# Commissioned Data Processing Agreement

in accordance with Art. 28 of the EU General Data Protection Regulation (GDPR)

between

**Name**

**and**

**address**

(hereinafter referred to as "**Controller"**)

and

**Name**

**and**

**address**

(hereinafter referred to as "**Processor"**)

(Together as the **“Parties”**)

**§ 1 - Subject matter**

1. **Principal Agreement.** This Commissioned Data Processing Agreement **(“Agreement”)** governs the obligations of the contracting parties in connection with the processing of the Controller’s personal data by the Processor under the agreement mentioned in Attachment 1 (“**Principal Agreement**”).

2. **Scope.** The subject, scope and purpose of the processing of personal data by the Processor can be found in Attachment 1 and in the Principal Agreement’s specification of services.

3. **Priority regulation**. The provisions of this Agreement including its Attachments shall take precedence over the provisions of the Principal Agreement.

 Should the EU Standard Contractual Clauses become part of the Agreement, they will take precedence over the provisions of this Agreement and its Attachments.

**§ 2 - Controller rights and duties**

1. **Role of the Controller.** The Controller is the responsible party within the meaning of Art. 4 (7) of the GDPR or (sub-)processor within the meaning of Art. 4 (8) of the GDPR of one/more controller(s) or of one/more other processor(s) whose data he processes on a (sub-)contract basis. He is in particular responsible for the lawfulness of the processing of personal data, as well as for the protection of the data subjects’ rights.

2. **Instructions.** The Controller has the right to issue instructions regarding the nature, scope and methods of the processing of personal data. The Controller shall generally issue instructions in writing or by e-mail. In case of urgency or due to other special circumstances, instructions may also be given orally or by telephone and shall always be confirmed afterwards by the Controller in writing or by e-mail without undue delay.

The persons authorized to issue instructions on behalf of the Controller and the entitled Processor’s recipients of instructions are listed in Attachment 1. The Parties shall notify each other in writing or by email without undue delay of any changes to the persons entitled to give or receive instructions.

**§ 3 - Processor rights and duties**

1. **Role of the Processor.** The term (Sub-) **“Processor”** shall have the same meaning as in Art. 4 (8) of the GDPR.

The Processor and any person acting under his authority with access to the data shall process the data exclusively for the purposes specified in Attachment 1 and within the framework of the Principle Agreement in accordance with the Controller's instructions – including with regard to transfers of personal data to a third country or an international organization-, unless the Processor is obliged by Union or Member State law to process the data in a certain way. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such notification on important grounds of public interest (Art. 28 (3) (2nd sentence) (a) of the GDPR).

The Processor shall document the instructions given to him in a suitable, clear form and shall make this documentation available to the Controller on request.

Any specific instructions at the commencement of the Agreement are stipulated in Attachment 1. Copies or duplicates of personal data will not be made without the knowledge of the Controller. Exceptions to this are back-up copies, insofar as they are necessary to guarantee proper data processing, as well as data required to comply with mandatory retention periods defined by law.

2. **Deletion, return.** Upon request by the Controller or without undue delay after completion of the contractual work the Processor shall, according to the Controller’s specification, return or destroy resp. delete in accordance with data protection legislations all personal data from the contractual relationship (this also applies to any existing copies), unless Union or Member State law requires storage of the personal data. The Processor shall inform the Controller of such a legal obligation, unless this is prohibited by law. The obligation to delete or return also applies to test and reject material. The deletion, destruction or complete return must be confirmed to the Controller in writing, stating the date. The plea of rights of retention, for example within the meaning of § 273 BGB, is excluded with regard to the processed data and the associated data carriers.

3. **Data Protection Officer or Data Protection Contact Person.** The Processor shall ensure the appointment of a Data Protection Officer if legally required or, if the appointment of a Data Protection Officer is not required by law, the Processor shall ensure the appointment of a Data Protection Contact Person.

 The contact details of the Data Protection Officer or the Data Protection Contact Person are listed in Attachment 1. Any changes shall be reported without undue delay to the Controller in writing or by email.

4. **Data secrecy.** The Processor is obliged to treat the data confidentially. The Processor shall comply with the provisions of the GDPR on the preservation of confidentiality in accordance with Art. 28 (3) (2nd sentence) (b), Art. 29 and Art. 32 (4) of the GDPR. Accordingly, the Processor shall only engage employees who are bound to confidentiality and have previously been made familiar with the data protection laws applicable. The confidentiality obligation of the Processor's employees shall also apply after termination of their employment contracts. These obligations of the Processor shall continue to apply after the termination of this Agreement.

5. **Legal compliance, monitoring.** The Processor is obliged to comply with all applicable legal regulations concerning the processing of personal data. The Processor shall regularly monitor compliance with the applicable data protection provisions, contractual obligations and the instructions of the Controller during the term of the Agreement and shall provide the Controller with appropriate proof of this upon request. The duty of control applies in particular to the internal processes as well as the technical and organizational measures. A concept for monitoring measures must be documented and presented to the Controller upon request.

6. **Support to the Controller in the fulfilment of its obligations according to the GDPR.** Considering the nature of the processing, the Processor shall, if possible, support the Controller with suitable technical and organizational measures in order to comply with its obligation to respond to data subject’s requests as set out in Chapter III of the GDPR. If the data subjects assert their rights with the Processor, the Processor must immediately forward the requests to the Controller. The Processor may only provide information to the data subjects, correct or delete their data or restrict the processing of the data in accordance with documented instructions from the Controller.

The Processor will also support the Controller in complying with the obligations set out in Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available.

 The Processor shall otherwise support the Controller to an appropriate extent in answering official or judicial enquiries and in dealing with other official or judicial measures (e.g. inspections) and shall provide the necessary information.

7. **Data breaches**. Personal data breaches at the Processor or at his Subprocessors must be reported to the Controller without undue delay after becoming aware of the breach and the information and documents required to comply with any reporting and notification obligations of the Controller pursuant to Art. 33 and Art. 34 GDPR shall be included. The Processor shall inform of all relevant circumstances, the measures taken and provide an assessment of the risks arising from the data breach to the data subjects concerned. The Processor shall answer any queries without undue delay and cooperate closely with the Controller in clarifying the circumstances. The notification of a data breach to the competent authority and the notification to the data subjects shall be made exclusively by the Controller.

The notification of the Processor must be sent simultaneously to the following e-mail addresses:

- E-mail address of the authorized representative referred to in Attachment 1 section 9

- Controller’s data protection functional mailbox, Attachment 1 section 13.

**§ 4 - Place of processing**

1. **Consent requirement for processing in a third country with poor data protection security.** The processing of the data by the Processor and the Subprocessors approved by the Controller (see § 7) shall in principle take place exclusively in the Federal Republic of Germany, in a Member State of the European Union, in a state which is a party to the Agreement on the European Economic Area or in a country where an adequacy decision has been issued by the European Commission in accordance with Art. 45 of the GDPR. Any relocation of processing to another country (**"third country with poor data protection security"**) requires the consent of the Controller and may only take place if the legal requirements for data transfers to third countries under the applicable data protection laws are met. The Processor shall complete section 7 of Attachment 1 and provide additional documents if necessary.

2. **Processing by Processor in a third country with poor data protection security.** If the processing of the data by the Processor takes place exclusively or also in a third country with poor data protection security, the EU standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (“EU standard contractual clauses 2021”) shall apply in respect of such processing. The selection of the module of these EU standard contractual clauses 2021 applicable to the processing shall be made in Attachment 1.

Controller and Processor shall cooperate closely in documenting compliance with the obligations resulting from the EU standard contractual clauses 2021. In order to meet the criteria set out in Clause 14 of the EU standard contractual clauses 2021, the Processor shall provide the Controller with all information required in this respect. In particular, the Processor shall answer the Controller’s questions truthfully, comprehensively and within a reasonable period of time regarding the applicability of legal provisions and practices or their practical implementation in the relevant third countries with poor data protection security.

 If, due to the legal provisions and practices in these third countries with poor data protection security and in view of the particular circumstances of the processing, there is no reasonable assurance that the processing will be carried out in compliance with the EU standard contractual clauses 2021, the Processor shall, in consultation with the Controller, (i) implement additional technical and organizational measures and/or (ii) provide additional contractual assurances, which, taking into account these legal provisions and practices and the particular circumstances of the processing, provide a sufficient guarantee for the processing of the data in compliance with the Processor’s obligations under the EU standard contractual clauses 2021 (“Additional Measures and Assurances”).

 The processing of the data by the Processor may only start after the Controller’s questions mentioned in paragraph 2 have been answered by the Processor and after the Additional Measures and Assurances possibly required according to paragraph 3 have been taken or given.

3. **Processing by Subprocessors in a third country with poor data protection security (if Processor is established in the EU or in a country with an adequate level of data protection).** If Subprocessors within the meaning of § 7 (1) of a Processor established in the EU or in a country with an adequate level of data protection process data in a third country with poor data protection security, the Processor shall, in addition to the requirements set out in § 4 (1), ensure before the start of processing by these Subprocessors that the EU standard contractual clauses 2021 have been concluded with the Subprocessor or that Binding corporate rules within the meaning of Art. 47 of the GDPR apply to the Subprocessor. § 4 (2) paragraph 2 and 3 shall apply accordingly in the relationship between the Processor and Subprocessor. Upon request of the Controller, the Processor shall provide the Controller with a copy of the documents relevant insofar.

4. **Processing by Subprocessors in a third country with poor data protection security (if Processor is neither established in the EU nor in a country with an adequate level of data protection).** If Subprocessors within the meaning of § 7 (1) of a Processor neither based in the EU nor in a country with an adequate level of data protection process data in a third country with poor data protection security, the Processor shall, in addition to the requirements set out in § 4 (1), conclude contractual agreements with these Subprocessors before the start of the processing by these Subprocesors which ensure, with regard to the processing by the Subprocessors, that this processing takes place at a level of data protection which corresponds to the level guaranteed by the EU standard contractual clauses 2021 or by Binding corporate rules within the meaning of Art. 47 of the GDPR. § 4 (2) paragraph 2 and 3 shall apply accordingly in the relationship between the Processor and Subprocessor. Upon request of the Controller, the Processor shall provide the Controller with a copy of the documents relevant insofar.

**§ 5 - Liability**

The Processor shall be liable in accordance with the statutory provisions for damages of the Controller resulting from the Processor’s culpable breach of this Agreement or statutory data protection obligations affecting the Processor (Art. 82 GDPR). In this regard, any limitations of liability otherwise agreed between the parties (e.g. in the Principal Agreement) shall not apply.

**§ 6 Technical and organizational measures**

1. **General information.** The Processor shall take the appropriate technical and organizational measures within the meaning of Art. 28 paragraph 3 lit. c and Art. 32 of the GDPR, in particular in connection with Art. 5 paragraph 1, paragraph 2 of the GDPR to ensure a level of protection appropriate to the risk arising from the processing of the data.

In assessing the adequate level of protection, the contracting parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing, and the risks to data subjects.

 Against this background, the Processor shall implement at least the technical and organizational measures defined in Attachment 2.

Technical and organizational measures are subject to technical progress and continuous development. In this respect, the Processor is permitted, in consultation with the Controller, to implement alternative adequate measures, provided that the security level of the agreed technical and organizational measures is not fallen below. Changes must be documented and communicated to the controller immediately. Significant changes require the prior written consent of the controller.

2. **Certification.** In addition, the Processor must document and demonstrate the suitability for implementing adequate security measures by a corresponding TISAX or ISO/IEC 27001 certification.

The Processor is obliged to implement the safety measures required to achieve and maintain the certification, which he has specified in the certification procedure, as well as such measures contractually agreed in Attachment 2, throughout the term of the contract.

Deviations from certification according to TISAX or ISO/IEC 27001 are only permitted with the prior written consent of the responsible information security department of the Controller.

3.  **Audit rights.** With regard to the control obligations of the Controller before the start of data processing and during the term of the contract, the Processor shall ensure that the Controller can satisfy himself of compliance with the technical and organizational measures taken.

4. **Data processing in private homes.** The processing of the contractual personal data in private homes is only permitted if an appropriate level of security is also guaranteed there by the Processor within the meaning of the GDPR and this agreement.

**§ 7 - Subprocessors**

1. **Use of Subprocessors.** The Controller agrees that the Processor may involve third parties ("Subprocessors") for the performance of the contractually agreed services and the processing of data in connection therewith, provided that the requirements of the following paragraphs are guaranteed.
2. **Subprocessors permitted at the time of conclusion of this Agreement**. The Processor is permitted to use the Subprocessors listed in Attachment 1.
3. **Further Subprocessors**. The Controller shall be informed by the Processor in writing or by e-mail without undue delay, but no later than 45 calendar days prior to the assignment, of any intended assignment of additional Subprocessors or replacement of existing Subprocessors, so that the Controller has sufficient time to raise objections to such assignment before the assignment. The Processor shall provide the Controller with the necessary information to enable the Controller to exercise his right of objection according clause 9 of the EU standard contractual clauses 2021. The processing of data by the Subprocessor is only permitted once all legal requirements and those resulting from this Agreement are met.
4. **Agreements with Subprocessors.** The Processor must ensure that the contractual agreements with the Subprocessors have the same contractual data protection obligations to which the Processor is subject under this Agreement. The Processor shall regularly check compliance with these data protection obligations by the Subprocessors, in particular the implementation of the necessary technical and organizational measures.
5. **Liability.** If the Subprocessor does not fulfill its data protection obligations, the Processor is liable to the Controller for compliance with the obligations of that Subprocessor.

**§ 8 – Audit rights of the Controller**

1. **Audit rights.** The Controller has the right to verify compliance with the provisions of this Agreement, the instructions issued and the applicable data protection laws, either by itself or through a suitable third party appointed by the Controller and obliged to maintain secrecy. In particular, the Processor shall provide the Controller with all necessary information to prove compliance with the obligations laid down in Art. 28 of the GDPR and enable on-site inspections and other checks to be carried out by the Controller or another auditor appointed by the Controller.

2. **Duty to provide assistance.** The Processor assures assistance in these checks to a reasonable extent, if necessary. In particular, the Processor shall grant access to data processing systems, provide the necessary information and make available the necessary documentation.

3. **Execution.** Inspections at the Processor's premises must be announced in due time and must not disproportionately affect its business operations.

**§ 9 – Notification duties**

1. **Unlawful instructions.** The Processor shall inform the Controller without undue delay if he assesses an instruction issued by the Controller to infringe the GDPR or other Union or Member State data protection provisions. The Processor is entitled to suspend the execution of the corresponding instruction until it is confirmed or amended by the Controller.

2. **Controls by the data protection authorities.** Any investigations or actions taken by the data protection authorities againstthe Processor must be notified to the Controller without undue delay, insofar as the data of the Controller is affected. The Processor shall put remedy to any objections raised by the data protection authorities without undue delay and notify the Controller accordingly.

3. **Errors and irregularities.** Insofar as the data of the Controller is affected, the Processor shall notify the Controller without undue delay of any malfunctions, detected or suspected infringements to the applicable data protection laws or this Agreement made by the Processor or the Processor’s employees, as well as any suspicion of data breaches or irregularities in the processing of the data. This applies in particular with regard to any reporting and notification obligations of the Controller in accordance with Art. 33 and 34 of the GDPR.

**§ 10 - Term**

1. **Term.** The term of this Agreement shall correspond to the term of the Principal Agreement.

2. **Continuity.** If the Processor effectively continues to process the Controller’s personal data beyond the term of the Principal Agreement (e.g. storage due to retention obligations defined by law), the provisions of this Agreement continue to apply.

**§ 11 - Miscellaneous**

1. **Changes.** Changes to this Agreement must always be made in writing, unless otherwise specified in this Agreement.
2. **Adjustments.** Insofar as adaptations of this Agreement are necessary for the parties to comply with the legal requirements, they shall make the corresponding adaptations without undue delay.
3. **Expenses.** The services by the Processor under this Agreement are compensated by the remuneration set out in the Principal Agreement.
4. **Third-party measures**. If the Controller’s personal data at the Processor is jeopardized as a result of third-party measures such as seizure, insolvency or settlement proceedings, or as a result of other comparable events, the Processor must inform the Controller without undue delay.
5. **Severability clause.** Should individual sections of this Agreement be or become ineffective, this does not affect the validity of the rest of the Agreement. The Controller and the Processor undertake to replace the invalid provision with a legally permissible provision that comes as close as possible to the purpose of the invalid provision and meets the requirements of Art. 28 of the GDPR.

4. **Applicable law, place of jurisdiction.** This agreement is governed by law of the Federal Republic of Germany excluding the United Nations Convention of April 11, 1980 on Contracts for the International Sale of Goods (CISG). The sole place of jurisdiction is that of the Controller.

5. **Attachments.** Attachments 1 to 3 form an integral part of the Agreement.

Attachment 1 Description of Data Processing

Attachment 2 Technical and Organizational Security Measures

Attachment 3 EU standard contractual clauses 2021

\* \* \*

|  |
| --- |
| **Controller** |
| Name (printed): Click or tap here to enter text.Function / Title:Click or tap here to enter text.Place, Date:Click or tap here to enter text.Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  | Name (printed): Click or tap here to enter text. Function / Title:Click or tap here to enter text.Place, Date:Click or tap here to enter text.Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  |

|  |
| --- |
| **Processor** |
| Name (printed): Click or tap here to enter text. Function / Title:Click or tap here to enter text.Place, Date:Click or tap here to enter text.Signature: \_\_\_\_\_\_\_\_ | Name (printed): Click or tap here to enter text. Function / Title:Click or tap here to enter text.Place, Date:Click or tap here to enter text.Signature: \_\_\_ \_\_\_\_ |

**ATTACHMENT 1 - Description of the Commissioned Data Processing**

1. **Principal Agreement**

Principal Agreement within the meaning of § 1 section 1 of this Agreement:

Title: ……

Parties: ……

Date: ……

2. **Subject matter of the processing**

The subject matter of the processing is the performance of the following services by the Processor:

……

3. **Scope and purpose of data processing / data processing measures**

More detailed description of the processing in terms of scope and purpose:

……

4. **Categories of data subjects**

The following groups of persons are affected by the Commissioned Data Processing:

[ ]  **Employees.** Employees of the own group company, with the meaning of employee of the Controller.

*e.g. Employees, trainees, applicants, former employees*

[ ]  **Group employees.** Employees of another group company, with the meaning of employee of a VW Group company, but not of the Controller.

*e.g. Employees of other MAN companies, Scania employees, Audi employees*

[ ]  **Partner company employees.** Employees of a supplier, service provider, joint venture, temporary employment agency

*e.g. Employees from partner companies (e.g. IT service providers, suppliers), employees from joint ventures, temporary employees*

[ ]  **Customers.** Any person who has a customer business relationship with the Controller

*e.g. Vehicle buyers, bank customers, insurance policy holders, rental customers*

[ ]  **Other business partners.** Any natural or legal person with whom the Controller has a business relationship, except customers

*e.g. Suppliers, importers or service partners themselves; intermediaries, shareholders, freelancers*

[ ]  **Outsiders.** Any person who has no business relationship with the Controller

*e.g. Visitors, guests, interested parties*

[ ]  **Children.** The assessment of whether the data subject is a child is governed by the respective national law.

 *e.g. in Germany, persons under the age of 16 are referred to as children*

5. **Categories of personal data**

The Commissioned Data Processing includes the following types of personal data:

[ ]  **Professional contact and (work) organization data**

*e.g. surname, first name, gender, address, e-mail address, telephone number, mobile phone number, company, area, department, cost center, personnel numbers, responsibilities, functions*

[ ]  **Data regarding IT use**

*e.g. UserID, roles, authorizations, login times, computer name, IP address, GID, Legic No.*

[ ]  **Motor vehicle usage data with vehicle identification number/license plate number, guarantee, warranty, product liability, safe vehicle operation.** Data generated during motor vehicle use that is linked to vehicle identification numbers/license plate numbers and is relevant in connection with workshop repairs, guarantees and warranties, or is important for product liability, or if its availability is necessary for safe vehicle operation.

[ ]  **Private contact and identification data**

*e.g. surname, first name, gender, address, e-mail address, telephone number, mobile phone number, date and place of birth, identification numbers, nationality*

[ ]  **Contract data**

*e.g. products purchased, (financial) services, date of purchase agreement, purchase price, extras, warranties*

[ ]  **Motor vehicle data with vehicle identification number/license plate number: comfort settings, multimedia, navigation.** Data generated during motor vehicle usage that is linked to vehicle identification numbers/license plate numbers and that relates to comfort settings such as seat position, preferred radio stations, air conditioning settings, GPS data, e-mail/text contact information

[ ]  **Motor vehicle usage data with vehicle identification numbers/license plate number: assist systems, vehicle handling characteristics**
Data produced during motor vehicle usage linked to vehicle identification numbers/license plate numbers and that relates to vehicle handling characteristics or the use of assist systems and their specific operational data

[ ]  **Position data**

*e.g. GPS, radio network location, movement profile, WLAN hotspot location*

[ ]  **Data concerning personal/professional relationships and characteristics**

*e.g. data on spouse or children, marital status, portrait photo, honorary office, job title, professional career, length of service, tasks, activities, dates of entry and exit, qualifications, assessments / evaluations*

[ ]  **Remuneration and time management data**

*e.g. pay scale group, payroll accounting, special payments, garnishment, daily attendance times, reasons for absence*

[ ]  **Solvency and bank data**

*e.g. payment behavior, balance sheets, data from credit agencies, credit score values, financial circumstances, bank account details, credit card number*

[ ]  **Special categories of personal data**: Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (fingerprints, voice recognition, iris scan, etc.), data concerning health, data concerning sexual life or sexual orientation.

Only in the event that special categories of personal data are being processed in third countries with poor data protection security:

a) Please specifically indicate here the relevant special categories of personal data:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

b) Please indicate here the limitations and safeguards agreed in relation to the special categories of personal data referred to in a), which take full account of the nature of the data and the risks involved, e.g. strict purpose limitation, access restrictions, records of access to data, restrictions on onward transfers or additional security measures

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[ ]  **Personal data on criminal offences / administrative offences:** Data relating to criminal offences or suspected criminal offences.

[ ]  **Special category: Employee photo.** Portrait photo published by the employee on a voluntary basis (e.g. intranet telephone book, internal social media platform)

6. **Further description of the data transfer**

If the EU standard contractual clauses 2021 are part of the Agreement, please provide further information here:

a) Frequency of data transfer to third countries with poor data security (multiple answers possible):

 [ ]  one time [ ]  regularly [ ]  continuously

b) Duration for which the personal data will be stored or, if this is not possible, the criteria for determining this duration (multiple answers possible):

 [ ]  No or only volatile storage

 [ ]  Storage until the individual processing purpose has been achieved

 [ ]  Storage until termination of the Principal Agreement

 If applicable, criteria for determining the duration:

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

c) Competent supervisory authority

 Supervisory authority responsible for the Controller:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7. **Special instructions at the start of the Agreement**

[ ]  Anonymization of certain data: …

[ ]  Prohibition of the transmission of data: …

[ ]  Deletion of the data after every ... month

[ ]  The following policies, manuals and company agreements must be observed: …

[ ]  …

8. **Processing location** *Multiple answers possible!*

[ ]  Germany

[ ]  Member State of the European Union or part of the European Economic Area

Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.
Iceland, Norway, Liechtenstein

[ ]  Countries with an adequate level of data protection, currently:

Andorra, Argentina, Australia (Restricted for passenger data only), Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, South Korea, Switzerland, United Kingdom, United States of America (USA; only if certified according to the EU-U.S. Data Privacy Framework) and Uruguay.

[ ]  Third country with poor data protection security: …..

If data processing takes place in a third country with poor data protection security, at least one of the additional admissibility requirements listed below must be met. Please tick all applicable alternatives.

[ ]  Module 2 of the EU standard contractual clauses 2021 is completed between the Controller and every Processor in a third country with poor data protection security.

[ ]  Module 3 of the EU standard contractual clauses 2021 is completed between the Processor and any Subprocessor in a third country with poor data protection security.

[ ]  The data processing is covered by consent of the data subjects.

[ ]  The Processor and every Subprocessor are subject to Binding corporate rules within the meaning of Art. 47 of the GDPR.

9. **Authorized person to issue instructions and carry out verification on behalf of the Controller**

Name: ……

Contact details (e-mail, telephone, address): ……

10. **Responsible recipient for receiving instructions on behalf of the Processor**

Name: ……

Contact details (e-mail, telephone, address): ……

11. **Processor’s Data Protection Officer or Data Protection Contact Person**

[ ]  The Processor has appointed the following Data Protection Officer:

 Name: ……

 Contact details (e-mail, telephone, address): ……

[ ]  The Processor has appointed the following Data Protection Contact Person:

 Name: ……

 Contact details (e-mail, telephone, address): ……

12. **Subprocessors**

[ ]  The Processor shall not employ Subprocessors.

[ ]  The Processor employs the following Subprocessors:

No. \_\_ Subprocessor (name, legal form, address, contact person):

...

Processed data categories:

...

Processing activity of the Subprocessor (brief description of the tasks):

...

Duration of processing:

...

Processing (also) takes place in the following third countries with poor data protection security:

...

13. **Notification of Data Breaches**

The notification of data breaches of the Processor shall be sent to the following selected functional
e-mailboxes of the Controller:

[ ]  DSGVO-Zentralteam@man.eu

[ ]  mtb-iso@man.eu

[ ]  mtb-cdc@man.eu

[ ]  information-security@traton.com

[ ]  ...

14. **Data Processing in private homes (home office)**

[ ]  Yes, data processing may take place in private homes.

[ ]  No, there is no data processing in private homes.

**ATTACHMENT 2 - Technical and Organizational Security Measures**

1. The Processor has taken the following technical and organizational security measures:

... List of TOMs...

or.

Reference to a data security concept according to Art. 32 GDPR

1. The Processor has demonstrated his suitability by submitting the following certificate documents:

[ ]  VDA ISA (TISAX Label - shared with the Controller in the ENX database)

[ ]  ISO 27001 – certificate (including Statement of Applicability)

Other existing certifications: (in addition to the above basic requirements):

[ ]  Cloud Vendor Assessment (DCSO)

[ ]  BSI C5 (Federal Office for Information Security, Cloud)

[ ]  CSA STAR (Cloud Security Alliance)

[ ]  ISO 27017 (Extension of ISO 27001 with regard to Cloud Controls)

[ ]  ISO 27018 (Extension of ISO 27001 with regard to personal data)

3. Within the scope of the commissioned data processing, processing activities are also carried out for the lawfulness of which the conclusion of the EU standard contractual clauses 2021 is required. Therefore, the technical and organizational measures taken by the Importer(s) (including any relevant certifications) to ensure an adequate level of data protection, taking into account the nature, scope, circumstances and purposes of the processing, as well as the risks to the rights and freedoms of natural persons, are listed below and explained in more detail where applicable.

[ ]  Measures of pseudonymization and encryption of personal data.

Explanations:

[ ]  Measures to ensure the continued confidentiality, integrity, availability and resilience of systems and services related to processing.

Explanations:…

[ ]  Measures to ensure the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident.

Explanations:…

[ ]  Procedures for periodically reviewing, assessing and evaluating the effectiveness of technical and organizational measures to ensure the security of processing.

Explanations:…

[ ]  Measures for identification and authorization of the users.

Explanations:…

[ ]  Measures to protect the data during the transfer.

Explanations: …

[ ]  Measures to protect the data during the storage.

Explanations:…

[ ]  Measures to ensure the physical security of places where personal data are processed

Explanations: …

[ ]  Measures to ensure the logging of events.

Explanations: …

[ ]  Measures to ensure the system configuration, including the default configuration.

Explanations:…

[ ]  Measures for the internal governance and management of IT and IT security.

Explanations:…

[ ]  Measures for certification/quality assurance of processes and products.

Explanations:…

[ ]  Measures to ensure data minimization.

Explanations:…

[ ]  Measures to ensure data quality.

Explanations:…

[ ]  Measures to ensure limited data retention.

Explanations:…

[ ]  Measures to ensure accountability.

Explanations:…

[ ]  Measures to enable data portability and to ensure deletions.

Explanations:…

In the case of data transfers to (Sub-)Processors, the specific technical and organizational measures to be taken by the (Sub-)Processor to support the Controller and (in the case of data transfers from a Processor to a (Sub-)processor) to support the data exporter must also be
described.

 **ATTACHMENT 3 – EU Standard Contractual Clauses 2021**

**EU Standard Contractual Clauses pursuant to the Commission Implementing Decision (EU) 2021/914**

**SECTION I**

*Clause 1*

**Purpose and scope**

a) The purpose of these standard 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)[[1]](#footnote-2) 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 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) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

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

ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9 (b); Module Two: Clause 8.1 (b), 8.9 (a), (c), (d) and (e); Module Three: Clause 8.1 (a), (c) and (d) and Clause 8.9 (a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3 (b);

iii) Clause 9 - Module Two: Clause 9 (a), (c), (d) and (e); Module Three: Clause 9 (a), (c), (d) and (e);

iv) Clause 12 - Module One: Clause 12 (a) and (d); Modules Two and Three: Clause 12 (a), (d) and (f);

v) Clause 13;

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

vii) Clause 16 (e);

viii) Clause 18 - Modules One, Two and Three: Clause 18 (a) and (b); Module Four: 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 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 - Optional*

**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.

**SECTION II - OBLIGATIONS OF THE PARTIES**

*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.

**MODULE ONE Transfer controller to controller**

**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**

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[[2]](#footnote-3) 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**

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[[3]](#footnote-4) (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.

**MODULE TWO Transfer controller to processor**

**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 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**

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[[4]](#footnote-5) (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 defence 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.

**MODULE THREE Transfer processor to processor**

**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.[[5]](#footnote-6)

**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**

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.

**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[[6]](#footnote-7) (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 of Regulation (EU) 2016/679;

iii) the onward transfer is necessary for the establishment, exercise or defence 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.

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.

**MODULE FOUR Transfer processor to controller**

**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[[7]](#footnote-8), 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.

*Clause 9*

**Use of sub-processors**

**MODULE TWO Transfer controller to processor**

a) 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 45 calendar 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 Clauses, including in terms of third-party beneficiary rights for data subjects.[[8]](#footnote-9) 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.

**MODULE THREE Transfer processor to processor**

a) 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 45 calendar 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.[[9]](#footnote-10) 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**

**MODULE ONE Transfer controller to controller**

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.[[10]](#footnote-11) 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.

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.

**MODULE TWO Transfer controller to processor**

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.

**MODULE THREE Transfer processor to processor**

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.

**MODULE FOUR Transfer processor to controller**

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**

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.

**MODULE ONE Transfer controller to controller**

**MODULE TWO Transfer controller to processor**

**MODULE THREE Transfer processor to processor**

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**

**MODULE ONE Transfer controller to controller**

**MODULE FOUR Transfer processor to controller**

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.

**MODULE TWO Transfer controller to processor**

**MODULE THREE Transfer processor to processor**

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**

**MODULE ONE Transfer controller to controller**

**MODULE TWO Transfer controller to processor**

**MODULE THREE Transfer processor to processor**

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.

**SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

*Clause 14*

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

**MODULE ONE Transfer controller to controller**

**MODULE TWO Transfer controller to processor**

**MODULE THREE Transfer processor to processor**

**MODULE FOUR Transfer processor to controller** (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 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[[11]](#footnote-12);

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). [For Module Three: 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 fulfil 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 [for Module Three: , 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 [for Module Three: 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**

**MODULE ONE Transfer controller to controller**

**MODULE TWO Transfer controller to processor**

**MODULE THREE Transfer processor to processor**

**MODULE FOUR Transfer processor to controller** (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

**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.

[For Module Three: The data exporter shall forward the notification to the controller.]

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.). [For Module Three: 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. [For Module Three: 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.

**SECTION IV - FINAL PROVISIONS**

*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 [for Module Three: 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) [For Modules One, Two and Three: 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.] [For Module Four: 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**

**MODULE ONE Transfer controller to controller**

**MODULE TWO Transfer controller to processor**

**MODULE THREE Transfer processor to processor**

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.

**MODULE FOUR Transfer processor to controller**

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**

**MODULE ONE Transfer controller to controller**

**MODULE TWO Transfer controller to processor**

**MODULE THREE Transfer processor to processor**

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.

**MODULE FOUR Transfer processor to controller**

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

***Appendix***

**to the EU Standard Contractual Clauses**

*Annex I*

**A. List of Parties**

Data exporter:

|  |  |
| --- | --- |
| Name:  | Controller according this commissioned data processing agreement, page 1 |
| Address:  | Address of the Controller named in this contract on page 1 |
| Contact person’s name, position and contact details (data protection officer where applicable): | Cf. Attachment 1 item 15 |
| Activities relevant to the data transferred under these Clauses: | Cf. Attachment 1 items 2 and 3 |
| Signature, date  | n/a |
| Role:  | Controller |

Data importer:

|  |  |
| --- | --- |
| Name:  | Processor according this commissioned data processing agreement, page 1 |
| Address:  | Address of the Processor named in this contract on page 1 |
| Contact person’s name, position and contact details: | Cf. Attachment 1 item 11 |
| Activities relevant to the data transferred under these Clauses: | Cf. Attachment 1 items 2 and 3 |
| Signature, date  | n/a |
| Role:  | Processor |

**B. Description of Transfer**

1. Categories of data subjects whose personal data is transferred: Cf. Attachment 1 item 4.

2. Categories of personal data transferred: Cf. Attachment 1 item 5.

3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved:

Cf. Attachment 1 item 5 „Special categories of personal data”.

4. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Cf. Attachment 1 item 6 a).

5. Nature of the processing:

Cf. Attachment 1 item 3.

6. Purpose(s) of the data transfer and further processing:

Cf. Attachment 1 item 3.

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

Cf. Attachment 1 item 6 b).

8. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

Cf. Attachment 1 item 12.

**C. Competent Supervisory Authority**

Identify the competent supervisory authority/ies in accordance with Clause 13:

Cf. Attachment 1 item 6 c.

*Annex II*

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

The technical and organizational measures relevant for this Annex II are described in more detail in item 3 of Attachment 2 to this commissioned data processing agreement.

*Annex III*

**List of Sub-Processors**

The Controller has authorized the use of the following Sub-processors:

Cf. Attachment 1 item 12.

1. Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision (EU) 915/2021. [↑](#footnote-ref-2)
2. This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible. [↑](#footnote-ref-3)
3. The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses. [↑](#footnote-ref-4)
4. The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses. [↑](#footnote-ref-5)
5. See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725. [↑](#footnote-ref-6)
6. The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses. [↑](#footnote-ref-7)
7. This includes whether the transfer and further 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 per-son, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions or offences. [↑](#footnote-ref-8)
8. This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7. [↑](#footnote-ref-9)
9. This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7. [↑](#footnote-ref-10)
10. That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension. [↑](#footnote-ref-11)
11. As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies. [↑](#footnote-ref-12)