.

15.3.2. If any provision or part-provision of this Agreement is invalid, illegal or unenforceable, the Parties shall negotiate in good faith to amend such provision so that, as amended, it is legal, valid and enforceable, and, to the greatest extent possible, achieves the intended commercial result of the original provision.

15.4. Variation: Except as expressly provided in this Agreement, no variation of this Agreement shall be effective unless it is in writing and signed by the Parties (or their authorised representatives).

15.5. Governing law: This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with English law.


© All rights reserved by Heiko Maniero.

15.6. Jurisdiction: Each Party irrevocably agrees that the English courts shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims).


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## Schedule 1 – Summary of the Processing activities

1. Processing by the Processor

   a. Scope of the Processing

      See Services Agreement

   b. Purpose of the Processing

      See Services Agreement

   c. Duration of the Processing

      Duration of Services Agreement

2. Types of Personal Data

   Customer data, data of potential customers, employee data, data of business partners, supplier data.

3. Categories of Data Subject

   Customers, potential customers, employees, business partners, suppliers.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

## Schedule 2 – Specific security measures

See APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

# CCPA-CPRA CONTRACTOR AGREEMENT

This CCPA-CPRA Contractor Agreement is concluded on the same date as the Services Agreement (as defined below) and is concluded by and between

(1) the **Business**, named with its contact details as a Party in the Services Agreement; and

(2) the **Contractor**, named with its contact details as a Party in the Services Agreement.

For the purpose of this **Agreement** the term **Contractor** shall include an **Independent Contractor** and/or a **Service Provider** and/or a **Third Party** as defined by CCPA where required to include such parties and/or to allow the conclusion of this Agreement with them as contractual partners.

(each a **Party** and together the **Parties**)

## 1. Preamble

1.1. The Contractor is a provider of professional Services (**Services**). The Parties entered into an Agreement which describes the Services provided by the Contractor to or on behalf of the Business in more detail (**Services Agreement**).

1.2. The Parties have agreed to enter into this Agreement in relation to the Processing of Personal Information by the Contractor in the course of providing the Services. The terms of this Agreement are intended to apply in addition to and not in substitution of the terms of the Services Agreement.

## 2. Definitions and interpretation

2.1. In this Agreement, in CCPA related written or verbal communication, in the Services Agreement and in any of its amendments the terms **Advertising and Marketing, Aggregate Consumer Information, Biometric Information, Business, Business Associate, Business Controller Information, Business Purpose, Collected, Collection, Collects, Commercial Credit Reporting Agency, Commercial Purposes, Common Branding, Consent, Consumer, Consumer Privacy Fund, Contractor, Control, Controlled, Covered Person, Cross-Context Behavioral Advertising, Dark Pattern, Deidentified, Designated Methods For Submitting Requests, Device, Director, Family, Fraudulent Concealment, Health Care Operations, Homepage, Household, Identifiable Private Information, Independent Contractor, Individually Identifiable Health Information, Infer, Inference, Intentionally Interacts, Management Employee, Medical Information, Nonpersonalized Advertising, Officer, Owner, Ownership Information, Patient Information, Payment, Person, Personal Information, Precise Geolocation, Processing, Profiling, Protected Health Information, Provider Of Health Care, Pseudonymization, Pseudonymize, Publicly Available, Reidentify, Research, Right To Opt-Out, Sale, Security and Integrity, Sell, Selling,**


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

**Sensitive Personal Information, Service, Services, Share, Shared, Sharing, Sold, Specific Pieces Of Information, Specific Pieces Of Information Obtained From The Consumer, Third Party, Treatment, Unique Identifier, Unique Personal Identifier, Vehicle Information, Verifiable Consumer Request, Vessel Dealer, Vessel Information** and **all other terms defined by or under Data Protection Legislation** shall have the meanings given to them by Data Protection Legislation.

2.2. In addition to those terms, the following definitions shall apply:

**Affiliate** or **Affiliates** means each and any Person or undertaking under the Parties direction and in relation to either Party, any Person that directly or indirectly controls, is controlled by or is under common control with that Party (where control is defined as the direct or indirect ownership or control of at least 50% of the shares (including joint-ventures and partners in which a business has at least a 40% interest) or other equity securities, of a Person or of the power to direct or significantly influence the direction of the management, policies and voting interests of a Person whether by contract or otherwise).

**Authorized Person** means the Person(s) be nominated by the Business from time to time in writing.

**California Consumer Privacy Act** or **CCPA** means Title 1.81.5 California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100–1798.199), as amended or superseded from time to time.

**California Privacy Rights Act** or **CPRA** means the California Privacy Rights Act of 2020, (2020 Cal. Legis. Serv. Proposition 24, codified at Cal. Civ. Code §§ 1798.100 et seq.), and its implementing regulations, as amended or superseded from time to time.

**Data Protection Legislation** means CCPA and CPRA as well as any regulation adopted, published, administered, implemented, or enforced by the California Privacy Protection Agency or by the Attorney General to further the purposes of CCPA and/or CPRA, and any related case-law.

**Natural Person** means any living individual that is a subject to the Data Protection Legislation.

**Personnel** means in relation to a Party an employee of, a Management Employee of, Owner of, Director of, Officer of, Medical Staff Member of, or other Natural Person of that Party on whatever terms employed or engaged.

**Sub-Contractor** means any other Person (whether or not an Affiliate of the Contractor, but excluding the Contractor's Personnel) appointed by or on behalf of the Contractor or its Sub-Contractors to Process Personal Information for a Business Purpose on behalf of the Business under this Agreement or the Services Agreement, and any other Person engaged to assist the Contractor in Processing Personal Information for a Business Purpose on behalf of the Business, and any other Person engaged by the Contractor engages another Person to assist in Processing Personal Information for a Business Purpose.

2.3. For the purpose of this Agreement the term CCPA shall include CPRA.

2.4. Clause, schedule and paragraph headings shall not affect the interpretation of this Agreement.

2.5. A **Person** shall include a Natural Person, corporate or unincorporated body (whether or not having separate legal personality).


© All rights reserved by Heiko Maniero.

2.6. A reference to a **Company** shall include any Company, corporation or other body corporate, partnership, sole proprietorship, nonprofit, or government agency wherever and however incorporated or established.

2.7. Unless the context otherwise requires, any reference to a Party shall be deemed to include that Party's Affiliates and where an obligation is imposed on a Party under this Agreement, it will be required to procure compliance with such obligation by that Party's Affiliate where appropriate. For the avoidance of doubt, compliance shall be ensured by the Party that is affiliated with an Affiliate.

2.8. Unless the context otherwise requires, words in the singular shall include the plural and, in the plural, shall include the singular and a reference to one gender shall include a reference to the other genders.

2.9. A reference to a statute or statutory provision is a reference to it as amended, superseded, extended or re-enacted from time to time and shall include all subordinate legislation made from time to time under that statute or statutory provision, and the related case-law.

2.10. Unless the context otherwise requires, a reference to writing or written includes email but not fax.

2.11. Any words following the terms **including**, **include**, **in particular** or **for example** or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.

## 3. Scope of this Agreement

This Agreement shall apply only where, and to the extent that, the Contractor Processes Personal Information that is subject to Data Protection Legislation on behalf of the Business as a Contractor in course of providing Services pursuant to the Services Agreement.

## 4. Compliance with Data Protection Legislation

4.1. Each Party shall comply with all applicable requirements of Data Protection Legislation.

4.2. Without prejudice to the generality of this clause, the Business will ensure that it has all necessary appropriate Consents and notices in place to enable the lawful transfer to and Processing of the Personal Information by the Contractor in connection with the performance of the Contractor's obligations under the Services Agreement and this Agreement.

4.3. To the extent within the Business's Control having regard to the Contractor's obligations under the Services Agreement and this Agreement, the Business shall be responsible for the accuracy and quality of the Personal Information Processed by the Contractor under the Services Agreement and this Agreement.

## 5. Specification of the Personal Information which is disclosed to and/or Processed by the Contractor (1798.100 (d) (1) CCPA)


© All rights reserved by Heiko Maniero.

5.1. The Personal Information which is disclosed by the Business for limited and specified purposes are:

Types of Personal Information: Customer data, data of potential customers, employee data, data of business partners, supplier data, consumer data.

Categories of Data Subjects: Customers, potential customers, employees, business partners, suppliers, consumers.

Limited and specified purposes: To fulfill the contractual obligations described in the Services Agreement.

## 6. General obligations of the Contractor (1798.140 (j) (1) and (ag) (1) CCPA)

6.1. The Contractor shall not Sell or Share Personal Information.

6.2. The Contractor shall not retain, use, or disclose the Personal Information for any purpose other than for the Business Purposes specified in the Services Agreement or in this Agreement, including retaining, using, or disclosing the Personal Information for a Commercial Purpose other than the Business Purposes specified in the Services Agreement or in this Agreement, or as otherwise permitted by Data Protection Legislation.

6.3. The Contractor shall not retain, use, or disclose the information outside of the direct Business relationship between the Contractor and the Business.

6.4. The Contractor shall not combine the Personal Information that the Contractor receives pursuant to the Services Agreement with the Business with Personal Information that it receives from or on behalf of another Person or Persons, or Collects from its own interaction with the Consumer, provided that the Contractor may combine Personal Information to perform any Business Purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185 CCPA, except as provided for in paragraph (6) of subdivision (e) of Section 1798.140 CCPA and in regulations adopted by the California Privacy Protection Agency.

6.5. The Contractor certifies that it understands the restrictions above and that the Contractor will comply with them.

6.6. The Contractor permits the Business to monitor the Contractor's compliance with the Services Agreement and this Agreement through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

6.7. The Contractor shall only Process Personal Information for the purposes expressly specified in the Services Agreement or this Agreement or otherwise in accordance with the Business's documented instructions as given by an Authorized Person, unless the Contractor is required by any applicable law to which the Contractor is subject, to Process Personal Information for


© All rights reserved by Heiko Maniero.

any other purposes, in which case the Contractor shall, to the extent permitted by such applicable law, inform the Business of such legal requirement before undertaking such Processing.

## 7. Sub-Contractor (1798.140 (j) (2) and (ag) (2) CCPA)

7.1. If the Contractor engages any other Person to assist it in Processing Personal Information for a Business Purpose on behalf of the Business, or if any other Person engaged by the Contractor engages another Person to assist in Processing Personal Information for that Business Purpose, it shall notify the Business of that engagement, and the engagement shall be pursuant to the Services Agreement binding the other Person to observe all the requirements set forth in paragraph (1) of subdivision (j) of Section 1798.140 CCPA and/or paragraph (1) of subdivision (ag) of Section 1798.140 CCPA.

7.2. The Contractor has the Business's general authorization for the engagement of Sub-Contractor's from an agreed list that is subject to notification, and from time to time, after changes have been occurred, to re-notification. The Contractor shall specifically inform in writing the Business of any intended changes of that list through the addition or replacement of Sub-Contractor's at least thirty (30) days in advance, thereby giving the Business sufficient time to be able to object to such changes prior to the engagement of the concerned Sub-Contractor(s). The Contractor shall provide the Business with the information necessary to enable the Business to exercise the right to object.

7.3. Where the Contractor engages a Sub-Contractor for carrying out specific processing activities for a Business Purpose on behalf of the Business, it shall do so by way of a contract which imposes on the Sub-Contractor, in substance, the same privacy obligations as the ones imposed on the Contractor in accordance with the Services Agreement and this Agreement and Data Protection Legislation. The Contractor shall ensure that the Sub-Contractor complies with the obligations to which the Contractor is subject pursuant to the Services Agreement and this Agreement and to Data Protection Legislation.

7.4. At the Business's request, the Contractor shall provide a copy of such a Sub-Contractor agreement and any subsequent amendments to the Business. To the extent necessary to protect business secrets or other confidential information, including Personal Information, the Contractor may redact the text of the agreement prior to sharing the copy.

7.5. The Contractor shall remain fully responsible to the Business for the performance of the Sub-Contractor's obligations in accordance with its contract with the Contractor. The Contractor shall notify the Business of any failure by the Sub-Contractor to fulfill its contractual obligations.

7.6. The Contractor shall with regards to any Sub-Contractor undertake appropriate due diligence prior to Processing of Personal Information that is Processed for a Business Purpose on behalf of the Business by the Sub-Contractor to ensure that the Sub-Contractor is capable of providing the level of protection for Personal Information as it is required by the Services Agreement, this Agreement and Data Protection Legislation.

7.7. The Contractor shall ensure that the Personnel of all its Sub-Contractors and their other Sub-Contractors and all individuals responsible for handling Consumer inquiries about the Business'


© All rights reserved by Heiko Maniero.

privacy practices or the Business' compliance with Data Protection Legislation are informed of all requirements in Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.125, and 1798.130 CCPA, and how to direct Consumers to exercise their rights under those sections (see paragraph (6) of subdivision (a) of Section 1798.130).

## 8. Obligation of Contractor to comply with applicable obligations (1798.100 (d) (2) CCPA)

8.1. The Contractor is obliged to comply with all applicable obligations of, and to provide the same level of privacy protection as required by Data Protection Legislation.

8.2. The Contractor certifies to be, and to take from time to time all steps to stay at all times, in full compliance with Data Protection Legislation whenever acting as a Contractor on behalf of the Business as well as when acting as a Business in the meaning given in subdivision (d) of Cal. Civ. Code 1798.140 for its own Commercial Purposes and/or Business Purposes whenever the Contractor is Processing Personal Information of Personnel of the Business.

## 9. Right to help ensure compliance with Business' obligations (1798.100 (d) (3) CCPA)

9.1. The Contractor grants the Business the right to take reasonable and appropriate steps to help ensure that the Contractor uses the Personal Information transferred in a manner consistent with the Business' obligations under Data Protection Legislation.

## 10. Right to audit (1798.140 (j) (1) (C) CCPA)

10.1. The Contractor permits the Business, any Authorized Person or any other auditor mandated by the Business, on reasonable notice and during the Contractor's normal Business hours (but without notice, in the case of any reasonably suspected breach of this Agreement) to (a) gain access to, and take copies of, the processing records and any other information held at the Contractor's premises; and (b) inspect documents and electronic data and the Contractor's systems, facilities and equipment, for the purpose of auditing and certifying the Contractor's compliance with its obligations under the Services Agreement and this Agreement.

10.2. Such audit rights may be exercised only once in any calendar year during the term of the Services Agreement and for a period of three years following the expiry or termination of the Services Agreement. The Contractor shall give all necessary assistance to the conduct of any audits.

10.3. The Contractor further agrees that it shall provide the Business with such assistance as it may reasonably request in connection with any compulsory or voluntary audit or inspection by the California Privacy Protection Agency or by the Attorney General.

## 11. Notification of failure to comply with Data Protection Legislation (1798.100 (d) (4) CCPA)

11.1. The Contractor shall notify the Business if it makes the determination that it can no longer meet its obligations under Data Protection Legislation.

## 12. Stop and remediate unauthorized use of Personal Information (1798.100 (d) (5) CCPA)


© All rights reserved by Heiko Maniero.

12.1. The Contractor grants the Business the right, upon notice, including under Section 1798.100 (d) (4) CCPA, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Information.

## 13. Deletion of Consumer's Personal Information (1798.105 (c) (3) and (d) CCPA)

13.1. The Contractor shall cooperate with the Business in responding to a Verifiable Consumer Request, and at the direction of the Business, shall delete, or enable the Business to delete and shall notify any of its own Service Providers or Contractors to delete Personal Information about the Consumer Collected, Used, Processed, or Retained by the Contractor.

13.2. The Contractor shall notify any Service Providers, Contractors, or Third Parties who may have accessed Personal Information from or through the Contractor, unless the information was accessed at the direction of the Business, to delete the Consumer's Personal Information unless this proves impossible or involves disproportionate effort.

13.3. The Contractor shall not be required to comply with a deletion request submitted by the Consumer directly to the Contractor to the extent that the Contractor has Collected, Used, Processed, or Retained the Consumer's Personal Information in its role as a Contractor to the Business.

13.4. The Contractor acting pursuant to its Services Agreement with the Business, another Service Provider, or another Contractor, is not required to comply with a Consumer's request to delete the Consumer's Personal Information if it is reasonably necessary for the Business or Contractor to maintain the Consumer's Personal Information in order to (1) complete the transaction for which the Personal Information was Collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the Consumer, or reasonably anticipated by the Consumer within the context of a Business' ongoing Business relationship with the Consumer, or otherwise perform a contract between the Business and the Consumer, or (2) help to ensure security and integrity to the extent the use of the Consumer's Personal Information is reasonably necessary and proportionate for those purposes, or (3) debug to identify and repair errors that impair existing intended functionality, or (4) exercise free speech, ensure the right of another Consumer to exercise that Consumer's right of free speech, or exercise another right provided for by law, or (5) comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code, or (6) engage in public or peer-reviewed scientific, historical, or statistical research that conforms or adheres to all other applicable ethics and privacy laws, when the Business' deletion of the information is likely to render impossible or seriously impair the ability to complete such research, if the Consumer has provided informed Consent, or (7) enable solely internal uses that are reasonably aligned with the expectations of the Consumer based on the Consumer's relationship with the Business and compatible with the context in which the Consumer provided the information, or (8) comply with a legal obligation.

## 14. Sell or Share of Personal Information by another Service Provider, another Contractor or Third Party (1798.115 (d) CCPA)


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

14.1. The Contractor shall contractually prevent any other Service Provider, or other Contractor or Third Party from Selling or Sharing Personal Information about a Consumer that has been Sold to, or Shared with, the other Service Provider, or other Contractor or the Third Party by the Contractor unless the Consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120 CCPA.

14.2. Where the Contractor acts, based on the relationship between the Business to a client of the Business (for the avoidance of doubt, where the Business is a Contractor for another Business) as another Service Provider, or other Contractor or Third Party, the Contractor shall not Sell or Share Personal Information about a Consumer that has been Sold to, or Shared with, the Contractor by the Business, unless the Consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120 CCPA.

## 15. Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information (1798.121 (a) and (c) CCPA)

15.1. In case the Contractor assists the Business in performing the purposes authorized by subdivision (a) of Section 1798.121 CCPA, the Contractor shall not use the Sensitive Personal Information after it has received instructions from the Business and to the extent it has actual knowledge that the Personal Information is Sensitive Personal Information for any other purpose.

15.2. The Contractor shall limit its use of the Consumer's Sensitive Personal Information that are Processed on behalf of the Business under this Agreement to that use which is necessary to perform the Services or provide the goods, and shall Process only in accordance with documented instructions given by the Business. The Contractor shall not disclose the Consumer's sensitive Personal Information to any Third Party.

## 16. Disclosure, Correction, and Deletion requirements (1798.130 CCPA)

16.1. In case the Business receives a Verifiable Consumer Request pursuant to Section 1798.110 CCPA or 1798.115 CCPA the Contractor shall assist the Business in answering such request.

16.2. The Contractor shall not comply with a Verifiable Consumer Request received directly from a Consumer or a Consumer's Authorized Agent, pursuant to Section 1798.110 CCPA or 1798.115 CCPA, to the extent that the Contractor has Collected Personal Information about the Consumer in its role as a Contractor. In such case the Contractor shall inform the Business without undue delay about receiving the Verifiable Consumer Request.

16.3. The Contractor shall provide assistance to the Business with respect to the Business' response to a Verifiable Consumer Request, including, but not limited to, by providing to the Business the Consumer's Personal Information in the Contractor's possession, which the Contractor obtained as a result of providing Services to the Business, and by correcting inaccurate information or by enabling the Business to do the same.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

16.4. The Contractor shall disclose and deliver the required information to the Business free of charge, correct inaccurate Personal Information, or delete a Consumer's Personal Information, based on the Consumer's request, within fifteen (15) days of receiving a Request from the Business.

16.5. The Contractor shall assist the Business through appropriate technical and organizational measures in complying with the requirements of subdivisions (d) to (f), inclusive, of Section 1798.100 CCPA, taking into account the nature of the Processing.

## 17. General Assistance by the Contractor, Assistance with Consumer Rights

Whenever required, the Contractor shall assist the Business to comply with Data Protection Legislation, including, but not limited to, assisting to comply with the obligations imposed on Businesses by Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.121, 1798.125, 1798.130, and 1798.135 CCPA.

## 18. Opt-Out and Advertising and Marketing (1798.140 (e) (6) CCPA)

18.1. The Contractor shall not combine the Personal Information of opted-out Consumers that the Contractor receives from, or on behalf of, the Business with Personal Information that the Contractor receives from, or on behalf of, another Person or Persons or Collects from its own interaction with the Consumer for the purpose of providing advertising and marketing to the Consumer.

## 19. Processing of other Personal Information by the Business and the Contractor for their own Business Purposes (1798.145 (m) (1) and (n) (1) CCPA)

19.1. The Business is collecting and Processing Personal Information about Natural Persons in the course of these Natural Persons acting as a job applicant to, employee of, Owner of, Director of, Officer of, Medical Staff Member of, Independent Contractor of, another Service Provider of, another Contractor of, or Third Party of the Contractor or its Sub-Contractors to the extent that the Natural Person's Personal Information is Collected and used by the Business solely within the context of the Natural Person's role or former role as a job applicant to, employee of, Owner of, Director of, Officer of, Medical Staff Member of, an Independent Contractor of, another Service Provider of, another Contractor of, or Third Party of the Contractor and/or its Sub-Contractors. The Personal Information may include, but is not limited to, emergency contact information and information that is necessary for the Business to retain to administer benefits for another Natural Person.

19.2. The Business is collecting and Processing Personal Information reflecting written or verbal communications or transactions between the Business and the Consumer, where the Consumer is a Natural Person who acted or is acting as a job applicant to, an employee, Owner, Director, Officer, or Independent Contractor, another Service Provider of, another Contractor of, or Third Party of a Company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transactions with the Business occur solely within the context of the Business conducting due diligence regarding, or providing or receiving a product or service to or from such Company, partnership, sole proprietorship, nonprofit, or government agency.


© All rights reserved by Heiko Maniero.

19.3. The Contractor shall inform any job applicant to, employee of, Owner of, Director of, Officer of, Medical Staff Member of, Independent Contractor of, another Service Provider of, another Contractor of, or Third Party of such Company, partnership, sole proprietorship, nonprofit, or government agency that is engaged with the Contractor for a Business Purpose on behalf of the Business, the Contractor and/or its Sub-Contractors about the transparency document published by the Business on its Homepage that contains information in regards to obligations imposed on Businesses by Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.121, 1798.125, 1798.130, and 1798.135 CCPA for these groups of Natural Persons.

19.4. The Contractor shall publish a document on its Homepage that contains information in regards to the obligations imposed on Businesses by Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.121, 1798.125, 1798.130, and 1798.135 CCPA and inform any job applicant to, employee of, Owner of, Director of, Officer of, Medical Staff Member of, Independent Contractor of, another Service Provider of, another Contractor of, or Third Party of the Business of whose Personal Information is Collected or Processed by the Contractor for its own Business Purposes about its own publication.

## 20. Reliability of and contract with the Contractor's Personnel, access limitation, training, and information requirements

20.1. The Contractor shall take reasonable steps to ensure reliability of those of its Personnel who may have access to any Personal Information that is Processed for a Business Purpose on behalf of the Business.

20.2. The Contractor shall ensure that those of its Personnel authorized to Process Personal Information under the Service Agreement or this Agreement (a) are aware of the confidential nature of the Personal Information, and (b) are bound by obligations of confidentiality by virtue of a written contract between the Contractor and such Persons; and (c) have received appropriate training on the handling of Personal Information and on their responsibilities in relation to the Processing of Personal Information.

20.3. The Contractor shall implement reasonable security procedures and practices as well as technical and organizational measures to ensure that those of its Personnel only have access to such part or parts of the Personal Information that is Processed for a Business Purpose on behalf of the Business as is strictly necessary for the performance of their duties and obligations.

20.4. The Contractor shall ensure that its Personnel and all individuals responsible for handling Consumer inquiries about the Business' privacy practices or the Business' compliance with Data Protection Legislation are informed of all requirements in Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.125, and 1798.130 CCPA, and how to direct Consumers to exercise their rights under those sections (see paragraph (6) of subdivision (a) of Section 1798.130).

## 21. Reasonable security procedures and practices (1798.150 (a) (1) CCPA)


© All rights reserved by Heiko Maniero.

21.1. Where appropriate and/or required to protect the rights and freedoms of Natural Persons, the Contractor shall encrypt and/or redact Personal Information that is Processed for a Business Purpose on behalf of the Business, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5 CCPA.

21.2. To the extend such Personal Information is Processed for a Business Purpose on behalf of the Business, the Contractor shall encrypt email addresses, passwords, security questions and security answers that would permit access to an account.

21.3. The Contractor shall implement and maintain at all times reasonable security procedures and practices appropriate to the nature of the information to protect all Personal Information that is Processed for a Business Purpose on behalf of the Business, pursuant to Section 1798.81.5 CCPA.

21.4. The Contractor has implemented reasonable security procedures and practices and published them on its Homepage and/or communicated them to the Business. The Contractor may add to, amend, or replace the reasonable security procedures and practices for security reasons and shall notify the Business in writing where it has done so at least ten (10) days before such changes are in effect, thereby giving the Business sufficient time to be able to object to such changes prior to them becoming effective. The Contractor shall provide the Business with the information necessary to enable the Business to exercise the right to object.

21.5. The Contractor shall, in relation to the Personal Information that is Processed for a Business Purpose on behalf of the Business, ensure ongoing confidentiality, integrity, availability and resilience of processing systems and Services, and the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident.

## 22. Liability and indemnification (1798.145. (i) (1) and (2) CCPA)

22.1. The Business shall not be liable under CCPA if the Contractor receiving Personal Information from the Business uses it in violation of the restrictions set forth in CCPA. At the time of disclosing the Personal Information, the Business does not have actual knowledge, or reason to believe, that the Service Provider or Contractor intends to commit such a violation.

22.2. The Contractor agrees to indemnify, defend, and hold harmless the Business from and against any loss, cost, or damage of any kind (including reasonable outside attorneys' fees) to the extent arising out of any breach of Data Protection Legislation by the Contractor, and/or its negligence or willful misconduct.

## 23. Obligations upon expiry or termination of the Services Agreement

23.1. Notwithstanding the Contractor’s obligations under the Services Agreement following its expiry or termination, the Contractor shall promptly and in any event within thirty (30) days of the expiry or termination of the Services Agreement, at the Business’s option (given by any Authorized Person) either delete or return (in such format and on such media or by such means as the Parties shall agree in writing) all copies of the Personal Information Processed by the Contractor


© All rights reserved by Heiko Maniero.

and/or its Sub-Contractors for a Business Purpose on behalf of the Business under this Agreement or the Services Agreement.

23.2. Where the Business has instructed the Contractor to delete the Personal Information, the Contractor shall do so in accordance with best industry practices for the reliable and secure deletion of data or for the secure destruction of confidential material.

23.3. The Contractor (and those of its Sub-Contractors, as appropriate) may retain a copy of the Personal Information Processed for a Business Purpose on behalf of the Business under this Agreement or the Services Agreement to the extent required by any applicable law to which the Contractor (or any Sub-Contractor) is subject and only for such period as shall be required by such applicable law. Where applicable, the Contractor shall notify the Business of such requirement and shall ensure that such Personal Information are kept confidential and not Processed for any other purpose.

23.4. The Business may require the Contractor to provide a written certificate confirming that it has complied with its obligations under this paragraph.

## 24. Notification of Personal Information Security Breaches

24.1. The Contractor shall notify the Business without undue delay after becoming aware of a Personal Information Security Breach affecting the Personal Information Processed for a Business Purpose on behalf of the Business under this Agreement or the Services Agreement, providing sufficient information to enable the Business to evaluate the impact of such Personal Information Security Breach and to meet any obligations of the Business in accordance with Data Protection Legislation.

24.2. The Contractor shall provide the Business with such assistance as the Business may reasonably request and take such reasonable commercial steps as the Business may request in order to evaluate, investigate, mitigate and remediate any Personal Information Security Breach (including, where applicable, communicating any Personal Information Security Breach to affected Consumers).

## 25. General provisions

25.1. Term and termination: Except in respect of any provision of this Agreement that expressly or by implication is intended come into or continue in force on or after the expiry or termination of the Services Agreement, this Agreement shall be coterminous with the Services Agreement.

25.2. Third Party rights: A Person who is not a Party to this Agreement shall not have any rights to enforce any terms of this Agreement.

25.3. Severance: If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this clause shall not affect the validity and enforceability of the rest of this Agreement. If any provision or part-provision of this Agreement is invalid, illegal or


© All rights reserved by Heiko Maniero.

unenforceable, the Parties shall negotiate in good faith to amend such provision so that, as amended, it is legal, valid and enforceable, and, to the greatest extent possible, achieves the intended commercial result of the original provision.

25.4. Variation: Except as expressly provided in this Agreement, no variation of this Agreement shall be effective unless it is in writing and signed by the Parties (or their authorized representatives) or otherwise accepted by the Parties.

25.5. This Agreement supersedes any conflicting or inconsistent provisions in the Services Agreement or any other contract between the Parties related to the Processing of Personal Information subject to the Data Protection Legislation and, in the event of ambiguity, this Agreement will prevail. The Services Agreement or any other contract between the Parties, as amended and modified by this Agreement, otherwise remain in full force and effect.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

# Data Processing Agreement, Joint Controllership Agreement and Cross-Border Personal Data Transfer and Sharing Agreement for the United Arab Emirates

This Data Processing Agreement, Joint Controllership Agreement and Cross-Border Personal Data Transfer and Sharing Agreement for the United Arab Emirates (**Agreement**) is concluded on the same date as the Services Agreement (as defined below) and is concluded by and between

(1) the **Controller**, named with its Company details as a Party in the Services Agreement; and

(2) the **Other Party**, named with its Company details as a Party in the Services Agreement.

(together the **Parties**)

## 1. Preamble

1.1 The Other Party is a provider of professional services (**Services**) and/or provides its Services as a Joint-Controller. The Parties entered into an agreement which describes the Services provided by the Other Party acting on behalf of the Controller or as an Other Controller, or acting jointly with the Controller, in detail (**Services Agreement**).

1.2 The Parties have agreed to enter into this Agreement in relation to the Processing of Personal Data by the Other Party, or jointly by the Other Party and the Controller, in the course of providing the Services. The terms of this Agreement are intended to apply in addition to and not in substitution of the terms of the Services Agreement.

## 2. Definitions and interpretation

2.1 **PDPL** means the Decree Law No. 45 of 2021 as issued at the Presidential Palace in Abu Dhabi and published in the Official Gazette which is in force since 2nd of January 2022, as amended or superseded from time to time. The legal definitions from Art. 1 PDPL apply and shall have the meanings given to them by Data Protection Legislation.

2.2 **Other Controller** means an establishment or natural person acting as a Controller, who has Personal Data and who, given the nature of his/her activity, specifies the method, criteria and purpose of Processing such Personal Data, whether individually or jointly with other persons or establishments, that is Processing Personal Data that originated from the Controller, whether the data is transferred in a Cross-Border Personal Data Transfer, Shared, or Processed within the United Arab Emirates.

2.3 **Joint-Controller** means an establishment or natural person who Processes Personal Data jointly with the Controller.


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

2.4 **Data Protection Legislation** means the Decree Law No. 45 of 2021 as well as any regulation adopted, published, administered, implemented, or enforced by the Government of the United Arab Emirates or by one of the seven emirates, as amended or superseded from time to time, all related Executive Regulations regarding or concretizing the PDPL, and any related case-law.

## 3. Applicability of the Agreement

This Agreement shall apply to the Processing of Personal Data, whether totally or partially, through automatically operated electronic systems or other means, by (1) any Other Controller, Joint-Controller or Processor located in the United Arab Emirates who carries out the activities of Processing Personal Data of Data Subjects inside or outside the United Arab Emirates, and (2) any Other Controller, Joint-Controller or Processor located outside the United Arab Emirates who carries out the activities of Processing Personal Data of Data Subjects inside the United Arab Emirates, as long as (3) such Personal Data is or will be Processed on behalf of the Controller, or in Joint-Controllership with the Controller, or is or will be Subject to a Cross-Border Personal Data Transfer and/or Sharing for Processing Purposes executed or initiated by or jointly with the Controller.

## 4. Compliance with Data Protection Legislation

4.1 Each Party shall comply with all applicable requirements of Data Protection Legislation. This Clause is in addition to, and does not relieve any Party from complying with, a Party's obligations under Data Protection Legislation.

4.2 If the Other Party is a Processor, without prejudice to the generality of this Clause, the Controller will ensure that it has all necessary Consents and notices in place to enable the lawful transfer to and Processing of the Personal Data by the Processor in connection with the performance of its obligations under the Services Agreement.

4.3 If the Other Party is a Processor, to the extent within the Controller's control having regard to the Processor's obligations under the Services Agreement, the Controller shall be responsible for the accuracy and quality of the Personal Data Processed by the Processor.

4.4 If the Other Party is a Processor, the Processor shall have an ongoing obligation throughout the duration of the Services Agreement to identify and report to the Controller best practice techniques relating to the Processing of Personal Data and the emergence of new and evolving technologies which could improve the availability, confidentiality and/or integrity of the Processing of Personal Data.

## 5. Sub-Processors

5.1 If the Processing involves more than one Processor (**Sub-Processor**), the Processing must be made in accordance with a contract or written agreement whereby their obligations, responsibilities and roles related to the Processing are clearly defined.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

5.2 The Controller hereby authorizes the Other Party to appoint Sub-Processors (General Written Authorization). The Other Party shall name all its Sub-Processors to the Controller prior to initiation of Processing.

5.3 With respect to each Sub-Processor appointed by the Other Party under General Written Authorization, the Other Party shall (a) undertake appropriate due diligence prior to the Processing of Personal Data by such Sub-Processor to ensure that it is capable of providing the level of protection for Personal Data required by the terms of the Services Agreement and this Agreement, and (b) enter into a written Agreement with the Sub-Processor incorporating terms which are substantially similar (and no less onerous) than those set out in this Agreement and which meet the requirements stipulated by PDPL.

5.4 In regard to the Agreement between the Controller and the Other Party, the Other Party remain fully liable to the Controller for all acts or omissions of its Sub-Processor as though they were its own.

5.5 To the extent that the Other Party has already appointed any Sub-Processors prior to the Processing of any Personal Data under this Agreement, the Other Party shall ensure that its obligations under this Section are met.

5.6 Where the Other Party proposes any changes concerning the addition or replacement of any Sub-Processor, it shall notify the Controller in writing as soon as reasonably practicable prior to implementing such change specifying (a) the name of any Sub-Processor which it proposes to add or replace, and (b) the Processing activity or activities affected by the proposed change, and (c) the reasons for the proposed change; and (d) the proposed date for implementation of the change.

5.7 If within thirty (30) days of receipt of a notice the Controller (acting reasonably and in good faith) notifies the Other Party in writing of any objections to the proposed change, the Parties shall use their respective reasonable endeavors to resolve the Controller's objections. Where such resolution cannot be agreed within thirty (30) days of the Other Party's receipt of the Controller's objections (or such longer period as the Parties may agree in writing) the Controller may, notwithstanding the terms of the Services Agreement, serve written notice on the Other Party to terminate the Services Agreement (to the extent that the provision of the Services are or would be affected by the proposed change).

5.8 The Other Party shall, upon the Controller's request, provide the Controller with copies of any Agreements between the Other Party and its Sub-Processors (which may be redacted to remove information which is confidential to the Other Party and/or its Sub-Processors and which is not relevant to the terms of this Agreement).

## 6. Data Subject's Consent and Exceptions

6.1 The Other Party shall Process Personal Data only with the Data Subject's Consent.

6.2 If the Other Party is a Processor, the Data Subject's Consent shall be obtained by the Controller. The Processor shall obtain proof of the Data Subject's Consent from the Controller before starting the Processing of Personal Data of Data Subject's.


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

6.3 If the Other Party and the Controller act as Joint-Controllers, the Data Subject's Consent may be obtained by either party. If the Data Subject's Consent was obtained by one of the Joint-Controllers, that Joint-Controller shall, before starting or initiating the Processing of Personal Data of Data Subject's, inform the second Joint-Controller about obtaining the required Consent.

6.4 If the Other Party is an Other Controller and/or in any case of a Cross-Border Personal Data Transfer and/or Sharing for Processing Purposes the Other Party shall obtain the Data Subject's Consent before starting the Processing of Personal Data of Data Subject's.

6.5 In the following cases, in which Processing is considered lawful, the Other Party may Process without the Data Subject's Consent, namely (1) if the Processing is necessary to protect the public interest, or (2) if the Processing is for Personal Data that has become available and known to the public by an act of the Data Subject, or (3) if the Processing is necessary to initiate or defend against any actions to claim rights or legal proceedings, or related to judicial or security procedures, or (4) if the Processing is necessary for the purposes of occupational or preventive medicine, for assessment of the working capacity of an employee, medical diagnosis, provision of health or social care, treatment or health insurance services, or management of health or social care systems and services, in accordance with the legislation in force in the United Arab Emirates, or (5) if the Processing is necessary to protect public health, including the protection from communicable diseases and epidemics, or for the purposes of ensuring the safety and quality of health care, medicines, drugs and medical devices, in accordance with the legislation in force in the United Arab Emirates, or (6) if the Processing is necessary for archival purposes or for scientific, historical and statistical studies, in accordance with the legislation in force in the United Arab Emirates, or (7) if the Processing is necessary to protect the interests of the Data Subject, or (8) if the Processing is necessary for the Controller or Data Subject to fulfill his/her obligations and exercise his/her legally established rights in the field of employment, social security or laws on social protection, to the extent permitted by those laws, or (9) if the Processing is necessary to perform a contract to which the Data Subject is a party or to take, at the request of the Data Subject, procedures for concluding, amending or terminating a contract, or (10) if the Processing is necessary to fulfill obligations imposed by other laws of the United Arab Emirates on Controllers, or (11) any other cases set by the Executive Regulations of PDPL.

## 7. Personal Data Processing Controls

The Other Party shall Process Personal Data only according to the following controls, namely (1) Processing must be made in a fair, transparent and lawful manner, and (2) Personal Data must be collected for a specific and clear purpose, and may not be Processed at any subsequent time in a manner incompatible with that purpose. However, Personal Data may be Processed if the purpose of Processing is similar or close to the purpose for which such data is collected, and (3) Personal Data must be sufficient for and limited to the purpose for which the Processing is made, and (4) Personal Data must be accurate and correct and must be updated whenever necessary, and (5) Appropriate measures and procedures must be in place to ensure erasure or correction of incorrect Personal Data, and (6) Personal Data must be kept securely and protected from any breach, infringement, or illegal or unauthorized Processing by establishing and applying appropriate technical and organizational measures and procedures


© All rights reserved by Heiko Maniero.

in accordance with the laws and legislation in force in this regard, and (7) Personal Data may not be kept after fulfilling the purpose of Processing. It may only be kept in the event that the identity of the Data Subject is anonymized using the “Anonymization” feature, and (8) any other controls set by the Executive Regulations of PDPL.

## 8. Conditions for Consent to Data Processing

8.1 If the Other Party is an Other Controller or acts jointly as a Joint-Controller with the Controller, the Other Party shall be able to prove the Consent of the Data Subject to Process his/her Personal Data in the event that the Processing is based on such Consent.

8.2 If the Other Party is an Other Controller, or acts jointly as a Joint-Controller with the Controller, the Other Party shall be able to prove that Consent was given in a clear, simple, unambiguous and easily accessible manner, whether in writing or electronic form and that the Consent language indicated the right of the Data Subject to withdraw, at any time, its Consent and that such withdrawal could be easily made, and that such withdrawal shall not affect the legality and lawfulness of the Processing made based on the Consent given prior to the withdrawal.

## 9. General Obligations of the Other Party

9.1 The Other Party shall take appropriate technical and organizational measures and procedures to apply the necessary standards to protect and secure Personal Data, in order to maintain its confidentiality and privacy and to ensure that it is not infringed, damaged, altered or tampered with, taking into account the nature, scope and purposes of Processing and the potential risks to the confidentiality and privacy of the Personal Data of the Data Subject. The Parties agreed on the required technical and organizational measures and procedures in APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

9.2 The Other Party shall apply the appropriate measures, both when defining the means of Processing or during the Processing itself, in order to comply with the provisions of PDPL, including the controls stipulated in Article 5 PDPL. Such measures may include Pseudonymization.

9.3 The Other Party shall apply the appropriate technical and organizational measures with respect to default settings to ensure that the Processing of Personal Data is limited to its intended purpose. This obligation applies to the amount and type of Personal Data collected, the type of Processing to be made thereon, and the period of storage and accessibility of such data.

9.4 The Other Party shall maintain a special record of Personal Data which must include the data of the Controller and Data Protection Officer, as well as a description of the categories of Personal Data held thereby, data of the persons authorized to access such Personal Data, the Processing durations, restrictions and scope, the mechanism of erasure, modification or Processing of Personal Data, the purpose of Processing and any data related to the movement and Cross-Border Processing of such data, while indicating the technical and organizational procedures related to information security and Processing operations, provided that the Controller provides this record to the UAE Data Office whenever requested to do so.


© All rights reserved by Heiko Maniero.

9.5 The Other Party shall appoint only Processors who provide sufficient guarantees to apply technical and organizational measures in a manner that ensures that the Processing meets the Processing requirements, rules and controls stipulated by PDPL, the Executive Regulations of PDPL and decisions issued in implementation of PDPL.

9.6 The Other Party shall provide the UAE Data Office, based on a decision from the competent judicial authority, with any information requested thereby in exercise of its competencies stipulated by PDPL and the Executive Regulations of PDPL.

9.7 The Other Party shall fulfill any other obligations set by the Executive Regulations of PDPL. The Other Party shall monitor and abide the Executive Regulations of PDPL.

## 10. General Obligations of the Other Party if that Party acts as a Processor

10.1 This Section 10 applies only if the Other Party acts as a Processor and Processes Personal Data on behalf of the Controller. The Clauses of Section 10 of this Agreement shall supersede any conflicting Clauses in other Sections of this Agreement regarding to the Processor.

10.2 The Processor shall make and carry out the Processing in accordance with the instructions of the Controller and the contracts and agreements concluded between them that specify in particular the scope, subject, purpose and nature of the Processing, the type of Personal Data and categories of Data Subjects. The Parties determined the scope, subject, purpose and nature of the Processing, the type of Personal Data and categories of Data Subjects in the Services Agreement and/or in APPENDIX 8 – DESCRIPTION OF THE PROCESSING OR THE TRANSFER.

10.3 The Processor shall apply the appropriate technical and organizational measures and procedures to protect Personal Data at the design stage, both when defining the means of Processing or during the Processing itself, taking into consideration the cost of applying such measures and procedures and the nature, scope and purposes of the Processing. The Parties agreed on the technical and organizational measures and procedures in APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

10.4 The Processor shall make the Processing according to the purpose and period set therefor and notify the Controller if the Processing exceeds the set period, in order to extend such period or issue the appropriate directions. Whenever required, the notifications shall be made within two working days after such event occurred or is determined.

10.5 The Processor shall not take any action that would disclose the Personal Data or the results of Processing, except in cases permitted by law.

10.6 The Processor shall protect and secure the Processing operation and secure the media and electronic devices used in the Processing and the Personal Data stored therein.

10.7 The Processor shall maintain a special record of Personal Data Processed on behalf of the Controller, which must include the data of the Controller, Processor and Data Protection Officer, as well as a description of the categories of Personal Data held thereby, data of the persons authorized to access such Personal Data, the Processing durations, restrictions and scope, the


© All rights reserved by Heiko Maniero.

mechanism of erasure, modification or Processing of Personal Data, the purpose of Processing and any data related to the movement and Cross-Border Processing of such data, while indicating the technical and organizational procedures related to information security and Processing operations, provided that the Processor provides this record to the UAE Data Office whenever requested to do so.

10.8 The Processor shall provide all means to prove abidance thereby to the provisions of PDPL, at the request of the Controller or UAE Data Office.

10.9 The Processor shall make and carry out the Processing in accordance with the rules, requirements and controls set by PDPL and the Executive Regulations of PDPL, or as instructed by the UAE Data Office.

10.10 The Executive Regulations of PDPL shall set the procedures, controls, conditions, and technical and standard criteria related to the Processors obligations. The Processor shall monitor and abide the Executive Regulations of PDPL.

## 11. General Obligations if the Parties act as Joint-Controllers

11.1 This Section 11 shall apply only if the Controller and the Other Party act jointly as Joint-Controllers. The Clauses of Section 11 of this Agreement shall supersede any conflicting Clauses in other Sections of this Agreement regarding to the Joint-Controllers.

11.2 The Joint-Controllers determined the scope, subject, purpose and nature of the Processing, the type of Personal Data and categories of Data Subjects in the Services Agreement and/or in APPENDIX 8 – DESCRIPTION OF THE PROCESSING OR THE TRANSFER.

11.3 The Joint-Controllers shall jointly ensure compliance with Data Protection Legislation when Processing Personal Data. Both controllers are equally responsible for the legality and lawfulness of joint Processing.

11.4 Regardless of the place of Business of each Joint-Controller, both Joint-Controllers agree that the UAE Data Office is the competent supervisory authority.

11.5 The Controller undertakes to provide the Data Subject's with all information regarding the Data Subject's Rights under PDPL. The Controller acts as the contact point for Data Subjects.

11.6 The Joint-Controllers shall jointly take the appropriate technical and organizational measures and procedures to apply the necessary standards to protect and secure Personal Data, in order to maintain its confidentiality and privacy and to ensure that it is not infringed, damaged, altered or tampered with, taking into account the nature, scope and purposes of Processing and the potential risks to the confidentiality and privacy of the Personal Data of the Data Subject. The Parties agreed on the technical and organizational measures and procedures in APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

11.7 The Joint-Controllers shall jointly apply the appropriate measures, both when defining the means of Processing or during the Processing itself, in order to comply with the provisions of


© All rights reserved by Heiko Maniero.

PDPL, including the controls stipulated in Article 5 PDPL. Such measures may include Pseudonymization.

11.8 The Joint-Controllers shall jointly apply the appropriate technical and organizational measures with respect to default settings to ensure that the Processing of Personal Data is limited to its intended purpose. This obligation applies to the amount and type of Personal Data collected, the type of Processing to be made thereon, and the period of storage and accessibility of such data. The Parties agreed on the technical and organizational measures and procedures in APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

11.9 The Joint-Controllers shall jointly maintain a special record of Personal Data which must include the data of the Controller and Data Protection Officer, as well as a description of the categories of Personal Data held thereby, data of the persons authorized to access such Personal Data, the Processing durations, restrictions and scope, the mechanism of erasure, modification or Processing of Personal Data, the purpose of Processing and any data related to the movement and Cross-Border Processing of such data, while indicating the technical and organizational procedures related to information security and Processing operations, provided that the Controller provides this record to the UAE Data Office whenever requested to do so.

11.10 The Joint-Controllers shall jointly appoint only Processors who provide sufficient guarantees to apply technical and organizational measures in a manner that ensures that the Processing meets the Processing requirements, rules and controls stipulated by PDPL, the Executive Regulations of PDPL and decisions issued in implementation of PDPL.

11.11 The Joint-Controllers shall jointly provide the UAE Data Office, based on a decision from the competent judicial authority, with any information requested thereby in exercise of its competencies stipulated by PDPL and the Executive Regulations of PDPL.

11.12 The Joint-Controllers shall jointly appoint a Data Protection Officer in accordance with Section 13 of this Agreement.

## 12. Reporting a Personal Data Breach

12.1 The Other Party shall, immediately upon becoming aware of any infringement or breach of the Personal Data of the Data Subject that would prejudice the privacy, confidentiality and security of such data, report such infringement or breach and the results of the investigation to the Controller.

12.2 Such reporting shall be accompanied by the following data and documents, namely (a) the nature, form, causes, approximate number and records of the infringement or breach, and (b) the data of the Data Protection Officer appointed by the Other Party, and (c) the potential and expected effects of the infringement or breach, and (d) the procedures and measures taken thereby and proposed to be applied to address this infringement or breach and reduce its negative effects, and (e) documentation of the infringement or breach and the corrective actions taken by the Other Party, and (f) any other requirements that the UAE Data Office demands from the Controller.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

12.3 The Other Party will assist the Controller by all means to allow the Controller to notify the Data Subject in the event that the infringement or breach would prejudice the privacy, confidentiality and security of his/her Personal Data and advise him/her of the procedures taken thereby, within such period and in accordance with such procedures and conditions as set by the Executive Regulations of PDPL.

## 13. Appointment of Data Protection Officer

13.1 The Other Party shall appoint a Data Protection Officer who has sufficient skills and knowledge of Personal Data Protection, in any of the following cases, namely (a) if the Processing would cause a high-level risk to the confidentiality and privacy of the Personal Data of the Data Subject as a result of adopting technologies that are new or associated with the amount of data, or (b) if the Processing will involve a systematic and comprehensive assessment of Sensitive Personal Data, including Profiling and Automated Processing, or (c) if the Processing will be made on a large amount of Sensitive Personal Data.

13.2 The Data Protection Officer may be employed or authorized by the Other Party, whether inside or outside the United Arab Emirates.

13.3 The Other Party shall specify the contact address of the Data Protection Officer and notify the UAE Data Office.

## 14. Responsibilities of the Data Protection Officer of the Other Party

14.1 The Data Protection Officer of the Other Party shall be responsible for ascertaining compliance by the Other Party with the provisions of PDPL, the Executive Regulations of PDPL, and the instructions issued by the UAE Data Office.

14.2 The Data Protection Officer of the Other Party shall, in particular, undertake the following duties and powers, namely (a) verifying the quality and validity of the procedures adopted by both the Controller and Processor, and (b) receiving requests and complaints related to Personal Data in accordance with the provisions of PDPL and the Executive Regulations of PDPL, and (c) providing technical advice related to the procedures of periodic evaluation and examination of Personal Data Protection systems and intrusion prevention systems of the Controller and Processor, documenting the results of such evaluation, and providing appropriate recommendations in this regard, including risk assessment procedures, and (d) acting as a liaison between the Controller or Processor, as the case may be, and the UAE Data Office regarding their implementation of the provisions of Personal Data Processing stipulated by PDPL, and (e) any other duties or powers specified under the Executive Regulations of PDPL.

14.3 The Data Protection Officer of the Other Party shall maintain the confidentiality of the information and data received thereby in implementation of the duties and powers given thereto pursuant to the provisions of PDPL and the Executive Regulations of PDPL and in accordance with the legislation in force in the United Arab Emirates.

## 15. Obligations of the Other Party towards the Data Protection Officer


© All rights reserved by Heiko Maniero.

15.1 The Other Party shall provide all means to ensure that the Data Protection Officer performs the responsibilities and duties assigned thereto, as stipulated in Article 11 PDPL, in a proper manner, including, in particular, the following, namely (a) ensuring that he/she is appropriately and timely engaged in all matters relating to Personal Data Protection, and (b) ensuring that he/she is provided with all the necessary resources and support to perform the duties assigned by PDPL, and (c) not to terminate his/her service or impose any disciplinary penalty for a reason related to the performance of his/her duties in accordance with the provisions of PDPL, and (d) ensuring that he/she is not assigned to duties that lead to a conflict of interest with the duties assigned under PDPL.

15.2 Data Subject's shall communicate directly with the Data Protection Officer of the Controller for any matters related to his/her Personal Data and the Processing under PDPL in order to exercise his/her rights in accordance with the provisions of PDPL. The Data Protection Officer of the Other Party shall refer Data Subject's to the Data Protection Officer of the Controller. Only where the Other Party acts as the Controller, the Data Protection Officer of the Other Party shall communicate directly with Data Subject's. If the Other Party and the Controller act as Joint-Controllers, the Data Protection Officers of both parties coordinate how to and who responds to Data Subject's.

## 16. Right to Obtain Information, Right to Request Personal Data Transfer, Right to Correction or Erasure of Personal Data, Right to Restrict Processing, Right to Stop Processing, Right to Processing and Automated Processing

16.1 The Other Party shall take all appropriate technical and organizational measures and procedures to ensure the Data Subject's Rights, and to allow the Controller to comply with any request made by any Data Subject regarding the Right to Obtain Information, Right to Request Personal Data Transfer, Right to Correction or Erasure of Personal Data, Right to Restrict Processing, Right to Stop Processing, Right to Processing and Automated Processing and any other Right granted by Data Protection Legislation.

16.2 The Other Party shall provide appropriate and clear ways and mechanisms to enable the Data Subject to communicate with the Other Party and place requests regarding the Data Subject's Rights stipulated by PDPL. The Other Party shall inform the Controller about any request of a Data Subject regarding any Data Subject Right without undue delay.

## 17. Personal Data Security

17.1 The Other Party shall establish and take appropriate technical and organizational measures and procedures to ensure achievement of the information security level that is commensurate with the risks associated with Processing, in accordance with the best international standards and practices, which may include (a) encryption of Personal Data and application of Pseudonymization, and (b) application of procedures and measures that ensure the confidentiality, safety, validity and flexibility of Processing systems and services, and (c) application of procedures and measures that ensure the timely retrieval and access of Personal Data in the event of any physical or technical failure, and (d) application of procedures that ensure a smooth testing, evaluation and assessment of the effectiveness of technical and organizational measures so as to ensure the security of Processing. The Parties agreed on the


© All rights reserved by Heiko Maniero.

technical and organizational measures and procedures in APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

17.2 When evaluating the level of information security, the Other Party shall be taken into account (a) risks associated with Processing, including Personal Data damage, loss, accidental or illegal modification, disclosure or unauthorized access, whether transmitted, stored or Processed, and (b) the costs, nature, scope and purposes of Processing, as well as the different potential risks to the privacy and confidentiality of the Personal Data of the Data Subject.

## 18. Assessment of Personal Data Protection Impact

18.1 Subject to the nature, scope and purposes of Processing, the Other Party shall, before starting the Processing, assess the impact of the proposed Processing on Personal Data Protection, when using any of the modern technologies that would pose a high risk to the privacy and confidentiality of the Personal Data of the Data Subject (**Impact Assessment**).

18.2 The Impact Assessment shall be required (a) if the Processing involves a systematic and comprehensive assessment of the personal aspects of the Data Subject based on Automated Processing, including Profiling, which would have legal consequences or would seriously affect the Data Subject, and (b) if the Processing will be made on a large amount of Sensitive Personal Data.

18.3 The Impact Assessment must include, at a minimum (a) a clear and systematic explanation of the impact of the proposed Processing on Personal Data Protection and the purpose of such Processing, and (b) an assessment of the necessity and suitability of Processing for the purpose of PDPL, and (c) an assessment of the potential risks to the privacy and confidentiality of the Personal Data of the Data Subject, and (d) the proposed procedures and measures to minimize the potential risks to Personal Data Protection.

18.4 The Other Party may make a single assessment for a set of Processing operations of similar natures and risks.

18.5 The Other Party shall coordinate with the Data Protection Officer when assessing the impact of Personal Data Protection.

18.6 The Other Party shall review the assessment outcomes periodically to ensure that the Processing is carried out in accordance with the assessment, in case the levels of risks associated with the Processing operations are different.

## 19. Cross-Border Personal Data Transfer and Sharing for Processing Purposes if there is an Adequate Level of Protection

The Other Party may transfer Personal Data outside the United Arab Emirates in the following cases approved by the Office, namely (1) if the country or territory to which the Personal Data is to be transferred has special legislation on Personal Data Protection therein, including the most important provisions, measures, controls, requirements and rules for protecting the privacy and confidentiality of the Personal Data of the Data Subject and his/her ability to exercise his/her rights, and provisions related to imposing appropriate measures on the


© All rights reserved by Heiko Maniero.

Controller or Processor through a supervisory or judicial authority, and (2) if the United Arab Emirates accedes to bilateral or multilateral agreements related to Personal Data Protection with the countries to which the Personal Data is to be transferred.

## 20. Cross-Border Personal Data Transfer and Sharing for Processing Purposes if there is not an Adequate Level of Protection

20.1 With the exception of what is stated in Article 22 PDPL, the Other Party may transfer Personal Data outside the United Arab Emirates in the following cases: (a) In countries where there is no data protection law, Establishments operating in the United Arab Emirates and in those countries may transfer data under a contract or agreement that obliges the Establishment in those countries to implement the provisions, measures, controls and requirements set out by PDPL, including provisions related to imposing appropriate measures on the Controller or Processor through a competent supervisory or judicial authority in that country, which shall be specified in the contract, or (b) the express Consent of the Data Subject to transfer his/her Personal Data outside the United Arab Emirates in a manner that does not conflict with the security and public interest of the United Arab Emirates, or (c) if the transfer is necessary to fulfill obligations and establish, exercise or defend rights before judicial authorities, or (d) if the transfer is necessary to enter into or execute a contract between the Controller and Data Subject, or between the Controller and a other Party to achieve the Data Subject's interest, or (e) if the transfer is necessary to perform a procedure relating to international judicial cooperation, or (f) if the transfer is necessary to protect the public interest.

20.2 The Other Party shall observe and comply with the Executive Regulations of PDPL that set the controls and requirements for the cases referred above, which must be met for transferring Personal Data outside the United Arab Emirates.

20.3 Whereas the Other Party is an Establishment in a country where there is no data protection law, and receives Personal Data in a Cross-Border Personal Data Transfer from the Controller and/or receives Personal Data that is Shared for Processing Purposes by the Controller, the Other Party agrees to implement the provisions, measures, controls and requirements set out by PDPL, including provisions related to imposing appropriate measures on the Other Party through a competent supervisory or judicial authority. The competent judicial authority is the arbitral tribunal referred to in Section 23 of this Agreement. The parties agree that the UAE Data Office is the competent supervisory authority.

## 21. Obligations upon expiry or termination of the Services Agreement

21.1 Notwithstanding the Other Party's obligations under the Services Agreement following its expiry or termination, the Other Party shall promptly and in any event within thirty (30) days of the expiry or termination of the Services Agreement, at the Controller's option either delete or return (in such format and on such media or by such means as the Parties shall agree in writing) all copies of the Personal Data Processed by the Other Party and/or its Sub-Processors on behalf of the Controller or originating from the Controller.

21.2 Where the Controller has instructed the Other Party to delete the Personal Data, the Other Party shall do so in accordance with best industry practice for the reliable and secure deletion of data and for the secure destruction of confidential material.


© All rights reserved by Heiko Maniero.

21.3 The Other Party (and those of its Sub-Processors, as appropriate) may retain a copy of the Personal Data Processed by and under this Agreement to the extent required by any applicable law to which the Other Party (or any Sub-Processor) is subject and only for such period as shall be required by such applicable law. Where applicable, the Other Party shall notify the Controller of such requirement and shall ensure that such Personal Data are kept confidential and not Processed for any other Purpose.

21.4 The Controller may require the Other Party to provide a written certificate confirming that it has complied with its obligations under this Section.

## 22. Liability and indemnification

22.1 The Other Party shall be liable for any violation of Data Protection Legislation or this Agreement by the Other Party or its Sub-Processors.

22.2 The Other Party agrees to indemnify, defend, and hold harmless the Controller from and against any loss, cost, or damage of any kind (including reasonable outside attorneys' fees) to the extent arising out of any breach of Data Protection Legislation by the Other Party, and/or its negligence or willful misconduct, or its Sub-Processors.

## 23. Arbitration Clause

23.1 All disputes arising out of or in connection with this contract or its validity shall be finally settled under the rules of arbitration of the German Institution for Arbitration e. V. (DIS), excluding ordinary legal action.

23.2 The arbitral tribunal consists of a single arbitrator. The parties hereby irrevocably agree that the sole arbitrator may be appointed by attorney-at-law Mr. Ulrich Baumann and / or Prof. Dr. h.c. Heiko Jonny Maniero, whereby the above-mentioned persons can appoint themselves also to the arbitrator in the respective arbitration procedure, as far as the own designation no conflicts of interests stand against. The seat of the arbitral tribunal is Abu Dhabi.

23.3 The language of the proceedings is German.

23.4 The law applicable in the case is the Law of the United Arab Emirates.

## 24. General provisions

24.1 Except in respect of any provision of this Agreement that expressly or by implication is intended come into or continue in force on or after the expiry or termination of the Services Agreement, this Agreement shall be coterminous with the Services Agreement.

24.2 A Person who is not a Party to this Agreement shall not have any rights to enforce any terms of this Agreement.


© All rights reserved by Heiko Maniero.

24.3 If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this Clause shall not affect the validity and enforceability of the rest of this Agreement.

24.4 Except as expressly provided in this Agreement, no variation of this Agreement shall be effective unless it is in writing and signed by the Parties (or their authorized representatives).


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

# Standard Contract for Outbound Cross-border Transfer of Personal Information (People's Republic of China)

The Personal Information Handler and the Overseas Recipient will carry out the activities concerning the outbound cross-border transfer of Personal Information in accordance with this Contract. The Parties have entered into or agreed to enter into a commercial contract to further the commercial acts related to such activities, namely the Main-Agreement on the date of conclusion of the Main-Agreement.

The major body of this Contract is drafted in accordance with the requirements of the *Measures for the Standard Contract for Outbound Cross-border Transfer of Personal Information*. Other agreements between the Parties, if any, may be specified in Appendix II. The Appendix forms an integrated part of this Contract.

### *Article 1 Definitions*

In this Contract, unless the context otherwise requires:

1. "Personal Information Handler" refers to any organization or individual that independently decides the purpose and method of the Personal Information handling activities and transfers Personal Information outside the territory of the People's Republic of China.

2. "Overseas Recipient" refers to an organization or individual outside the territory of the People's Republic of China that receives Personal Information from the Personal Information Handler.

3. Personal Information Handler or Overseas Recipient are referred to individually as a "Party", and collectively as the "Parties".

4. "Personal Information Subject" refers to a natural person identified by or associated with the Personal Information.

5. "Personal Information" refers to all kinds of information related to identified or identifiable natural persons that are electronically or otherwise recorded, excluding information that has been anonymized.

6. "Sensitive Personal Information" refers to the Personal Information that, once leaked or illegally used, is likely to result in damage to the personal dignity of any natural person or damage to his or her personal or property safety, including biometric recognition, religious belief, specific identity, medical health, financial account, personal whereabouts, and the Personal Information of minors under the age of 14.

7. "Regulatory Authority" refers to the Cyberspace Administration of the People's Republic of China at the provincial level or above.

8. "Relevant Laws and Regulations" refer to the laws and regulations of the People's Republic of China, such as the *Cybersecurity Law of the People's Republic of China*, the *Data Security Law*


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

*of the People's Republic of China*, the *Personal Information Protection Law of the People's Republic of China*, the *Civil Code of the People's Republic of China*, *Civil Procedure Law of the People's Republic of China*, and *Measures for the Standard Contract for Outbound Cross-border Transfer of Personal Information*.

9. The meanings of other terms not defined in the Contract are in line with those stipulated in the Relevant Laws and Regulations.

***Article 2 Obligations of the Personal Information Handler***

The Personal Information Handler shall perform the following obligations:

1. Handle Personal Information in accordance with the Relevant Laws and Regulations. The Personal Information to be transferred overseas shall be limited to the minimum scope required for the purpose of handling.

2. Inform the Personal Information Subject of matters such as the name and contact information of the Overseas Recipient, the purpose of handling, method of handling, type of Personal Information, retention periods, and the methods and procedures for the Personal Information Subject to exercise his/her rights specified in Appendix I "*Description of the Outbound Cross-border Transfer of Personal Information*". Where Sensitive Personal Information is transferred overseas, the Personal Information Subject shall be informed of the necessity of the outbound cross-border transfer of Sensitive Personal Information and the impact on the rights and interests of the Personal Information Subject, unless otherwise provided in the laws and administrative regulations that such notification is not required.

3. If Personal Information is transferred overseas based on the consent of the individual, the separate consent of the Personal Information Subject shall be obtained. Where the Personal Information involves that of a minor under the age of 14, the separate consent of the minor's parent or any other guardian, shall be obtained. Where written consent is required by laws and administrative regulations, the written consent shall be obtained.

4. Inform the Personal Information Subject that the Personal Information Handler and the Overseas Recipient have agreed that the Personal Information Subject is a third-party beneficiary under this Contract, and if the Personal Information Subject fails to raise an express rejection within thirty days, the Personal Information Subject shall be entitled to act as a third-party beneficiary in accordance with the Contract.

5. Make reasonable efforts to ensure that the Overseas Recipient has taken the following technical and organizational measures to perform its obligations under this Contract (taking into account potential Personal Information security risks that may be caused by the purpose of Personal Information handling, the type, scale, scope and sensitivity of the Personal Information, the scale and frequency of the transfer, the period of the outbound cross-border transfer of Personal Information, the period of retention by the Overseas Recipient, and other matters that may lead to a Personal Information security risk): APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

6. Provide copies of Relevant Laws and Regulations and technical standards to the Overseas Recipient upon request.


© All rights reserved by Heiko Maniero.

7. Reply to inquiries from the Regulatory Authority about the Overseas Recipient's handling activities.

8. Carry out a Personal Information Protection Impact Assessment in accordance with the Relevant Laws and Regulations regarding the proposed transfer of Personal Information to the Overseas Recipient. The assessment shall focus on the following matters:

   (1) the legality, legitimacy and necessity of the purpose, scope and method of handling Personal Information by the Personal Information Handler and Overseas Recipient;

   (2) the scale, scope, type, and sensitivity of Personal Information to be transferred overseas, and the risks that the outbound cross-border transfer may pose to Personal Information rights and interests;

   (3) the obligations that the Overseas Recipient undertakes to assume, and whether the organizational and technical measures and capabilities to perform such obligations are sufficient to ensure the security of the Personal Information to be transferred overseas;

   (4) risk of Personal Information being tampered with, destroyed, leaked, lost, illegally used, etc. after the outbound cross-border transfer, and whether there are channels for individuals to smoothly exercise Personal Information rights and interests etc.;

   (5) in accordance with Article 4 hereof, to evaluate whether the performance of this Contract will be affected by the local policies and regulations with respect to protection of Personal Information; and

   (6) other matters that may affect the security of outbound cross-border transfer of Personal Information.

   The Personal Information Protection Impact Assessment Report shall be kept for at least three years.

9. Provide a copy of this Contract to the Personal Information Subject upon the Personal Information Subject 's request. If trade secrets or confidential business information are involved, the relevant contents of the copy of this Contract may be appropriately redacted, provided that such redaction will not affect the understanding of the Personal Information Subject.

10. Assume a burden of proof for the performance of obligations under this Contract.

11. In accordance with Relevant Laws and Regulations, provide the Regulatory Authority with all information as described in Article 3.11, including all compliance audit results.

### *Article 3 Obligations of the Overseas Recipient*

The Overseas Recipient shall perform the following obligations:

1. Handle the Personal Information in accordance with Appendix I "*Description of the Outbound Cross-border Transfer of Personal Information*". Where the Overseas Recipient handles the Personal Information in a way beyond the purpose and method of the Personal Information handling, and types of the Personal Information as agreed, it shall obtain the separate consent

 © All rights reserved by Heiko Maniero.

of the Personal Information Subject in advance if the handling of Personal Information is based on the consent of the Personal Information Subject; where the Personal Information of a minor under the age of 14 is involved, the separate consent of the minor's parent, or any other guardian, shall be obtained.

2. Where the Overseas Recipient is contracted by the Personal Information Handler to handle Personal Information, the Overseas Recipient shall handle the Personal Information in accordance with the agreement with the Personal Information Handler and shall not handle the Personal Information in a way beyond the purpose or method of the Personal Information handling.

3. Provide a copy of this Contract to the Personal Information Subject upon the Personal Information Subject's request. If trade secrets or other confidential business information are involved, relevant parts of this Contract may be appropriately redacted, provided that such redaction will not affect the understanding of the Personal Information Subject.

4. Handle the Personal Information in a manner that has the least impact on the rights and interests of the Personal Information Subject.

5. The retention period of Personal Information shall be the minimum period necessary for achieving the purpose of handling. Upon expiry of the retention period, the Personal Information (including all back-up copies) shall be deleted. Where the handling of Personal Information is contracted by the Personal Information Handler, and the personal information handling agreement fails to become effective, becomes null and void, or is cancelled or terminated, the Personal Information being handled shall be returned to the Personal Information Handler or deleted, and a written statement shall be provided to the Personal Information Handler. If it is technically difficult to delete the Personal Information, the handling of the Personal Information, other than the storage and any necessary measures taken for security protection, shall be ceased.

6. Ensure the security of Personal Information handling in the following ways:

   (1) take technical and organizational measures including but not limited to those listed in Article 2.5 of this Contract and carry out regular inspections to ensure the security of Personal Information; and

   (2) ensure that the personnel authorized to handle Personal Information perform their confidentiality obligations and establish access control permissions of minimum authorization.

7. In the event that Personal information is or may be tampered with, destroyed, leaked, lost, illegally used, provided or accessed without authorization, the Overseas Recipient shall:

   (1) promptly take appropriate measures to mitigate the adverse impact on the Personal Information Subject;

   (2) immediately notify the Personal Information Handler and report to the Regulatory Authority in accordance with the Relevant Laws and Regulations. The notice shall contain the following contents:


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

i. the type of Personal Information to which the tampering with, destruction, leakage, loss, illegal use, unauthorized provision or access occurs or may occur, the cause of such event or potential event, and the potential harm;

ii. remedial measures that have been taken;

iii. measures that can be taken by the Personal Information Subject to mitigate harm; and

iv. contact information of the person, or team, in charge of handling the situation.

(3) where the Relevant Laws and Regulations require the notification of the Personal Information Subject, the content of the notice shall include the foregoing contents in Article 3.7. (2) above; where the handling of Personal Information is contracted by the Personal Information Handler, the Personal Information Handler shall notify the Personal Information Subject;

(4) record and retain all the situations thereof relating to the occurrence or potential occurrence of tampering, destruction, leakage, loss, illegal use, unauthorized provision or access, including all remedial measures taken.

8. The Overseas Recipient may provide Personal Information to the third party located outside the territory of the People's Republic of China only, if all of the following requirements are met:

(1) there is a necessity from the business perspective;

(2) the Personal Information Subject has been informed of such third party's name, contact information, the purpose of handling, method of handling, type of Personal Information, retention periods, and the methods and procedures for the Personal Information Subject to exercise his/her rights. Where Sensitive Personal Information is provided to such third party, the Personal Information Subject should also be informed of the necessity of the outbound cross-border transfer of Sensitive Personal Information and the impact on the rights and interests of the Personal Information Subject. However, unless otherwise provided by laws and administrative regulations that such notification is not required;

(3) where the handling of Personal Information is based on the consent of the Personal Information Subject, the separate consent of the Personal Information Subject shall be obtained; where the Personal Information of a minor under the age of 14 is involved, the separate consent of the minor's parent, or any other guardian, shall be obtained. Where written consent is required by laws and administrative regulations, such written consent shall be obtained;

(4) enter into a written agreement with the third party to ensure that the handling of Personal Information by the third party meets the standards for protection of Personal Information required by the Relevant Laws and Regulations of the People's Republic of China, and the Overseas Recipient will assume the liability for the infringement of Personal Information Subject's rights due to the provision of Personal Information to the third party located outside the territory of the People's Republic of China;

(5) provide a copy of the above agreement to the Personal Information Subject upon the Personal Information Subject's request. If trade secrets or other confidential business


© All rights reserved by Heiko Maniero.

information are involved, relevant parts of the agreement may be appropriately redacted provided that such redaction will not affect the understanding of the Personal Information Subject.

9. Where the Overseas Recipient is contracted by the Personal Information Handler to handle Personal Information, and the Overseas Recipient intends to sub-contract the handling to a third party, the Overseas Recipient shall obtain the consent of the Personal Information Handler in advance and shall ensure that the sub-contractor will not handle Personal Information in a way beyond the purpose and method of the handling as specified in Appendix I "*Description of the Outbound Cross-border Transfer of Personal Information*", and shall monitor the Personal Information handling activities of the third party.

10. When making use of Personal Information for automated decision-making, the Overseas Recipient shall ensure the transparency of decision-making and fair and impartial results, and shall not carry out unreasonable or differential treatment of the Personal Information Subject in terms of transaction conditions, such as transaction price. Where automated decision-making is used for pushing information and commercial marketing to the Personal Information Subject, the Overseas Recipient shall also provide the Personal Information Subject with options that are not specific to the individuals' characteristics, or a convenient way for the Personal Information Subject to reject the automated decision-making.

11. Undertake to provide the Personal Information Handler with all necessary information required to comply with the obligations under this Contract, provide the Personal Information Handler access to review the necessary data documents, and files, or conduct a compliance audit of the handling activities under this Contract, and the Overseas Recipient shall facilitate the compliance audit conducted by the Personal Information Handler.

12. Maintain an accurate record of the Personal Information handling activities carried out for at least 3 years and provide the relevant records and documents to the Regulatory Authority directly or through the Personal Information Handler, as required by the Relevant Laws and Regulations.

**13.** Agree to be subject to supervision by the Regulatory Authority during an enforcement procedure related to supervising the implementation of this Contract, including but not limited to responding to inquiries and inspections by the Regulatory Authority, following the actions taken or decisions made by the Regulatory Authority, and providing written confirmation that necessary measures have been taken etc.

### *Article 4 The Impact of Personal Information Protection Policies and Regulations in the Overseas Recipient's Country or Region on the Performance of this Contract*

1. The Parties warrant that they have exercised reasonable care when entering into this Contract and are not aware of Personal Information protection policies and regulations in the Overseas Recipient's country or region (including any requirements on providing Personal Information or authorizing public authorities to access Personal Information) that would have an impact on the Overseas Recipient's performance of its obligations under this Contract.

2. The Parties declare that, when making the warranties in Article 4.1, they have conducted the assessment in conjunction with the following circumstances:

   (1) the specific circumstances of outbound cross-border transfer, including the purpose of


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

handling the Personal Information, the types, scale, scope and sensitivity of the Personal Information transferred, the scale and frequency of transfer, the period of the outbound cross-border transfer of Personal Information and the retention period of the Overseas Recipient, the previous experience of the Overseas Recipient with respect to outbound cross-border transfer and handling of similar Personal Information, whether any Personal Information security incident had occurred to the Overseas Recipient and whether such incident was timely and effectively handled, whether the Overseas Recipient has received any request to provide Personal Information to the public authority of the country or region where it is located and how the Overseas Recipient has responded to such request;

(2) the Personal Information protection policies and regulations of the country or region where the Overseas Recipient is located, including the following elements:

i. the existing Personal Information protection laws, regulations and generally applicable standards of the country or region;

ii. the regional or global organizations of Personal Information protection that the country or region accedes to, and binding international commitments made by the country or region; and

iii. the mechanisms for Personal Information protection implemented in the country or region, such as whether there are supervision and enforcement authorities and relevant judicial authorities responsible for protecting Personal Information.

(3) the Overseas Recipient's security management system and technical capabilities.

3. The Overseas Recipient warrants that it has used its best efforts to provide the Personal Information Handler with the necessary relevant information for the assessment under Article 4.2.

4. The Parties shall keep a record of any such assessment carried out under Article 4.2 as well as the assessment results.

5. Where the Overseas Recipient is unable to perform this Contract due to any change in the policies and regulations on Personal Information protection of the country or region where the Overseas Recipient is located (including any change of laws or mandatory measures in the country or region where the Overseas Recipient is located), the Overseas Recipient shall notify the Personal Information Handler immediately after being aware of the aforesaid change.

6. If the Overseas Recipient receives a request for provision of Personal Information under this Contract from a governmental authority or judicial authority in the country or region where the Overseas Recipient is located, it shall promptly notify the Personal Information Handler.

### *Article 5 Rights of the Personal Information Subject*

The Parties agree that the Personal Information Subject shall be entitled to the following rights as a third-party beneficiary under this Contract.

1. The Personal Information Subject, in accordance with Relevant Laws and Regulations, has the right to know and to make decisions on the handling of the Personal Information, the right

 © All rights reserved by Heiko Maniero.

to restrict or refuse handling of the Personal Information Subject's Personal Information by others, the right to request access to, copy, correct, supplement or delete the Personal Information, and the right to request others to explain the rules for the handling of the Personal Information Subject's Personal Information.

2. When the Personal Information Subject requests to exercise the above-mentioned rights regarding their Personal Information that has been transferred overseas, the Personal Information Subject may request the Personal Information Handler to take appropriate measures for the realization of those rights, or directly make the request to the Overseas Recipient. If the Personal Information Handler is unable to realize those rights, it shall notify the Overseas Recipient and request the Overseas Recipient to assist in the realization.

3. The Overseas Recipient shall, as notified by the Personal Information Handler or requested by the Personal Information Subject, realize the rights that the Personal Information Subject is entitled to within a reasonable period and in accordance with the Relevant Laws and Regulations.

   The Overseas Recipient shall inform the Personal Information Subject about the relevant information which shall be true, accurate and complete, in an obvious way and using clear and understandable language.

4. If the Overseas Recipient intends to refuse the request of the Personal Information Subject, it shall inform the Personal Information Subject the reasons of the refusal, as well as the channels for the Personal Information Subject to raise complaints with the relevant Regulatory Authority and seek judicial remedies.

5. The Personal Information Subject, as a third-party beneficiary to this Contract, has the right to claim against one or both, the Personal Information Handler and the Overseas Recipient, in accordance with this Contract and require them to perform the following clauses under this Contract relating to the rights of the Personal Information Subject:

   (1) Article 2, except for Articles 2.5, 2.6 and 2.7;
   (2) Article 3, except for Articles 3.7(2) and 3.7(4), 3.9, 3.11, 3.12 and 3.13;
   (3) Article 4, except for Articles 4.5 and 4.6;
   (4) Article 5;
   (5) Article 6;
   (6) Article 8.2 and 8.3; and
   (7) Article 9.5.

   The above agreement shall not affect the rights and interests of the Personal Information Subject in accordance with the Personal Information Protection Law of the People's Republic of China.

### *Article 6 Remedies*

1. The Overseas Recipient shall identify a contact person who is authorized to respond to enquiries or complaints concerning the handling of Personal Information, and it shall promptly deal with any enquiries or complaints from the Personal Information Subject. The Overseas Recipient shall notify the Personal Information Handler of the contact information and shall


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

inform the Personal Information Subject of the contact information in a manner which is easy to understand, by separate notice or announcement on its website. To be specific: The contact person who is authorized to respond to enquiries or complaints concerning the handling of Personal Information is the Data Protection Officer of the Overseas Recipient, that can be contacted over the phone number and email address published on the website of the Overseas Recipient. For more details, see Appendix "CAC", that will be or is filed with the local CAC.

2. If a dispute arises between either Party and the Personal Information Subject with respect to the performance of this Contract, such Party shall notify the other Party and the Parties shall cooperate to resolve the dispute.

3. If the dispute cannot be resolved amicably and the Personal Information Subject exercises the rights as a third-party beneficiary in accordance with Article 5, the Overseas Recipient shall accept that the Personal Information Subject may safeguard his/her rights through either of the following means:

   (1) lodging a complaint with the Regulatory Authority; and

   (2) bringing a lawsuit to the court specified in Article 6.5.

4. The Parties agree that when the Personal Information Subject exercises the rights as a third-party beneficiary with respect to a dispute under this Contract, if the Personal Information Subject chooses to apply the Relevant Laws and Regulations of the People's Republic of China, such choice shall prevail.

5. The parties agree that if the Personal Information Subject exercises the rights as a third-party beneficiary with respect to a dispute under this Contract, the Personal Information Subject may file a lawsuit with a competent court in accordance with the Civil Procedure Law of the People's Republic of China.

6. The Parties agree that the choices made by the Personal Information Subject to safeguard his/her rights will not impair the rights of the Personal Information Subject to seek remedies in accordance with other laws and regulations.

### *Article 7 Termination of the Contract*

1. If the Overseas Recipient breaches the obligations specified in this Contract or the Overseas Recipient is unable to perform this Contract due to a change in the policies and regulations on Personal Information protection in the Overseas Recipient's country or region (including amendment to the laws or adoption of compulsory measures in the Overseas Recipient's country or region), the Personal Information Handler may suspend the provision of Personal Information to the Overseas Recipient until the breach is corrected or the Contract is terminated.

2. In case of any of the following circumstances, the Personal Information Handler shall be entitled to terminate this Contract and notify the Regulatory Authority where necessary:

   (1) where the Personal Information Handler has suspended the provision of Personal Information to the Overseas Recipient for more than one month in accordance with Article 7.1;

   (2) the Overseas Recipient's compliance with this Contract will violate the laws and

 © All rights reserved by Heiko Maniero.

regulations of its own country or region;

(3) the Overseas Recipient seriously or persistently breaches the obligations under this Contract;

(4) the Overseas Recipient or the Personal Information Handler have breached this Contract pursuant to a final decision of a competent court or the regulatory body supervising the Overseas Recipient; and

The Overseas Recipient may also terminate this Contract in case of sub-paragraph (1), (2) or (4) of above.

3. The Contract may be terminated upon mutual agreement by the Parties, provided that such termination shall not exempt the Parties from the obligations of protecting Personal Information during the handling of the Personal Information.

4. If the Contract is terminated, the Overseas Recipient shall promptly return or delete the Personal Information (including all back-up copies) received hereunder and provide the Personal Information Handler with a written statement. If it is technically difficult to delete the Personal Information, any handling of the Personal Information, other than the storage and taking necessary security protection measures, shall be ceased.

### *Article 8 Liability for Breach of the Contract*

1. Each Party shall be liable to the other Party for any damage as a result of its breach of this Contract.

2. Each Party shall bear civil liabilities to the Personal Information Subject if its breach of this Contract infringes the rights of the Personal Information Subject, without prejudice to the administrative, criminal or other legal liabilities that shall be assumed by the Personal Information Handler under the Relevant Laws and Regulations.

3. The Parties shall assume joint and several liability in accordance with the law. The Personal Information Subject shall have the right to request each Party or the Parties to assume liability. When the liability assumed by one Party exceeds the liability such Party shall be assumed, it shall have the right to claim against the other Party accordingly.

### *Article 9 Miscellaneous*

1. If this Contract conflicts with any other legal documents existing between the Parties, the provisions of this Contract shall prevail.

2. The formation, validity, performance and interpretation of this Contract and any dispute between the Parties arising from this Contract shall be governed by the Relevant Laws and Regulations of the People's Republic of China.

3. All notices shall be promptly transmitted or posted by electronic mail, cable, telex, facsimile (confirmation copy sent by airmail), or registered airmail to (specified address in the Main Agreement or such other address as may be substituted for such address by written notice). Receipt of any notice under this Contract shall be deemed to have been received seven days


© All rights reserved by Heiko Maniero.

after its postmark-date in the case of registered airmail and three working days after dispatch in the case of e-mail, cable, telex or facsimile transmission.

4. Any dispute arising from this Contract between the Parties, the Personal Information Handler and the Overseas Recipient, as well as a claim by either Party against the other for recovery of compensation already paid to the Personal Information Subject, shall be resolved by the Parties through negotiation; if such negotiation fails, either Party may adopt any of the following methods to resolve the dispute (check the box for the chosen arbitration institution, if arbitration is required):

(1) Arbitration. The dispute shall be submitted to:

☐ China International Economic and Trade Arbitration Commission
☐ China Maritime Arbitration Commission
☐ Beijing Arbitration Commission (Beijing International Arbitration Center)
☐ Shanghai International Arbitration Center
X Other arbitration institutions that are members of the Convention on the Recognition and Enforcement of Overseas Arbitral Awards

The arbitration shall be conducted in Munich, Germany (the place of arbitration) in accordance with its arbitration rules then in force.

(2) Litigation. Submit the dispute to a Chinese court with jurisdiction in accordance with the applicable laws.

5. This Contract shall be interpreted in accordance with Relevant Laws and Regulations and shall not be interpreted in a manner inconsistent with the rights and obligations set forth in Relevant Laws and Regulations.

6. This Contract shall be executed in two originals, and the Parties, the Personal Information Handler and the Overseas Recipient, shall each hold one original(s), with equal legal effect.

This contract is signed or concluded online (implemented as terms and conditions and is and original and valid without signature).

**Personal Information Handler:** Authorized Person, that signed the Main Agreement

Date: Date of Main Agreement

**Overseas Recipient**: Authorized Person, that signed the Main Agreement

Date: Date of Main Agreement


© All rights reserved by Heiko Maniero.

## *Appendix I*

### *Description of the Outbound Cross-border Transfer of Personal Information*

The details of the outbound cross-border transfer of Personal Information under this Contract are as follows:

1. Purpose of handling: see APPENDIX 8 – DESCRIPTION OF THE PROCESSING OR THE TRANSFER

2. Method of handling: published as "Nature of (sub-) processing" in APPENDIX 8 – DESCRIPTION OF THE PROCESSING OR THE TRANSFER

3. The scale of Personal Information to be transferred overseas: Processing and transfer on a small scale. For more details, see Appendix "CAC", that will be or is filed with the local CAC.

4. Type of Personal Information to be transferred overseas ( please refer to the *Information Security Technologies - Personal Information Security Specifications (GB/T 35273)* and relevant standards):

   Personal Information (3.1 in GB/T 35273-2020)
   PI Subject (3.3 in GB/T 35273-2020)
   PI Controller (3.4 in GB/T 35273-2020)
   Explicit consent (3.6 in GB/T 35273-2020)
   Consent (3.7 in GB/T 35273-2020)
   Personalized display (3.16 in GB/T 35273-2020)
   Business function (3.17 in GB/T 35273-2020)

   For more details, see Appendix "CAC", that will be or is filed with the local CAC.

5. Type of Sensitive Personal Information to be transferred abroad (please refer to the *Information Security Technologies - Personal Information Security Specifications (GB/T 35273)* and relevant standards, if applicable): None.

6. The Overseas Recipient transfers Personal Information only to the following third parties outside the People's Republic of China (if applicable): N/A.

7. Method of transfer: Online Transfer.

8. Retention period after the cross-border transfer:

   From date of Main Agreement to Date of Termination of Main Agreement (which cannot be determined yet).

9. Storage location after the outbound cross-border transfer: Office und legal entity address of Overseas Recipient, or its sub-processors storage locations.

10. Other matters (to be filled in as appropriate): None.

## *Appendix II*


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

Other Terms as Agreed by the Parties (If Necessary): None.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

# Standard Contract for Outbound Cross-border Transfer of Personal Information (People's Republic of China)

为了确保境外接收方处理个人信息的活动达到中华人民共和国相关法律法规规定的个人信息保护标准，明确个人信息处理者和境外接收方个人信息保护的权利和义务，经双方协商一致，订立本合同。

**双方确认并同意，本合同的中文版本为双方签订的正式版本。 非正式的英文翻译版本仅供无法阅读中文的人士理解参考。 如果双方同意签订本合同的英文版本，该等同意应被理解为双方已经签订了本合同的中文版本。**

个人信息处理者：见附件 7-相关方名单

地址：见附件 7-相关方名单

联系方式：见附件 7-相关方名单

联系人：见附件 7-相关方名单　　职务：见附件 7-相关方名单


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

境外接收方：见附件 7-相关方名单

地址：见附件 7-相关方名单

联系方式：见附件 7-相关方名单

联系人：见附件 7-相关方名单　　职务：见附件 7-相关方名单


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

个人信息处理者与境外接收方依据本合同约定开展个人信息出境活动，与此活动相关的商业行为，双方【已】/【约定】于【主协议签订日期】订立一份商业合同，即主协议。

本合同正文根据《个人信息出境标准合同办法》的要求拟定，在不与本合同正文内容相冲突的前提下，双方如有其他约定可在附录二中详述，附录构成本合同的组成部分。

## 第一条 定义

在本合同中，除上下文另有规定外：

（一）"个人信息处理者"是指在个人信息处理活动中自主决定处理目的、处理方式的，向中华人民共和国境外提供个人信息的组织、个人。

（二）"境外接收方"是指在中华人民共和国境外自个人信息处理者处接收个人信息的组织、个人。

（三）个人信息处理者或者境外接收方单称"一方"，合称"双方"。

（四）"个人信息主体"是指个人信息所识别或者关联的自然人。

（五）"个人信息"是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

（六）"敏感个人信息"是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

（七）"监管机构"是指中华人民共和国省级以上网信部门。

（八）"相关法律法规"是指《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国民法典》《中华人民共和国民事诉讼法》《个人信息出境标准合同办法》等中华人民共和国法律法规。

（九）本合同其他未定义术语的含义与相关法律法规规定的含义一致。

## 第二条 个人信息处理者的义务

个人信息处理者应当履行下列义务：

（一）按照相关法律法规规定处理个人信息，向境外提供的个人信息仅限于实现处理目的所需的最小范围。

（二）向个人信息主体告知境外接收方的名称或者姓名、联系方式、附录一"个人信息出境说明"中处理目的、处理方式、个人信息的种类、保存期限，以及行使个人信息主体权利的方式和程序等事项。向境外提供敏感个人信息的，还应当向个人信息主体告知提供敏感个人信息的必要性以及对个人权益的影响。但是法律、行政法规规定不需要告知的除外。

（三）基于个人同意向境外提供个人信息的，应当取得个人信息主体的单独同意。涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。法律、行政法规规定应当取得书面同意的，应当取得书面同意。

（四）向个人信息主体告知其与境外接收方通过本合同约定个人信息主体为第三方受益人，如个人信息主体未在 30 日内明确拒绝， 则可以依据本合同享有第三方受益人的权利。

（五）尽合理地努力确保境外接收方采取如下技术和管理措施


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

（综合考虑个人信息处理目的、个人信息的种类、规模、范围及敏感程度、传输的数量和频率、个人信息传输及境外接收方的保存期限等可能带来的个人信息安全风险），以履行本合同约定的义务：详见附件 9 – 技术和管理措施

（六）根据境外接收方的要求向境外接收方提供相关法律规定和技术标准的副本。

（七）答复监管机构关于境外接收方的个人信息处理活动的询问。

（八）按照相关法律法规对拟向境外接收方提供个人信息的活动开展个人信息保护影响评估。重点评估以下内容：

1.个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性。

2.出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对个人信息权益带来的风险。

3.境外接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全。

4.个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等。

5.按照本合同第四条评估当地个人信息保护政策和法规对合同履行的影响。

6.其他可能影响个人信息出境安全的事项。保


© All rights reserved by Heiko Maniero.

存个人信息保护影响评估报告至少 3 年。

（九）根据个人信息主体的要求向个人信息主体提供本合同的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对本合同副本相关内容进行适当处理。

（十）对本合同义务的履行承担举证责任。

（十一）根据相关法律法规要求，向监管机构提供本合同第三条第十一项所述的信息，包括所有合规审计结果。

## 第三条 境外接收方的义务

境外接收方应当履行下列义务：

（一）按照附录一"个人信息出境说明"所列约定处理个人信息。如超出约定的处理目的、处理方式和处理的个人信息种类，基于个人同意处理个人信息的，应当事先取得个人信息主体的单独同意；涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。

（二）受个人信息处理者委托处理个人信息的，应当按照与个人信息处理者的约定处理个人信息，不得超出与个人信息处理者约定的处理目的、处理方式等处理个人信息。

（三）根据个人信息主体的要求向个人信息主体提供本合同的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对本合同副本相关内容进行适当处理。

（四）采取对个人权益影响最小的方式处理个人信息。

（五）个人信息的保存期限为实现处理目的所必要的最短时间， 保存期限届满的，应当删除个人信息（包括所有备份）。受个人信息处理者委托处理个人信息，委托合同未生效、无效、被撤销或者终止的，应当将个人信息返还个人信息处理者或者予以删除，并向个人信息处理者提供书面说明。删除个人信息从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理。


© All rights reserved by Heiko Maniero.

（六）按下列方式保障个人信息处理安全：

1.采取包括但不限于本合同第二条第五项的技术和管理措施，并定期进行检查，确保个人信息安全。

2.确保授权处理个人信息的人员履行保密义务，并建立最小授权的访问控制权限。

（七）如处理的个人信息发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问，应当开展下列工作：

1.及时采取适当补救措施，减轻对个人信息主体造成的不利影响。

2.立即通知个人信息处理者，并根据相关法律法规要求报告监管机构。通知应当包含下列事项：

（1）发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问的个人信息种类、原因和可能造成的危害。

（2）已采取的补救措施。

（3）个人信息主体可以采取的减轻危害的措施。

（4）负责处理相关情况的负责人或者负责团队的联系方式。


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

3.相关法律法规要求通知个人信息主体的，通知的内容包含本项第2目的事项。受个人信息处理者委托处理个人信息的，由个人信息处理者通知个人信息主体。

4.记录并留存所有与发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问有关的情况，包括采取的所有补救措施。

（八）同时符合下列条件的，方可向中华人民共和国境外的第三方提供个人信息：

1.确有业务需要。

2.已告知个人信息主体该第三方的名称或者姓名、联系方式、处理目的、处理方式、个人信息种类、保存期限以及行使个人信息主体权利的方式和程序等事项。向第三方提供敏感个人信息的，还应当向个人信息主体告知提供敏感个人信息的必要性以及对个人权益的影响。但是法律、行政法规规定不需要告知的除外。

3.基于个人同意处理个人信息的，应当取得个人信息主体的单独同意。涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。法律、行政法规规定应当取得书面同意的，


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

应当取得书面同意。

4.与第三方达成书面协议，确保第三方的个人信息处理活动达到中华人民共和国相关法律法规规定的个人信息保护标准，并承担因向中华人民共和国境外的第三方提供个人信息而侵害个人信息主体享有权利的法律责任。

5.根据个人信息主体的要求向个人信息主体提供该书面协议的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对该书面协议相关内容进行适当处理。

（九）受个人信息处理者委托处理个人信息，转委托第三方处理的，应当事先征得个人信息处理者同意，要求该第三方不得超出本合同附录一"个人信息出境说明"中约定的处理目的、处理方式等处理个人信息，并对该第三方的个人信息处理活动进行监督。

（十）利用个人信息进行自动化决策的，应当保证决策的透明度和结果公平、公正，不得对个人信息主体在交易价格等交易条件上实行不合理的差别待遇。通过自动化决策方式向个人信息主体进行信息推送、商业营销的，应当同时提供不针对其个人特征的选项，或者向个人信息主体提供便捷的拒绝方式。

（十一）承诺向个人信息处理者提供已遵守本合同义务所需的必要信息，允许个人信息处理者对必要数据文件和文档进行查阅，或者对本合同涵盖的处理活动进行合规审计，并为个人信息处理者开展合规审计提供便利。

（十二）对开展的个人信息处理活动进行客观记录，保存记录至少3 年，并按照相关法律法规要求直接或者通过个人信息处理者向监


© All rights reserved by Heiko Maniero.

管机构提供相关记录文件。

（十三）同意在监督本合同实施的相关程序中接受监管机构的监督管理，包括但不限于答复监管机构询问、配合监管机构检查、服从监管机构采取的措施或者作出的决定、提供已采取必要行动的书面证明等。

## 第四条

## 境外接收方所在国家或者地区个人信息保护政策和法规对合同履行的影响

（一）双方应当保证在本合同订立时已尽到合理注意义务，未发现境外接收方所在国家或者地区的个人信息保护政策和法规（包括任何提供个人信息的要求或者授权公共机关访问个人信息的规定）影响境外接收方履行本合同约定的义务。

（二）双方声明，在作出本条第一项的保证时，已经结合下列情形进行评估：

1.出境的具体情况，包括个人信息处理目的、传输个人信息的种类、规模、范围及敏感程度、传输的规模和频率、个人信息传输及境外接收方的保存期限、境外接收方此前类似的个人信息跨境传输和处理相关经验、境外接收方是否曾发生个人信息安全相关事件及是否进行了及时有效地处置、境外接收方是否曾收到其所在国家或者地区公共机关要求其提供个人信息的请求及境外接收方应对的情况。

2.境外接收方所在国家或者地区的个人信息保护政策和法规，包括下列要素：

（1） 该国家或者地区现行的个人信息保护法律法规及普遍适用


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

的标准。

（2） 该国家或者地区加入的区域性或者全球性的个人信息保护方面的组织，以及所作出的具有约束力的国际承诺。

（3） 该国家或者地区落实个人信息保护的机制，如是否具备个人信息保护的监督执法机构和相关司法机构等。

3.境外接收方安全管理制度和技术手段保障能力。

（三）境外接收方保证，在根据本条第二项进行评估时，已尽最大努力为个人信息处理者提供了必要的相关信息。

（四）双方应当记录根据本条第二项进行评估的过程和结果。

（五）因境外接收方所在国家或者地区的个人信息保护政策和法规发生变化（包括境外接收方所在国家或者地区更改法律，或者采取强制性措施）导致境外接收方无法履行本合同的，境外接收方应当在知道该变化后立即通知个人信息处理者。

（六）境外接收方接到所在国家或者地区的政府部门、司法机构关于提供本合同项下的个人信息要求的，应当立即通知个人信息处理者。

## 第五条 个人信息主体的权利

双方约定个人信息主体作为本合同第三方受益人享有以下权利：


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

（一）个人信息主体依据相关法律法规，对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理， 有权要求查阅、复制、更正、补充、删除其个人信息，有权要求对其个人信息处理规则进行解释说明。

（二）当个人信息主体要求对已经出境的个人信息行使上述权利时，个人信息主体可以请求个人信息处理者采取适当措施实现，或者直接向境外接收方提出请求。个人信息处理者无法实现的，应当通知并要求境外接收方协助实现。

（三）境外接收方应当按照个人信息处理者的通知，或者根据个人信息主体的请求，在合理期限内实现个人信息主体依照相关法律法规所享有的权利。

境外接收方应当以显著的方式、清晰易懂的语言真实、准确、完整地告知个人信息主体相关信息。

（四）境外接收方拒绝个人信息主体的请求的，应当告知个人信息主体其拒绝的原因，以及个人信息主体向相关监管机构提出投诉和寻求司法救济的途径。

（五）个人信息主体作为本合同第三方受益人有权根据本合同条款向个人信息处理者和境外接收方的一方或者双方主张并要求履行本合同项下与个人信息主体权利相关的下列条款：

1. 第二条，但第二条第五项、第六项、第七项、第十一项除外。

2. 第三条，但第三条第七项第 2 目和第 4 目、第九项、第十一项、第十二项、第十三项除外。

3. 第四条，但第四条第五项、第六项除外。

4. 第五条。

5. 第六条。


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

6.第八条第二项、第三项。

7.第九条第五项。

上述约定不影响个人信息主体依据《中华人民共和国个人信息保护法》享有的权益。

## 第六条 救济

（一）境外接收方应当确定一个联系人，授权其答复有关个人信息处理的询问或者投诉，并应当及时处理个人信息主体的询问或者投诉。境外接收方应当将联系人信息告知个人信息处理者，并以简洁易懂的方式，通过单独通知或者在其网站公告，告知个人信息主体该联系人信息，具体为：境外接收方授权答复有关个人信息处理的询问或者投诉的联系人为境外接收方的数据保护人员。个人信息主体可通过境外接收方网站公布的电话及电子邮件联系该等人员。更多详情，请参见附件"中国互联网信息办公室"，该文件将向或已向当地的中国互联网信息办公室备案。

（二）一方因履行本合同与个人信息主体发生争议的，应当通知另一方，双方应当合作解决争议。

（三）争议未能友好解决，个人信息主体根据第五条行使第三方受益人的权利的，境外接收方接受个人信息主体通过下列形式维护权利：

1.向监管机构投诉。

2.向本条第五项约定的法院提起诉讼。

（四）双方同意个人信息主体就本合同争议行使第三方受益人权利，个人信息主体选择适用中华人民共和国相关法律法规的，从其选择。

（五）双方同意个人信息主体就本合同争议行使第三方受益人权利的，个人信息主体可以依据《中华人民共和国民事诉讼法》向有管辖权的人民法院提起诉讼。


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

（六）双方同意个人信息主体所作的维权选择不会减损个人信息主体根据其他法律法规寻求救济的权利。

## 第七条 合同解除

（一）境外接收方违反本合同约定的义务，或者境外接收方所在国家或者地区的个人信息保护政策和法规发生变化（包括境外接收方所在国家或者地区更改法律，或者采取强制性措施）导致境外接收方无法履行本合同的，个人信息处理者可以暂停向境外接收方提供个人信息，直到违约行为被改正或者合同被解除。

（二）有下列情形之一的，个人信息处理者有权解除本合同，并在必要时通知监管机构：

1.个人信息处理者根据本条第一项的规定暂停向境外接收方提供个人信息的时间超过 1 个月。

2.境外接收方遵守本合同将违反其所在国家或者地区的法律规定。

3.境外接收方严重或者持续违反本合同约定的义务。

4.根据境外接收方的主管法院或者监管机构作出的终局决定，境外接收方或者个人信息处理者违反了本合同约定的义务。

在本项第 1 目、第 2 目、第 4 目的情况下，境外接收方可以解除本合同。

（三）经双方同意解除本合同的，合同解除不免除其在个人信息处理过程中的个人信息保护义务。


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

（四）合同解除时，境外接收方应当及时返还或者删除其根据本合同所接收到的个人信息（包括所有备份），并向个人信息处理者提供书面说明。删除个人信息从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理。

## 第八条 违约责任

（一）双方应就其违反本合同而给对方造成的损失承担责任。

（二）任何一方因违反本合同而侵害个人信息主体享有的权利， 应当对个人信息主体承担民事法律责任，且不影响相关法律法规规定个人信息处理者应当承担的行政、刑事等法律责任。

（三）双方依法承担连带责任的，个人信息主体有权请求任何一方或者双方承担责任。一方承担的责任超过其应当承担的责任份额时，有权向另一方追偿。

## 第九条 其他

（一）如本合同与双方订立的任何其他法律文件发生冲突，本合同的条款优先适用。

（二）本合同的成立、效力、履行、解释、因本合同引起的双方间的任何争议，适用中华人民共和国相关法律法规。

（三）发出的通知应当以电子邮件、电报、电传、传真（以航空信件寄送确认副本）或者航空挂号信发往（具体地址以主协议中载明的地址为准）

或者书面通知取代该地址的其它地址。如以航空挂号信寄出本合同项下的通知，在邮戳日期后的 7 天应当视为收讫；如以电子邮件、电报、电传或者传真发出，在发出以后的 3 个工作日应当视为收讫。

（四）双方因本合同产生的争议以及任何一方因先行赔偿个人信息主体损害赔偿责任而向另一方的追偿，双方应当协商解决；协商解决不成的，任何一方可以采取下列第_种方式加以解决（如选择仲裁，请勾选仲裁机构）：

1. 仲裁。将该争议提交


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

□中国国际经济贸易仲裁委员会

□中国海事仲裁委员会

□北京仲裁委员会（北京国际仲裁中心）

□上海国际仲裁中心

√其他《承认及执行外国仲裁裁决公约》成员的仲裁机构_____

按其届时有效的仲裁规则在 德国慕尼黑 进行仲裁；

2.诉讼。依法向中华人民共和国有管辖权的人民法院提起诉讼。

（五）本合同应当按照相关法律法规的规定进行解释，不得以与相关法律法规规定的权利、义务相抵触的方式解释本合同。

（六）本合同正本一式贰份，双方各执 壹份，其法律效力相同。本合同于线上签订或签署（且可作为原始、有效的条款和条件执行，无需签名）


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

个人信息处理者：[签署主协议的授权签字人]_____

_____年_____月_____日[主协议签署日期]

境外接收方：[签署主协议的授权签字人]_____

_____年_____月_____日[主协议签署日期]

**附录一**

## 个人信息出境说明

根据本合同向境外提供个人信息的详情约定如下：

（一）处理目的：见附件 8-处理或传输说明

（二）处理方式：见附录 8-处理或传输说明中的“（次级）处理性质”


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

（三）出境个人信息的规模：小规模处理及传输个人信息。更多详情，请参见附件"中国互联网信息办公室"，该文件将向或已向当地的中国互联网信息办公室备案。

（四）出境个人信息种类（参考 GB/T 35273《信息安全技术 个人信息安全规范》和相关标准）：

个人信息（参考 GB/T 35273-2020 第 3.1 条）

个人信息主体（参考 GB/T 35273-2020 第 3.3 条）

个人信息控制者（参考 GB/T 35273-2020 第 3.4 条）

明示同意（参考 GB/T 35273-2020 第 3.6 条）

授权同意（参考 GB/T 35273-2020 第 3.7 条）

个性化展示（参考 GB/T 35273-2020 第 3.16 条）

业务功能（参考 GB/T 35273-2020 第 3.17 条）

更多详情，请参见附件"中国互联网信息办公室"，该文件将向或已向当地的中国互联网信息办公室备案。

（五）出境敏感个人信息种类（如适用，参考 GB/T 35273《信息安全技术 个人信息安全规范》和相关标准）：无

（六）境外接收方只向以下中华人民共和国境外第三方提供个人信息（如适用）：不适用

（七）传输方式：网络在线传输


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

（八）出境后保存期限：

自主协议生效之日至主协议终止之日（待确定）

（九）出境后保存地点：境外接收方的办公地址或注册地址，或其次级信息处理者的保存地点。

（十）其他事项（视情况填写）：无

**附录二**

## 双方约定的其他条款（如需要）

无。


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.

# Data Processing Agreement and National Joint Controllership Agreement to comply with PIPL (People's Republic of China)

This Data Processing Agreement and National Joint Controllership Agreement to comply with PIPL (People's Republic of China) (**Agreement**) is concluded on the same date as the Services Agreement (as defined below) and is concluded by and between

(1) the **Personal Information Handler**, named with its Company details as a Party in the Services Agreement (as defined below), and

(2) the **Entrusted Person**, named with its Company details as a Party in the Services Agreement (as defined below).

(together the **Parties**)

## 1. Preamble

1.1 The Entrusted Person is a provider of professional services (**Services**) and/or provides its Services as a Joint-Controller and is based in the People's Republic of China. The Personal Information Handler is also based in the People's Republic of China. The Parties entered into an agreement which describes the Services provided by the Entrusted Person acting on behalf of the Personal Information Handler, or acting jointly with the Personal Information Handler, in more detail (**Services Agreement**).

1.2 The Parties have agreed to enter into this Agreement in relation to the Processing of Personal Information by the Entrusted Person, or jointly by the Entrusted Person and the Personal Information Handler, in the course of providing the Services. The terms of this Agreement are intended to apply in addition to and not in substitution of the terms of the Services Agreement.

1.3 This Agreement applies to all activities involving the Handling of Personal Information of natural persons within the borders of the People's Republic of China.

## 2. Definitions and interpretation

2.1 **PIPL** means the Personal Information Protection Law of the People's Republic of China, passed at the 30th meeting of the Standing Committee of the 13th National People's Congress on August 20, 2021, that entered into force on November 1, 2021, as amended or superseded from time to time. The legal definitions from Article 73 PIPL shall apply.

2.2 **Personal Information** means all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization Handling.


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

2.3 **Personal Information Handling** includes Personal Information collection, storage, use, processing, transmission, provision, disclosure, deletion, etc.

2.4 **Sensitive Personal Information** means Personal Information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the Personal Information of minors under the age of 14.

2.5 **Data Protection Officer** means the Personal Information Protection Officer.

2.6 **Joint-Controller** means an Entrusted Person that qualifies as a Second PI Handler that jointly decides with the Personal Information Handler on the Personal Information Handling purposes and Handling methods.

2.7 **Data Protection Legislation** means the Personal Information Protection Law of the People's Republic of China as well as any regulation adopted, published, administered, implemented, or enforced by the Government of the People's Republic of China, as amended or superseded from time to time, and any related case-law.

## 3. General Obligations

3.1 Each Party shall comply with all applicable requirements of Data Protection Legislation. This Clause is in addition to, and does not relieve any Party from complying with, a Party's obligations under Data Protection Legislation.

3.2 If the Entrusted Person is Handling Personal Information on behalf of the Personal Information Handler, without prejudice to the generality of this Clause, the Personal Information Handler will ensure that it has all necessary Consents and notices in place to enable the lawful transfer of the Personal Information to the Entrusted Person in connection with the performance of its obligations under the Services Agreement.

3.3 If the Entrusted Person is Handling Personal Information on behalf of the Personal Information Handler, to the extent within the Personal Information Handler's control having regard to the Entrusted Person's obligations under the Services Agreement, the Personal Information Handler shall be responsible for the accuracy and quality of the Personal Information transferred to the Entrusted Person.

3.4 If the Entrusted Person is Handling Personal Information on behalf of the Personal Information Handler, the Entrusted Person shall have an ongoing obligation throughout the duration of the Services Agreement to identify and report to the Personal Information Handler best practice techniques relating to the Handling of Personal Information and the emergence of new and evolving technologies which could improve the availability, confidentiality and/or integrity of the Handling of Personal Information.

## 4. Sub-Handlers


© All rights reserved by Heiko Maniero.

4.1 If the Handling involves more than one Entrusted Person (**Sub-Handler**), the Handling must be made in accordance with a contract or written agreement whereby their obligations, responsibilities and roles related to the Handling are clearly defined.

4.2 The Personal Information Handler hereby authorizes the Entrusted Person to appoint Sub-Handlers (General Written Authorization). The Entrusted Person shall name all its Sub-Handlers to the Personal Information Handler prior to initiation of Handling.

4.3 With respect to each Sub-Handler appointed by the Entrusted Person under General Written Authorization, the Entrusted Person shall (a) undertake appropriate due diligence prior to the Handling of Personal Information by such Sub-Handler to ensure that it is capable of providing the level of protection for Personal Information required by the terms of the Services Agreement and this Agreement, and (b) enter into a written Agreement with the Sub-Handler incorporating terms which are substantially similar (and no less onerous) than those set out in this Agreement and which meet the requirements stipulated by PIPL.

4.4 In regard to the Agreement between the Personal Information Handler and the Entrusted Person, the Entrusted Person remain fully liable to the Personal Information Handler for all acts or omissions of its Sub-Handlers as though they were its own.

4.5 To the extent that the Entrusted Person has already appointed any Sub-Handlers prior to the Handling of any Personal Information under this Agreement, the Entrusted Person shall ensure that its obligations under this Section are met.

4.6 Where the Entrusted Person proposes any changes concerning the addition or replacement of any Sub-Handler, it shall notify the Personal Information Handler in writing as soon as reasonably practicable prior to implementing such change specifying (a) the name of any Sub-Handler which it proposes to add or replace, and (b) the Handling activity or activities affected by the proposed change, and (c) the reasons for the proposed change, and (d) the proposed date for implementation of the change.

4.7 If within thirty (30) days of receipt of a notice the Personal Information Handler (acting reasonably and in good faith) notifies the Entrusted Person in writing of any objections to the proposed change, the Parties shall use their respective reasonable endeavors to resolve the Personal Information Handler's objections. Where such resolution cannot be agreed within thirty (30) days of the Entrusted Person's receipt of the Personal Information Handler's objections (or such longer period as the Parties may agree in writing) the Personal Information Handler may, notwithstanding the terms of the Services Agreement, serve written notice on the Entrusted Person to terminate the Services Agreement (to the extent that the provision of the Services are or would be affected by the proposed change).

4.8 The Entrusted Person shall, upon the Personal Information Handler's request, provide the Personal Information Handler with copies of any Agreements between the Entrusted Person and its Sub-Handlers (which may be redacted to remove information which is confidential to the Entrusted Person and/or its Sub-Handlers and which is not relevant to the terms of this Agreement).

## 5. Obligations of the Entrusted Person (Art. 5, 6, 7, 8, 9, and 10 PIPL)


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

5.1 The Entrusted Person shall observe the principles of legality, propriety, necessity, and sincerity for Personal Information Handling. The Entrusted Person shall not Handle Personal Information in misleading, swindling, coercive, or other such ways.

5.2 The Entrusted Person shall Handle Personal Information only for clear and reasonable purposes, that shall be directly related to the Handling purpose, using methods with the smallest influence on individual rights and interests.

5.3 The Entrusted Person shall limit the collection of Personal Information to the smallest scope for realizing the Handling purpose, and not collect Personal Information excessive.

5.4 The Entrusted Person shall observe the principles of openness and transparency in the Handling of Personal Information, disclose the rules for Handling Personal Information and clearly indicate the purpose, method, and scope of Handling.

5.5 The Entrusted Person shall ensure the quality of Personal Information and avoid adverse effects on individual rights and interests from inaccurate or incomplete Personal Information.

5.6 The Entrusted Person shall bear full responsibility for its own Personal Information Handling activities and adopt all necessary measures to safeguard the security of the Personal Information it Handles. The Parties agreed on the required technical and organizational measures and procedures in APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

5.7 The Entrusted Person shall not illegally collect, use, process, or transmit other persons' Personal Information, or illegally sell, buy, provide, or disclose other persons' Personal Information, or engage in Personal Information Handling activities harming national security or the public interest.

## 6. Consent and Legal Grounds (Art. 13, 14, 15, and 16 PIPL)

6.1 In principle, the Entrusted Person shall Handle Personal Information with the individual's consent.

6.2 However, the Entrusted Person may Handle Personal Information without the individual's consent in cases (1) where necessary to conclude or fulfill a contract in which the individual is an interested party, or where necessary to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded collective contracts, or (2) where necessary to fulfill statutory duties and responsibilities or statutory obligations, or (3) where necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions, or (4) Handling Personal Information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest, or (5) when Handling Personal Information disclosed by persons themselves or otherwise already lawfully disclosed, within a reasonable scope in accordance with the provisions of PIPL, or (6) in other circumstances provided in laws and administrative regulations.


© All rights reserved by Heiko Maniero.

6.3 Where Personal Information is Handled by the Entrusted Person based on the individual's consent, said consent shall be given by individuals under the precondition of full knowledge, and in a voluntary and explicit statement. Where laws or administrative regulations provide that separate consent or written consent shall be obtained to Handle Personal Information, those provisions are to be followed by the Entrusted Person.

6.4 Where the Entrusted Person changes the purpose of Personal Information Handling, the Handling method, or the categories of Handled Personal Information, the Entrusted Person shall obtain the individual's consent again.

6.5 Where Personal Information is Handled by the Entrusted Person based on the individual's consent, the Entrusted Person shall inform individuals about their right to rescind their consent. The Entrusted Person shall provide a convenient way to withdraw consent.

6.6 The Entrusted Person shall not refuse to provide products or services on the basis that an individual does not consent to the Handling of its Personal Information or rescinds its consent, except where Handling Personal Information is necessary for the provision of products or services.

## 7. Transparency towards and Notifications of Individuals (Art. 17 and 18 PIPL)

7.1 The Entrusted Person shall, before Handling Personal Information, explicitly notify individuals truthfully, accurately, and fully, using clear and easily understood language, namely about (1) the name or personal name and contact method of the Entrusted Person, and (2) the purpose of Personal Information Handling and the Handling methods, the categories of Handled Personal Information, and the retention period, and (3) methods and procedures for individuals to exercise the rights provided by PIPL, and (4) other items that laws or administrative regulations provide shall be notified. Where the Entrusted Person Handles Personal Information exclusively for the Personal Information Handler, the Entrusted Person shall, before Handling Personal Information, explicitly notify and inform individuals by means of the Transparency Document that was published on the website of the Personal Information Handler.

7.2 Where a change occurs in the matters provided in the previous paragraph, individuals shall be notified by the Entrusted Person about the change.

7.3 Where the Entrusted Person notify the matters as provided under Section 7.1 through the method of formulating Personal Information Handling rules, the Handling rules shall be made public disclosed and convenient to read and store.

7.4 The Entrusted Person may not notify individuals about the items provided in Section 7.1 under circumstances where laws or administrative regulations provide that confidentiality shall be preserved or notification is not necessary.

7.5 Under emergency circumstances, where it is impossible to notify individuals in a timely manner in order to protect natural persons' lives, health, and the security of their property, the Entrusted Person shall notify them after the conclusion of the emergency circumstances.

## 8. Retention (Art. 19 PIPL)


© All rights reserved by Heiko Maniero.

8.1 The Entrusted Person shall, except where laws or administrative regulations provide otherwise, use the shortest period necessary to realize the purpose of the Personal Information Handling as retention period.

## 9. Rights and Obligations of each Party if the Parties act as Joint-Controllers (Art. 20 PIPL)

9.1 This Section 9 shall apply only if the Personal Information Handler and the Entrusted Person act jointly as Joint-Controllers. The Clauses of Section 9 of this Agreement shall supersede any conflicting Clauses in other Sections of this Agreement regarding to both Joint-Controllers.

9.2 This Agreement does not influence an individual's rights to demand any of the Joint-Controllers to perform under PIPL provisions.

9.3 Where the Joint-Controllers harm Personal Information rights and interests, resulting in damages, they bear joint liability according to the law.

9.4 The Joint-Controllers determined the scope, subject, purpose and nature of the Handling, the type of Personal Information and categories of individuals in the Services Agreement and/or in APPENDIX 8 – DESCRIPTION OF THE PROCESSING OR THE TRANSFER.

9.5 The Joint-Controllers shall jointly ensure compliance with Data Protection Legislation when Handling Personal Information. Both controllers are equally responsible for the legality and lawfulness of joint Handling.

9.6 The Personal Information Handler undertakes to provide the individuals with all information regarding their rights under PIPL. The Personal Information Handler acts as the contact point for individuals.

9.7 The Joint-Controllers shall bear joint responsibility for Personal Information Handling activities and adopt all necessary measures to safeguard the security of the Personal Information they Handle jointly. The Parties agreed on the technical and organizational measures and procedures in APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

9.8 The Joint-Controllers shall jointly appoint only Sub-Handlers which adopted necessary measures to safeguard the security of the Personal Information they Handle and comply with PIPL.

9.9 Each Joint-Controller shall appoint a Data Protection Officer. Both Data Protection Officers shall act jointly in good faith.

9.10 Where one of the Joint-Controllers provides a third party with Personal Information, that Joint-Controller shall notify individuals about the name or personal name of the recipient, their contact method, the Handling purpose, Handling method, and Personal Information categories, and obtain separate consent from the individuals.

9.11 Where one of the Joint-Controllers provides a third party with Personal Information, that third party shall Handle Personal Information within the scope of Handling purposes, Handling

 © All rights reserved by Heiko Maniero.

methods, Personal Information categories, etc. and when the third party is changing the original Handling purpose or Handling methods, that third party shall inform and obtain the individual's consent again.

## 10. General Obligations of the Entrusted Person (Art. 21 PIPL)

10.1 Where the Personal Information Handler entrust the Handling of Personal Information, it shall conclude an agreement with the Entrusted Person on the purpose for entrusted Handling, the time limit, the Handling method, categories of Personal Information, protection measures, as well as the rights and duties of both sides, etc., and conduct supervision of the Personal Information Handling activities of the Entrusted Person.

10.2 The time limit of Handling of Personal Information by the Entrusted Person is the duration of the Services Agreement. The protection measures are agreed on with APPENDIX 9 – TECHNICAL AND ORGANISATIONAL MEASURES.

10.3 The Personal Information Handler published a "List of (sub) processors, recipients in third countries and international organizations" on its website. In this document, the "Purpose for entrusted Handling" is published as "Subject matter of (sub-) processing", the "Handling method" is published as "Nature of (sub-) processing", and the "Categories of Personal Information" are published as "Categories of Personal Data".

10.4 The Personal Information Handler is granted the right to conduct supervision of the Personal Information Handling activities of the Entrusted Person.

10.5 The Entrusted Person shall Handle Personal Information exclusively according to this Agreement. The Entrusted Person shall not Handle Personal Information for Handling purposes or in Handling methods, etc., in excess of this Agreement.

10.6 If this Agreement does not take effect, is void, has been cancelled, or has been terminated, the Entrusted Person shall return the Personal Information to the Personal Information Handler or delete it, and may not retain it.

## 11. Mergers, separations, dissolution, declaration of bankruptcy, and other such reasons (Art. 22 PIPL)

11.1 The Entrusted Person shall not transfer any Personal Information Handled on behalf or for the Personal Information Handler due to mergers, separations, dissolution, declaration of bankruptcy, and other such reasons. Wherever such reason may occur, the Personal Information Handler is to be informed and shall decide on the transfer of Personal Information, the return of the Personal Information to the Personal Information Handler or the deletion of the Personal Information.

## 12. Notifications where Personal Information Handlers provide other Personal Information Handlers with the Personal Information they Handle (Art. 23 PIPL)

12.1 Where the Entrusted Person provide other Personal Information Handlers with the Personal Information it Handles, the Entrusted person shall notify individuals about the name or personal


© All rights reserved by Heiko Maniero.

name of the recipient, their contact method, the Handling purpose, Handling method, and Personal Information categories, and obtain separate consent from the individual.

12.2 Where the Entrusted Person provide other Personal Information Handlers with the Personal Information it Handles, the Entrusted person shall make sure by means of a contract that all recipients that Handle Personal Information within the above-mentioned scope of Handling purposes, Handling methods, Personal Information categories, etc. and where recipients change the original Handling purpose or Handling methods, the Entrusted Person shall make sure by means of a contract, that the recipients obtain the individual's consent again.

## 13. Automated Decision-Making (Art. 24 PIPL)

13.1 The Entrusted Person shall not use any methods for or engage with any automated decision-making regarding the Personal Information that is Handled for or on behalf of the Personal Information Handler.

## 14. Non Disclosure of Personal Information (Art. 25 PIPL)

14.1 The Entrusted Person shall not disclose any Personal Information Handled on behalf of the Personal Information Handler to third parties. Sub-Handlers are not considered to be third parties.

## 15. Major influence on individual rights and interests (Art. 27 PIPL)

15.1 Where the Entrusted Person Handles Personal Information that has been disclosed by the persons themselves or was otherwise lawfully disclosed, except where the person clearly refuses, and that may have a major influence on individual rights and interests, the Entrusted Person shall obtain personal consent in accordance with the provisions of PIPL.

## 16. Sensitive Personal Information (Art. 28, 29, 30, 31, and 32 PIPL)

16.1 In general, the Entrusted Person shall not Handle Sensitive Personal Information on behalf of the Personal Information Handler. However, if the Entrusted Person would Handle Sensitive Personal Information in exceptional circumstances on behalf of the Personal Information Handler, it may do so only where there is a specific purpose and a need to fulfill, and under circumstances of strict protection measures.

16.2 If the Entrusted Person would Handle Sensitive Personal Information in exceptional circumstances on behalf of the Personal Information Handler, the Entrusted Person shall obtain the individual's separate consent. Where laws or administrative regulations provide that written consent shall be obtained for Handling Sensitive Personal Information, those provisions are to be followed by the Entrusted Person.

16.3 If the Entrusted Person would Handle Sensitive Personal Information in exceptional circumstances on behalf of the Personal Information Handler, the Entrusted Person shall, in addition to the items set out in Article 17, Paragraph 1, of PIPL, also notify individuals of the


© All rights reserved by Heiko Maniero.

necessity and influence on the individual's rights and interests of Handling the Sensitive Personal Information, except where PIPL provides that it is permitted not to notify the individuals.

16.4 In general, the Entrusted Person shall not Handle Personal Information of minors under the age of 14 on behalf of the Personal Information Handler. However, if the Entrusted Person would Handle Personal Information of minors under the age of 14 in exceptional circumstances on behalf of the Personal Information Handler, the Entrusted Person shall obtain the consent of the parent or other guardian of the minor. Where the Entrusted Person Handle the Personal Information of minors under the age of 14, the Entrusted Person shall formulate specialized Personal Information Handling rules.

16.5 Where laws or administrative regulations provide that relevant administrative licenses shall be obtained or other restrictions apply to the Handling of Sensitive Personal Information, those provisions are to be followed by the Entrusted Person.

## 17. Cross-Border Provision of Personal Information (Art. 38, 39, 40, 41, 42 and 43 PIPL)

17.1 Where the Entrusted Person, on behalf of the Personal Information Handler, truly need to provide Personal Information outside the borders of the People's Republic of China for business or other such requirements, the Entrusted Person shall meet all requirements of PIPL.

17.2 In particular, in such case, the Entrusted Person shall meet one of the following conditions: (1) passing a security assessment organized by the State cybersecurity and informatization department according to Article 40 of PIPL, or (2) undergoing Personal Information protection certification conducted by a specialized body according to provisions by the State cybersecurity and informatization department, or (3) concluding a contract with the foreign receiving side in accordance with a standard contract formulated by the State cyberspace and informatization department, agreeing upon the rights and responsibilities of both sides, or (4) meet other conditions provided in laws or administrative regulations or by the State cybersecurity and informatization department.

17.3 Where treaties or international agreements that the People's Republic of China has concluded or acceded to contain relevant provisions such as conditions on providing personal data outside the borders of the People's Republic of China, those provisions may be carried out by the Entrusted Person.

17.4 The Entrusted Person shall adopt necessary measures to ensure that foreign receiving parties' Personal Information Handling activities reach the standard of Personal Information protection provided in PIPL.

17.5 Where the Entrusted Person provide Personal Information outside of the borders of the People's Republic of China, the Entrusted Person shall notify the individual about the foreign receiving side's name or personal name, contact method, Handling purpose, Handling methods, and Personal Information categories, as well as ways or procedures for individuals to exercise the rights provided in PIPL with the foreign receiving side, and other such matters, and obtain individuals' separate consent.


© All rights reserved by Heiko Maniero.

17.6 If the Entrusted Person is a Critical information infrastructure operator that is Handling Personal Information and reaches the quantities provided by the State cybersecurity and informatization department the Entrusted Person shall store Personal Information collected and produced within the borders of the People's Republic of China domestically. Where the Entrusted Person need to provide it abroad, the Entrusted Person shall pass a security assessment organized by the State cybersecurity and informatization department; where laws or administrative regulations and State cybersecurity and informatization department provisions permit that security assessment not be conducted, those provisions are to be followed by the Entrusted Person.

17.7 Competent authorities of the People's Republic of China, according to relevant laws and treaties or international agreements that the People's Republic of China has concluded or acceded to, or according to the principle of equality and mutual benefit, are to Handle foreign judicial or law enforcement authorities' requests regarding the provision of Personal Information stored domestically. Without the approval of the competent authorities of the People's Republic of China, the Entrusted Person may not provide Personal Information stored within the mainland territory of the People's Republic of China to foreign judicial or law enforcement agencies.

17.8 The Entrusted Person shall observe the lists of the State cybersecurity and informatization department that contain foreign organizations or individuals with limitations or prohibitions regarding the provision of personal information to them and shall under no circumstances transfer or provide Personal Information to any foreign organization or individual that is named or included on such lists.

17.9 Where the People's Republic of China has adopted reciprocal measures against any country or region on the basis of actual circumstances, based on Art. 43 PIPL, the Entrusted Person shall comply with any such decision, and where required, without undue delay cease and desist any transfer to the respective country or region.

## 18. Individuals' Rights in Personal Information Handling Activities (Art. 44, 45, 46, 47, 48, 49, and 50 PIPL)

18.1 The Entrusted Person shall comply with its own obligations under Art. 44, 45, 46, 47, 48, 49, and 50 PIPL and inform the Personal Information Handler, with undue delay, fully about any individual that has contacted the Entrusted Person regarding any Rights in Personal Information Handling Activities relating to any Personal Information Handled on behalf of the Personal Information Handler.

18.2 Where the Entrusted Person Handles Personal Information on behalf of the Personal Information Handler, the Entrusted Person shall, before Handling Personal Information, inform individuals about their Rights in Personal Information Handling Activities regarding the Personal Information Handler by means of the Transparency Document published on the website of the Personal Information Handler.

## 19. Other Duties of the Entrusted Person (Art. 51, 52, 53, 54, 55, 56, 57, 58 and 59 PIPL)

19.1 The Entrusted Person shall, on the basis of the Personal Information Handling purpose, Handling methods, Personal Information categories, as well as the influence on individuals'


Powered by LegalTech from Willing & Able and the Germany Certification Body. © All rights reserved by Heiko Maniero.

rights and interests, possibly existing security risks, etc., adopt at least the following measures to ensure Personal Information Handling conforms to the provisions of laws and administrative regulations, and prevent unauthorized access as well as Personal Information leaks, distortion, or loss: (1) formulate internal management structures and operating rules, and (2) implement categorized management of Personal Information, and (3) adopt corresponding technical security measures such as encryption, de-identification, etc., and (4) reasonably determine operational limits for Personal Information Handling, and regularly conducting security education and training for employees, and (5) formulate and organize the implementation of Personal Information security incident response plans, and (6) take other measures provided in laws or administrative regulations.

19.2 If the Entrusted Person has reached the quantities provided by the State cybersecurity and informatization department, it shall appoint a Personal Information Protection Officer, to be responsible for supervising Personal Information Handling activities as well as adopted protection measures, etc., and shall disclose the methods of contacting the Personal Information Protection Officer, and report the personal names of the Officer and contact methods to the departments fulfilling Personal Information protection duties and responsibilities.

19.3 If the Entrusted Person engages a Personal Information Handler outside the borders of the People's Republic of China, the Entrusted Person shall make sure that the foreign Personal Information Handler has dedicated an entity or appointed a representative within the borders of the People's Republic of China that is responsible for matters related to the Personal Information which it Handles, and that the name of the relevant entity or the personal name of the representative and contact method, etc., was reported to the departments fulfilling personal information protection duties and responsibilities.

19.4 The Entrusted Person shall regularly engage in audits of their Personal Information Handling and compliance with laws and administrative regulations.

19.5 When one of the following circumstances is present, the Entrusted Person shall conduct a Personal Information Protection Impact Assessment in advance, and record the Handling situation: (1) Handling Sensitive Personal Information, or (2) Using Personal Information to conduct automated decision-making, or (3) Entrusting Personal Information Handling, providing Personal Information to other Personal Information Handlers, or disclosing Personal Information, or (4) Providing Personal Information abroad, or (5) other Personal Information Handling activities with a major influence on individuals.

19.6 The Entrusted Person shall include the following content in the Personal Information Protection Impact Assessment: (1) whether or not the Personal Information Handling purpose, Handling method, etc., are lawful, legitimate, and necessary, and (2) the influence on individuals' rights and interests, and the security risks, and (3) whether protective measures undertaken are legal, effective, and suitable to the degree of risk. The Entrusted Person shall preserve the Personal Information Protection Impact Assessment Reports and Handling status records for at least three years.

19.7 Where a Personal Information leak, distortion, or loss occurs or might have occurred, the Entrusted Person shall immediately adopt remedial measures, and notify the Personal Information Handler to allow him to notify the departments fulfilling Personal Information

 © All rights reserved by Heiko Maniero.

protection duties and responsibilities and the individuals. The notification shall include the following items (1) the information categories, causes, and possible harm caused by the leak, distortion, or loss that occurred or might have occurred, and (2) the remedial measures taken by the Personal Information Handler and measures individuals can adopt to mitigate harm, and (3) the contact method of the Entrusted Person.

19.8 If the Entrusted Person is providing important Internet platform services, that have a large number of users, and its business models are complex, the Entrusted Person shall fulfill the obligations in Art. 58 PIPL.

19.9 The Entrusted Persons shall, according to the provisions of PIPL and relevant laws and administrative regulations, take necessary measures to safeguard the security of the Personal Information it Handles, and assist the Personal Information Handler in fulfilling its obligations provided in PIPL.

## 20. Legal Liability (Art. 66 PIPL)

20.1 Where the Entrusted Person has Handled Personal Information in violation of PIPL or Personal Information is Handled by the Entrusted Person without fulfilling Personal Information protection duties in accordance with the provisions of PIPL, and the Entrusted Person acted on behalf of the Personal Information Handler, the Personal Information Handler is entitled to order correction, and order the provisional suspension or termination of service provision of the application programs unlawfully Handling Personal Information.

## 21. Compensation for infringements (Art. 69 PIPL)

21.1 Where the Entrusted Person Handled Personal Information, and such operation is infringing Personal Information rights and interests and results in harm, and the Entrusted Person cannot prove they are not at fault, the Entrusted Person shall bear compensation and take responsibility for the infringement. Responsibility to compensate for infringement shall be determined according to the resulting loss to the individual or the Personal Information Handler's resulting benefits. Where the loss to the individual and the Personal Information Handler's benefits are difficult to determine, a court may determine compensation according to practical conditions.


Powered by LegalTech from Willing & Able and the Germany Certification Body.
© All rights reserved by Heiko Maniero.