Data Processing Agreement
in accordance with Art. 28 GDPR

between

Contracting Company (as indicated in the order or registration form)

hereinafter referred to as the "**Controller**"

and

Contracting Entity (as indicated in the order or registration form)

hereinafter referred to as the "**Processor**"
Processor and Controller collectively the "**Parties**"

Preamble

The Controller has selected the Processor to act as a service provider in accordance with Art. 28 of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, "**GDPR**").

This Data Processing Agreement, including all Annexes (hereinafter referred to collectively as the "**Agreement**"), specifies the data protection obligations of the parties from the underlying Order Form, the terms and conditions and/or the order descriptions (hereinafter referred to collectively as the "**Principal Agreement**").
The Processor guarantees the Controller that it will fulfil the Principal Agreement and this Agreement in accordance with the following terms:

Sect. 1 Scope and definitions

(1) The following provisions shall apply to all services of data processing provided by the Processor on behalf of the Controller under Art. 28 GDPR, which the Processor performs on the basis of the Principal Agreement, including all activities which may involve the processing of personal data by the Processor on behalf of the Controller.

(2) If this Agreement uses the term "data processing" or "processing" of data, this shall be generally understood to mean the use of personal data. Data processing or the processing of data shall mean any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(3) "Processor Affiliate" means an entity that owns or controls, is owned or controlled by or is under common control or ownership with Processor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

(4) Reference is made to further definitions set forth in Art. 4 GDPR.

Sect. 2 Subject matter and duration of the data processing

(1) The Processor shall process personal data on behalf and in accordance with the documented instructions of the Controller.

(2) The data processing may involve carrying out the following processing activities each as agreed and specified further in the Principal Agreement, among others:

- Online Lead Generation Service
- CRM Integration

(3) The duration of this Agreement corresponds to the duration of the Principal Agreement.

(4) The Controller may terminate this Agreement and the Principal Agreement at any time without prior notice in the event of a serious breach of this Agreement by the Processor, if the Processor fully or partially fails to execute instructions issued by the Controller, or if the Processor refuses to grant access to its business premises in breach of this Agreement. The use of the Controller's data for purposes other than those specified in this Agreement (Sect. 2) or the breach of an essential obligation of this Agreement by the Processor (such as data loss or the possibility of unauthorized access to the data by third parties) shall be considered a serious breach.

(5) Furthermore, even when the prerequisites pursuant to subsection 4 are not met, the Controller shall be entitled to terminate this Agreement and the Principal Agreement without notice if the Processor repeatedly breaches the terms of this Agreement. Prior to the termination, the Controller shall notify the Processor about the breach in writing or in text form (or email).

Sect. 3 Nature and purpose of the data processing

The nature and purpose of the processing of personal data by the Processor is specified in the Principal Agreement.

Sect. 4 Categories of data subjects

The categories of individuals affected by the processing of personal data under this Agreement ("data subjects") include:

- Controller's B2B clients and contact personnel of these clients
- Potential B2B clients and contact personnel of Controller
- Controller's website visitors

Sect. 5 Types of personal data

The following types of personal data shall be processed under this Agreement:

- Personal data (name, title)
- Contact details (email address, phone number, postal address)
- Contract data (contract details, services, Contracting Company's number)
- Contracting Company's history (phone calls, meetings, email)
- Website traffic and metadata

Sect. 6 Rights and duties of the Controller

(1) The Controller is solely responsible for assessing the lawfulness of the data processing and for safeguarding the rights of data subjects and is hence a controller within the meaning of Art. 4 (7) GDPR.

(2) The Controller is entitled to issue instructions concerning the nature, scale and method of data processing. Such instructions are also considered to be issued by the Controller when using and configuring the Processor's services and platform. Upon request by the Controller, the Processor shall confirm verbal instructions immediately in writing or in text form (e.g. by email).

(3) The Controller shall notify the Processor of any errors or irregularities detected in relation to the processing of personal data by the Processor.

Sect. 7 Duties of the Processor

(1) Data processing

The Processor shall process personal data exclusively in accordance with this Agreement and/or the underlying Principal Agreement and in accordance with the Controller's documented instructions. Any processing of data by the Processor other than in the manner described herein or in the Principal Agreement is prohibited. The Processor shall not process data provided for data processing for other purposes, in particular not for its own purposes. Copies or duplicates may not be made, unless this is part of the order, necessary in order to fulfil the Principal Agreement or unless the Controller has given its prior express written consent.

(2) Data subjects' rights

a. The Processor shall, within its capabilities, assist the Controller in complying with the rights of data subjects, particularly with respect to rectification, restriction of processing, deletion of data, notification and information. The Processor shall take appropriate technical and organizational measures for this purpose.

b. If instructed accordingly by the Controller, the Processor shall rectify, delete or restrict the processing of personal data processed on behalf of the Controller. The same applies if this Agreement stipulates the rectification, deletion or restriction of the processing of data. The Processor shall not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Controller, but only on documented instructions from the Controller (e-mail sufficient).

c. If a data subject contacts the Processor directly to have his or her data rectified, deleted or the processing restricted, the Processor shall forward this request to the Controller within a reasonable time upon receipt.

d. Controller instructs Processor to respond to data subject access requests directly (including providing information about the Controller). If Processor is unable to respond directly, Processor shall forward this request to the Controller within a reasonable time upon receipt.

Contact point for Data Subject Access Requests is the email privacy@dealfront.com

(3) Monitoring duties

a. The Processor undertakes to ensure, by means of appropriate controls, that the personal data processed on behalf of the Controller are processed solely in accordance with this Agreement and/or the Principal Agreement and/or the relevant instructions.

b. The Processor shall organize its business and operations in such a way that the data processed on behalf of the Controller are secured to the extent necessary in each case and protected from unauthorized access by third parties. The Processor will agree in advance with the Controller any changes in the organization of data processing on behalf of the Controller that are significant for data security.

c. The Processor confirms that it has appointed a Data Protection Officer in accordance with Art. 37 GDPR and that the Data Protection Officer shall monitor compliance with data protection and security laws. The appointed Data Protection Officer is:

Henri Markkanen
dpo@dealfront.com

In the event of a change of Data Protection Officer, the Processor will notify the Controller of this change in writing or in text form, naming the new Data Protection Officer.

(4) Information duties

a. The Processor shall inform the Controller immediately if, in its opinion, an instruction issued by the Controller violates legal regulations. In such cases, the Processor shall be entitled to suspend execution of the relevant instruction until it is confirmed or changed by the Controller.

b. The Processor shall assist the Controller in its maintenance of Records of Processing Activities pursuant to Art. 30 GDPR and provide the Controller with the necessary information in an appropriate manner. Furthermore, the Processor shall keep its own Record of Processing Activities with respect to all processing activities carried out on behalf of the Controller, as required in Art. 30 (2) GDPR.

c. The Processor shall notify the Controller without any reasonable delay of any breach of data protection regulations, of the Principal Agreement and the Agreement and/or the instructions issued by the Controller, where such breach occurs in the course of the processing of data carried out by the Processor, its employees or other third parties entrusted with the processing of data.

d. In the event that the Processor establishes, or if facts justify the assumption, that personal data processed by the Processor on behalf of the Controller have been unlawfully transmitted or otherwise unlawfully disclosed to third parties or that any other personal data breach has occurred, the Processor shall notify the Controller without delay and no later than 48 hours after becoming aware of the incident, providing information about

- time, nature and extent of the incident, including the number of datasets and data categories presumably affected
- possible detrimental consequences
- measures that have been taken by the Processor in order to prevent further personal data breaches in the acute case.

The Processor shall assist the Controller in the comprehensive and timely fulfilment of any reporting obligations.

(5) Location of processing

a. The processing and use of the data shall take place exclusively in the territory of the Federal Republic of Germany, in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any transfer to a third country requires the prior consent of the Controller and may only take place if the special requirements of Art. 44 et seqq. GDPR are fulfilled. This also applies to any data backups by Processor. Controller hereby expressly instructs Processor to involve Processor's affiliate based in the USA in the data processing in order to provide customer support during business hours of Processor's affiliate. In order to secure the data transfer, the Standard Contractual Clauses attached hereto as **Annex IV** are validly concluded.

b. If the processing of personal data is carried out outside the European Union, the Processor guarantees that a lawful cross-border data transfer mechanism is in place. The Processor shall inform the Controller immediately in writing if the lawful cross-border data transfer mechanism no longer applies or if it is foreseeable for the Processor that the lawful cross-border data transfer mechanism will no longer apply before the end of this Agreement.

c. The Processor shall indemnify the Controller against all claims by third parties arising from the fact that

- the lawful cross-border data transfer mechanism no longer applies due to circumstances for which the Processor is responsible, and/or
- the Processor has failed to inform the Controller in due time about the omission of the lawful cross-border data transfer mechanism.

This indemnity obligation also includes, in particular, any fines and administrative fines as well as the Controller's reasonable legal fees.

e. If the Processor's lawful cross-border data transfer mechanism ceases to apply, the Controller shall be entitled, at its own discretion,

- to terminate the Principal Agreement immediately or
- to request that the Processor, by a specified deadline, provide another lawful cross-border data transfer mechanism or conclude Standard Contractual Clauses which meet the requirements of the data protection authority responsible for the Controller, whereby the Processor shall bear the costs incurred by this procedure.

If the Processor fails to comply with the request on time, the Controller shall also be entitled to terminate the Principal Agreement. In the event of an extraordinary termination, the Processor shall, upon instruction by the Controller, assist the Controller at its own expense in transferring the personal data immediately to another processor named by the Controller.

f. If the processing of personal data takes place outside the EU, the Processor further guarantees that it has appointed a representative in the EU for the duration of the order, provided that this is necessary under the applicable data protection regulations. The representative shall be instructed to act as a contact point in addition to the Processor or in its place, in particular for supervisory authorities and data subjects, for all questions related to processing in order to ensure compliance with data protection regulations.

g. **Annex IV** to this Agreement contains the version of the "Controller to Processor Standard Contractual Clauses" valid at the time of the conclusion of this Agreement, included in the Commission Decision (EU) 2021/914 of 4 June 2021. If and to the extent that Standard Contractual Clauses apply, then nothing in this Agreement varies or modifies the provisions of these Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under these Standard Contractual Clauses. For the avoidance of doubt the Parties agree that, in case of contradicting or conflicting provisions contained in the Agreement and the Standard Contractual Clauses effectively concluded by and between the Parties, the provisions contained in the Standard Contractual Clauses shall prevail.

(6) <u>Other obligations of support and cooperation</u>

The Processor shall assist the Controller within its possibilities in ensuring compliance with the obligations pursuant to Art. 32 – 36 GDPR.

(7) Deletion of personal data after order completion

After termination of the Principal Agreement, the Processor shall be obliged to hand over to the Controller all personal data, documents and work results that are associated with the contractual relationship, as well as to delete them in compliance with data protection and data security regulations and in accordance with the instructions of the Controller. This also applies to any data backups made by the Processor.

Sect. 8 Monitoring rights of the Controller

(1) The Controller shall at all times be entitled to monitor compliance with the provisions on data protection and the contractual agreements to the extent necessary, and may perform the inspections itself or using third parties, in particular by obtaining information and inspecting the stored data and systems as well as other on-site checks. The Parties shall agree on the time of the inspection or auditing and other details ahead of time and at latest fourteen (14) days before the inspection. The auditing shall be carried out in a way that does not impede the obligations of Processor or its subcontractors in regard to third parties. The representatives of the Controller and the auditor must sign conventional non-disclosure commitments.

(2) The Processor will assist the Controller in carrying out inspections and contribute to the complete and speedy processing of the inspections. Controller shall be responsible for its own and Processor's expenses caused by the auditing.

(3) The Processor shall be obliged to provide the Controller with information insofar as this is necessary for carrying out the inspection.

Sect. 9 Docking Clause

(1) Any entity that is not a party to this Agreement may, with the prior written consent (email sufficient) of all Parties, accede to this Agreement at any time as a controller or a processor by completing the Annexes and signing Annex I.

(2) Once the Annexes mentioned in Sec. 9 (1) above are completed and signed, the acceding entity shall be treated as a Party to this Agreement and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(3) The acceding entity shall have no rights or obligations from this Agreement from the period prior to becoming a Party.

Sect. 10 Subprocessing

(1) The Controller authorizes the Processor to make use of other processors in accordance with the following subsections in Sect. 10 of this Agreement. This authorization shall constitute a general written authorization within the meaning of Art. 28 (2) GDPR. For the avoidance of doubt, subprocessing for the purpose of this Agreement means involving a third party appointed by or on behalf of the Processor to perform and conduct services which relate directly to the provisions of the Principal Agreement. This does not include ancillary services, such as telecommunication services, postal/transport services or maintenance (unless specifically covered as a service under the Principal Agreement).

(2) The Processor currently works with the subcontractors specified in **Annex III** and the Controller hereby agrees to their appointment.

(3) The Processor shall be entitled to appoint or replace other processors. The Processor shall inform the Controller in advance of any intended change regarding the appointment or replacement of another processor. The Controller may object to an intended change on reasonable grounds. If the parties are unable to reach an agreement concerning the use of a new subcontractor, the Controller is entitled to terminate the Agreement with thirty (30) days' notice, insofar as the change of subcontractor affects the Processing of Personal Data.

(4) A level of protection comparable to that of this Agreement must always be guaranteed when another processor is involved. The Processor is liable to the Controller for all acts and omissions of other processors it appoints. The Controller has the right to convince itself of the suitability of the other processor. The Processor shall provide the Controller with a copy of the subcontract upon request.

(5) In the subprocessing agreement with the other processor, the Processor must ensure that the provisions agreed between the Controller and the Processor and, if applicable, supplementary instructions from the Controller also apply in full to the other processor. This includes, in particular, the obligation to maintain confidentiality pursuant to Sect. 11 of this Agreement, the guarantee of technical and organizational measures to ensure an appropriate level of processing security, participation in the processing of inquiries from data subjects and the fulfilment of the agreed documentation obligations. In addition, the Controller shall be granted control and verification rights in the subprocessing agreement in accordance with this Agreement. In the subprocessing agreement, the details specified in Sect. 2,3,4 and 5 of this Agreement shall be specified in such a way that the responsibilities of the Processor and the other processors are clearly delimited. If more than one other processor is used, this also applies to the responsibilities between these other processors.

(6) The Processor shall regularly verify the other processor's compliance with its obligations. In particular, the Processor shall check in advance and on a regular basis during the term of the agreement that the other processor has taken the guaranteed and required technical and organizational measures to protect personal data. The result of the control must be documented by the Processor and transmitted to the Controller upon request.

(7) Processor Affiliates shall process personal data only as subprocessors.

Sect. 11 Confidentiality

(1) The Processor is obliged to maintain confidentiality when processing data for the Controller.

(2) The Processor guarantees that it is aware of the applicable data protection regulations and familiar with their application.

(3) In fulfilling its obligations under this Agreement, the Processor undertakes to employ only employees or other agents who are committed to confidentiality in the handling of personal data provided and who have been appropriately familiarized with the requirements of data protection. Upon request, the Processor shall provide the Controller with evidence of the confidentiality commitments.

(4) Insofar as the Controller is subject to other confidentiality provisions, it shall inform the Processor accordingly. The Processor shall oblige its employees to observe these confidentiality rules in accordance with the requirements of the Controller.

Sect. 12 Technical and organizational measures, Sensitive Data

(1) The technical and organizational measures described in **Annex II** are agreed upon as binding.

(2) The Processor shall observe the principles of due and proper data processing in accordance with Art. 32 in conjunction with Art. 5 (1) GDPR. It guarantees the contractually agreed and legally prescribed data security measures. It will take all necessary measures to safeguard the data and the security of the processing, in particular taking into account the state of the art, as well as to reduce possible adverse consequences for the affected parties. Measures to be taken include, in particular, measures to ensure appropriate pseudonymization and encryption, measures to protect the confidentiality, integrity, availability and resilience of systems and measures to ensure continuity of processing after incidents. In order to ensure an appropriate level of processing security at all times, the Processor will regularly evaluate the measures implemented and make any necessary adjustments. The Processor will notify the Controller in advance of any significant changes to the technical and organizational measures.

Sect. 13 Deletion and Return of Personal Data

(1) Copies or duplicates of the data processed on behalf of the Controller shall never be created without the knowledge of the Controller, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work and upon request by the Controller, at the latest upon termination of the Principal Agreement, the Processor shall hand over to the Controller or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

Sect. 14 Remuneration

The Processor's remuneration is specified in the Principal Agreement.

Sect. 15 Liability/Indemnification/Contractual penalty

(1) The Processor shall be liable to the Controller for any and all loss or damage culpably caused in the performance of the services under the Principal Agreement or by a breach of applicable statutory data protection obligations on the part of the Processor, its employees or parties commissioned by it to implement the Principal Agreement.

(2) Within the context of their contractual relationship under the Principal Agreement, the Controller and the Processor shall be obligated to compensate data subjects for damage caused by them arising from the unlawful or improper processing of their data within the meaning of the GDPR or other data protection provisions as stipulated in Art. 82 GDPR. As regards the parties inter se, the Processor shall indemnify the Controller against any and all claims for damages asserted against the Controller based on the Processor's culpable breach of its own obligations under data protection regulations or on non-observance of instructions lawfully issued by the Controller. The Controller shall bear the burden of proof for non-compliance of Processor with Processor's obligations under data protection regulations and for non-compliance with instructions lawfully issued by the Controller. The Controller shall also bear the burden of proof that the damages are due to the Processor's breach of duty and that Processor was responsible for such breach.

Sect. 16 Miscellaneous

(1) In case of contradictions between the provisions contained in this Agreement and provisions contained in the Principal Agreement, the provisions of this Agreement shall prevail.

(2) Amendments and supplements to these provisions must be in writing and expressly declare that the provisions in this Agreement are being changed and/or supplemented. The foregoing also applies to the formal requirement itself.

(3) This Agreement is exclusively subject to the laws as set forth below:

Contracting Dealfrontt affiliate is:	**Governing law:**	**Courts with exclusive jurisdiction are located in**
Dealfront Finland Oy	the laws of Finland under exclusion of the UN Sales Convention and without giving effect to any principles of conflicts of law	Helsinki, Finland
All other contracting entities	laws of the Federal Republic of Germany under exclusion of the UN Sales Convention and without giving effect to any principles of conflicts of law	place of the registered office of Dealfront Group GmbH

(4) In the event that access to the data which the Controller has transmitted to the Processor for data processing is jeopardized by third-party measures (measures taken by an insolvency administrator, seizure by revenue authorities, etc.), the Processor shall notify the Controller of such without undue delay.

Schedule of Annexes

Annex I List of Acceding Parties

Annex II Technical and organizational measures taken by the Processor to ensure the security of processing

Annex III Subprocessors pursuant to Sect. 10 of this Data Processing Agreement

Annex IV Standard Contractual Clauses - Controller to Processor

Annex I

List of Acceding Parties

Controller(s) (Identity and contact details of the controller(s) and, where applicable, of the respective controller's data protection officer

1. Company name:

   Address:

   Contract person's name, position and contact details:

Processor(s) (Identity and contact details of the processor(s) and, where applicable, of the respective processor's data protection officer

1. Company name:

   Address:

   Contract person's name, position and contact details:

Annex II

Technical and organizational measures to ensure the security of processing

The Processor guarantees that the following technical and organizational measures have been taken:

A. Encryption measures

Measures or operations in which a clearly legible text/information is converted into an illegible, i.e. not easily interpreted, character string (secret text) by means of an encryption method.

Description of the encryption measure(s):

- Data encryption in transit and at-rest

B. Measures to ensure confidentiality

1. **Physical access control**

Measures that physically deny unauthorized persons access to IT systems and data processing equipment used to process personal data, as well as to confidential files and data storage media.

Description of physical access control:

- Individual access control on need-to-know basis
- Monitoring the entrances to the facilities (data centres outsourced)
- Doors to the server rooms/cabinets and other security areas are always closed and access is regulated (data centres outsourced)
- Visitors or external service providers are admitted individually
- The disposal or reusing of equipment is regulated
- Clean desk and screen locking policy

2. **Logical access control**

Measures to prevent unauthorized persons from processing or using data which is protected by data privacy laws.

Description of logical access control system:

- Individual access control on need-to-know basis
- Detailed access and actions logging in all application infrastructure
- Technical monitoring 24/7

3. **Data access control**

Measures to ensure that persons authorized to use data processing systems can only access personal data according to their access rights, so that data cannot be read, copied, changed or removed without authorization during processing, use and storage.

Description of data access control:

- Individual access control on need-to-know basis
- Detailed access and actions logging in all application infrastructure
- All workstations are encrypted, antivirus software and screen lock in place
- Password policy in place, MFA enforced where applicable, SSO used widely

4. **Separation rule**

Measures to ensure that data collected for different purposes are processed separately and separated from other data and systems in such a way as to preclude the unplanned use of such data for other purposes.

Description of the separation control process:

- Authorization concepts
- Data encryption in transit and at-rest

C. Measures to ensure integrity

1. **Data integrity**

Measures to ensure that stored personal data cannot be corrupted by means of a malfunctioning of the system.

Description of data integrity:

- Continuous vulnerability scanning and penetration testing
- Technical monitoring 24/7

2. **Transport control**

Measures to ensure that the confidentiality and integrity of data is protected during transmission of personal data and transport of data carriers.

Description of transport control:

- Transmission of data via encrypted data networks or tunnel connections (VPN)
- Comprehensive logging procedures

4. **Input control**

Measures to ensure that it can be subsequently verified and ascertained whether and by whom personal data have been entered or modified in data processing systems.

Description of the input control process:

- Logging of all system activities

D. Measures to ensure availability and resilience

1. **Availability control**

Measures to ensure that personal data are protected against accidental destruction or loss.

Description of the availability control system:

- Data backup procedure
- Uninterrupted power supply
- Fire alarm system
- Air conditioning
- Alarm system
- Business continuity and emergency plans

2. **Quick recovery**

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

Description of the measures for quick recovery:

- Data backup procedure
- Regular tests of data recovery
- Business continuity and emergency plans

Annex III

Subprocessors pursuant to Sect. 10 Data Processing Agreement

The Processor currently works with the following subcontractors and the Controller hereby agrees to their appointment. The processing and use of personal data shall take place exclusively in the territory of the Federal Republic of Germany, in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any transfer to a third country requires the prior consent of the Controller and may only take place if the special requirements of Art. 44 et seqq. GDPR are fulfilled. This also applies to any data backups by Processor.

If data processing takes place outside the European Economic Area (EEA) or if access is made from outside the EEA, the following overview must also list the measures and guarantees that ensure an appropriate level of data protection during processing in accordance with Art. 44 GDPR ff. (e.g. EU Standard Contractual Clauses, Binding Corporate Rules or other arrangements by the European Commission).

Company: Amazon Web Services
Data processing activity: Hosting/Cloud Service Provider
Location: EU/EEA

Company: Dealfront Germany GmbH
Data processing activity: Data Infrastructure and IT security
Location: EU/EEA

Company: Dealfront Finland Oy
Data Processing activity: Data Infrastructure and IT security
Location: Finland

Company: Dealfront Inc.
Data Processing activity: Customer Support
Location: USA

Annex IV

STANDARD CONTRACTUAL CLAUSES

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

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

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

(b) Once it has completed the Appendix and signed Annex I, 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.

(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.

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 (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 benefiting 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.

Clause 9

Use of sub-processors

(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 two weeks 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. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

(a) 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.

(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

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

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

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

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

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

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

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

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

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer 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. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the

contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

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 of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

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

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

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

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

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

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

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

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. **Customer** (as indicated in the order or registration form)

Data importer(s):

2. **Contracting Party** (as indicated in the order or registration form)

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Please refer to section 4 of the data processing agreement concluded between Controller and Processor**.**

Categories of personal data transferred

Please refer to section 5 of the data processing agreement concluded between Controller and Processor

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

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

Nature of the processing

Please refer to section 3 of the data processing agreement concluded between Controller and Processor

Purpose(s) of the data transfer and further processing

Please refer to section 3 of the data processing agreement concluded between Controller and Processor

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

As long as needed in accordance with the corresponding Principal Agreement concluded between the Controller and the Processor.

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

As long as needed in accordance with the corresponding service agreement concluded between the Controller and the Processor.

C.COMPETENT SUPERVISORY AUTHORITY

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

The supervisory authority responsible for the data exporter

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Please refer to Annex II of the data processing agreement concluded between the Controller and the Processor.

ANNEX III –LIST OF SUB-PROCESSORS

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

Please refer to Annex III of the data processing agreement concluded between the Controller and the Processor.