DATA PRIVACY ADDENDUM

THIS DATA PRIVACY ADDENDUM (this "**DPA**") is an addendum to the Purchase Order Terms and Conditions ("**Terms**") issued by Martinrea International, Inc., or any affiliated company ("**Buyer"**) and the supplier of goods and/or services and its affiliates (collectively, "**Seller**"), (referred to individually as a "**Party**" and collectively as the "**Parties**").

This DPA reflects the Parties' agreement with respect to Seller's processing of Buyer Personal Data in connection with the Terms.

1. DEFINITIONS AND INTERPRETATION

1.1 All terms not defined herein will have the same meaning as set forth in the Terms. The following terms shall have the following meanings:

"Data Protection Laws" means for the purposes of this DPA, applicable laws relating to privacy and/or data protection, which are applicable to either Party. It shall include without limitation and as applicable (i) the EU e-Privacy Directive 2002/58/EC as implemented by countries within the European Economic Area ("**EEA**"); (ii) the the EU General Data Protection Regulation (EU) 2016/679 ("**GDPR**") as implemented by countries within the EEA; and (iii) other laws, rules and regulations that are similar, equivalent to, or successors to the laws that are identified in (i) through (ii) above.

"Buyer Personal Data" means personal data processed by Seller in connection with the provision of goods and/or services to Buyer.

"**Restricted Transfer**" means a transfer of personal data from or which originated in the EEA to a Third Country that is not considered to provide an "adequate level" of data protection by the European Commission and where such transfer is subject to the GDPR.

"**Standard Contractual Clauses**" means the Standard Contractual Clauses attached at Exhibit B.

"**Third Country**" means a country outside of the EEA.

The terms "**controller**", "**data subject**", "**joint controller**", "**personal data**", "**personal data breach**", "**processing**", "**processor**", and "**supervisory authority**" shall have the same meanings ascribed to them under the GDPR.

1.2 To the extent the terms contained in this DPA conflict with those contained in the Standard Contractual Clauses, the terms in the Standard Contractual Clauses shall prevail.

2. GENERAL

To the extent Seller, in connection with Seller's performance of its obligations under the Terms, is processing Buyer Personal Data and the GDPR applies to the processing of such Buyer Personal Data, the provisions as set forth in this section shall apply.

Seller as Controller

Where Seller acts as controller when processing Buyer Personal Data, Seller shall:

(i) only process Buyer Personal Data in accordance with Data Protection Laws and in accordance with the objectives and purposes for which Buyer and Seller entered into the Terms (and not for other purposes);

(ii) notify Buyer in the event of a dispute or claim brought by a data subject or a governmental authority concerning the processing of Buyer Personal Data;

(iii) notify Buyer as soon as possible where Seller is legally compelled to disclose Buyer Personal Data to a governmental authority before such disclosure, unless where legally prevented from doing so;

(iv) provide assistance to Buyer as may be reasonably be required to enable Buyer to comply with its obligations under Data Protection Laws;

(v) at the election of Buyer, return all Buyer Personal Data to Buyer at the end of the term of the Terms, or securely delete existing copies of such Buyer Personal Data unless applicable laws in the EEA require storage of such Buyer Personal Data beyond such term; and

(vi) ensure all Restricted Transfers of Buyer Personal Data are made in compliance with Data Protection Laws.

Seller as Processor

(a) Where Seller acts as processor when processing Buyer Personal Data, Seller shall:

(i) process Buyer Personal Data in accordance with Data Protection Laws and Buyer's instructions that are set out in this paragraph, the Terms and Buyer's future instructions in writing or in any other documented format (e.g. emails), including as to the subject-matter and duration of the processing, the nature and purpose of the processing, the type of Buyer Personal Data and categories of data subjects as set out in Exhibit A (Data Processing);

(ii) ensure that Seller's personnel, agents and contractors who process Buyer Personal Data are subject to appropriate obligations of confidentiality;

(iii) within 48 hours notify Buyer, and provide Buyer with copies, of all communications from, or requests made by, data subjects in relation to their

rights under Data Protection Laws and supervisory or other governmental authorities, in relation to Buyer Personal Data;

(iv) comply with Data Protection Laws and the terms of this DPA at its own cost; and

(v) ensure all Restricted Transfers of Buyer Personal Data are made in compliance with Data Protection Laws.

(vi) implement appropriate technical and organizational security measures in relation to Buyer Personal Data which, at a minimum, meet the requirements of the measures set out in Annex II to Exhibit B (irrespective of whether the Parties undertake a Restricted Transfer); and

(vii) taking into account the nature of Seller's processing of Buyer Personal Data and the information available, Seller will, within 24 hours, notify Buyer of personal data breaches in relation to the Buyer Personal Data that it becomes aware of, and at Buyer's request, provide assistance to Buyer in relation to personal data breaches.

(b) Where Seller acts as processor when processing Buyer Personal Data, and notwithstanding anything to the contrary in this DPA, in the event an actual or suspected personal data breach arises due to Seller's failure to comply with its obligations under the Terms, this DPA and/or Data Protection Laws, the Seller shall, on the instructions of Buyer, remedy any harm or potential harm caused by such personal data breach at its own cost. To the extent that a personal data breach gives rise to a need to:

(i) provide notification to supervisory or other governmental authorities, law enforcement agencies, individuals, or other persons; or,

(ii) undertake other remedial measures, (collectively a "**Remedial Action**"), the Seller shall be liable for the costs associated with such Remedial Actions as they may relate to Buyer Personal Data.

(c) Where Seller acts as processor when processing Buyer Personal Data, Seller shall at Buyer's request:

(i) taking into account the nature of Seller's processing activities, reasonably assist Buyer in relation to Buyer Personal Data, in connection with communications from, or requests made by data subjects or supervisory or other governmental authorities, including any privacy impact prior consultations with data protection authorities;

(ii) taking into account the nature of Seller's processing activities and the information available to Seller provide assistance to Buyer in

relation to the performance of data protection impact assessments by Buyer under Data Protection Laws; and

(iii) delete or return all Buyer Personal Data to Buyer at the end of the term of the Terms, and securely delete existing copies of such Buyer Personal Data unless Data Protection Laws in the EEA require storage of such Buyer Personal Data beyond such term.

(d) Where Seller acts as processor when processing Buyer Personal Data, at Buyer's request, Seller shall make available to Buyer all information reasonably necessary to demonstrate compliance with Seller's obligations under this DPA and Data Protection Laws and allow for and contribute to audits, including inspections, conducted by Buyer or another auditor mandated by Buyer or under Data Protection Laws, *unless* Seller notifies and substantiate to Buyer in writing if it believes in good faith that the exercise of rights under this subparagraph (e) would infringe Data Protection Laws.

3. INTERNATIONAL TRANSFERS

(a) Seller may transfer and otherwise process Buyer Personal Data outside the EEA, including by any sub-processor *provided* that such transfer is made in compliance with applicable Data Protection Laws. This includes but is not limited to Seller being responsible for implementing appropriate safeguards when transferring or procuring the transfer of Buyer Personal Data outside the EEA – even where such transfer is to Buyer. Nevertheless such transfer should in all cases be previously authorized by Buyer.

(b) To the extent the terms in the Terms conflict with those terms contained in Exhibit B, which contain the Standard Contractual Clauses, the terms in Exhibit B shall prevail to the extent such conflict relates to a Restricted Transfer.

(c) As applicable, Seller shall provide adequate notices to data subjects, and obtain valid consents from data subjects, in each case to the extent necessary for Buyer and/or its service providers or agents to process their personal data under the Terms which may include the transfer of the personal data outside of the EEA.

(d) The parties acknowledge that where Buyer ("**Data Exporter**") undertakes Restricted Transfer of Buyer Personal Data to Seller ("**Data Importer**"), the parties shall process the personal data which is subject to the Restricted Transfer in accordance with the terms of this DPA. The parties further acknowledge and agree that:

(i) if each of the Data Exporter and the Data Importer is a controller, Module 1 of the Standard Contractual Clauses, annexed hereto as Exhibit B, applies to the processing; and

(ii) if the Data Exporter is a controller and the Data Importer is a processor, Module 2 of the Standard Contractual Clauses applies to the processing.; and

(iii) if the Data Exporter is a processor and the Data Importer a controller, Module 4 of the Standard Contractual Clauses applies to the processing.

(e) The Parties acknowledge and agree that to the extent:

(i) the Data Importer is subject to the requirements of the GDPR with regards the processing of the personal data subject to a Restricted Transfer; and

(ii) the Data Importer's obligations in the Standard Contractual Clauses conflict with Data Importer's obligations under the GDPR in regard the processing of such personal data;

Data Importer shall only need to comply with its obligations under the GDPR with regard to such processing where such obligation under the GDPR is more onerous.

(f) Buyer's issuance of an Order under these Terms and Seller's expression of acceptance of an Order, including Seller's commencement of (i) work on or shipment of the goods subject to an Order, whichever occurs first, or (ii) performance of all or any portion of the services shall constitute signature by an authorized representative of Buyer and Seller of the Standard Contractual Clauses.

4. AMENDMENT This DPA may be modified in accordance with the provisions on modification in the Terms.

4.2 Notwithstanding the foregoing, the Parties acknowledge that should the European Commission publish new standard contractual clauses or similar (or amendments to the existing Standard Contractual Clauses) to address Restricted Transfers, and where Buyer determines such new or amended clauses are required to address the Restricted Transfers, such new or amended clauses will replace the Standard Contractual Clauses attached to this DPA upon Buyer's notification to Seller thereof. All Restricted Transfers will be thereafter made pursuant to such new or amended clauses.

Exhibit A – Data Processing

Nature of the processing	Automated and manual processing including: Collection Use Analysis Transfer Storage Erasure Other
Subject matter and purpose of the processing	To provide Buyer with Services under the Terms
Duration of the processing	For the duration of the Terms and thereafter deleted or returned to Buyer
Categories of data subjects	Employees Officers Directors Contractors Business associates Customers Other
Types of personal data	Name Address Telephone number Email address Date of birth

	Bank details Employment / education history Salary Government ID numbers Other

Exhibit B – 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)1 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

---

[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 […].

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 Four: Clause 8.1 (b) and Clause 8.3(b);

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Modules 1 and 2: 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, thoseterms shall have the same meaning as in that Regulation.

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

(c) These Clauses shall not be interpreted in a way that conflicts with rights andobligations 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 organisationalmeasures, 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 thetransfer, as set out in Annex I.B. It may only process the personal data for another purpose:

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

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

(c) 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 providingmeaningful 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 Appendices 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 withoutundue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limitedto 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] of the data andall 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 dataimporter 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 personaldata 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 whommore information can be obtained. To the extent it is not possible for the data

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable byanyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

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 databreach, 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] (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:

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

---

[3] The Terms on the European Economic Area (EEA Terms) 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 Terms 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.

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

(c) 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;

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

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

(f) 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 describedin Annex II and personal data, the data exporter may redact part of the text of the Appendix tothese 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. Onrequest, 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 tothe 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, thedata 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 subjectshall, 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 dataimporter 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 itspossible 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 tothe 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 partylocated outside the European Union[4] (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:

(a) 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;

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

(c) 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

(d) 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 accountrelevant 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.

---

[4] The Terms on the European Economic Area (EEA Terms) 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 Terms 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.

(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 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[5], 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**

[5] 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 person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

(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 thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[6] 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.

---

[6] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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.[7] 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 todo so under the laws of the country of destination, provided that such laws lays downsuitable 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

---

[7] That period may be extended by a maximum of two more months, to the extent necessary taking into accountthe complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(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 humanbeing.

(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 therequest.

(f) The data importer may refuse a data subject's request if such refusal is allowed underthe 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 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

(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 issueamicably 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;

(i) 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 causesthe 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

(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

(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 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[8];

(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

---

[8] As regards the impact of such laws and practices on compliance with these Clauses, different elements maybe 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 whethertheir 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.

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 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 shallinclude 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 asmuch 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 itis 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 thedata 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 morethan 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) **MODULES ONE AND TWO:** 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.

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 deletionof the data to the data exporter. Until the data is deleted or returned, the data importershall 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

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 Spain.

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 Spain.

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 Spain.

(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 Spain.

APPENDIX

ANNEX I

A. LIST OF PARTIES

	Module 1	Module 2	Module 4
Data Exporter Name: **Data Exporter Address:** **Data Exporter Contact Person:**	• Buyer details as provided in the Order • Seller details as provided in the Order	Buyer details as provided in the Order	Seller details as provided in the Order
Role of Data Exporter:	Controller	Controller	Processor
Data Importer Name: **Data Importer Address:** **Data Importer Contact Person:**	• Buyer details as provided in the Order • Seller details as provided in the Order	Seller details as provided in the Order	Buyer details as provided in the Order
Role of Data Importer:	Controller	Processor	Controller
Activities relevant to the data transferred under these Clauses:	Commercial and sales activities and Seller/Buyer relationship and account management related to the provision of Services and Goods to Buyer under the Terms		
Signature of Buyer:	Through issuance of the Terms the data exporter will be deemed to have signed this Annex I		
Signature of Seller:	Through acceptance of the Order and/or the Terms, including commencement of (i) work on the goods or shipment of the goods, both subject to the Terms, whichever occurs first, or (ii) performance of all or any portion of the services subject to the Terms, the data importer will have deemed to have signed this Annex I		

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
See Exhibit A to these Terms.

Categories of personal data transferred
See Exhibit A to these Terms.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully takeinto 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.
See Exhibit A to these Terms.

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

Nature of the processing
Personal data will be subject to automated and manual processing operations including, collection, use, analysis, transfer, storage and erasure.

Purpose(s) of the data transfer and further processing
To provide/ receive the goods and services under the Terms, including for account management purposes.

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

Buyer as data importer: For as long as necessary to fulfil the purposes for which it was transferred, including for the purposes of satisfying any legal, accounting or reporting requirements. To determine the appropriate retention period, the amount, nature and sensitivity of the personal data are considered, together with the necessity and purposes for the processing (including, whether such purposes can be achieved through other means) and the potential risk of harm from unauthorized use or disclosure of the personal data

Seller as data importer: Until termination or expiry of the Terms and thereafter returned or deleted in accordance with paragraph 22 of the Terms.

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

For the subject matter, nature and duration as identified above

C. COMPETENT SUPERVISORY AUTHORITY – MODULES 1 and 2 ONLY

Identify the competent supervisory authority/ies in accordance with Clause 13:
Pursuant to Clause 13, the supervisory authority of the EEA country where (i) the data exporter is established; or where (ii) the EU representative of the data exporter is established; or where (iii) the data subjects whose personal data are transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located.

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

Where Seller is Data Importer: Data importer shall implement, at a minimum, the following physical, technical, and organizational security measures to ensure a level of security in line with the nature, scope, context, and purpose of the processing of personal data and the risk the processing present for the rights and freedoms of data subjects:

1. **Physical Measures**
    a) Implement and enforce physical access controls to processing premises and facilities, provisioning access to the processing facilities on the basis of the role (need to know), and utilizing physical Access Control Mechanisms such as Electronic Access Control (EAC) cards to access server rooms, install CCTV systems, etc.
    b) Audit trails of all admissions into and out of server rooms must be maintained and reviewed by hosting center management on a periodic and need to know basis.
    c) Establish and implement adequate physical protection measures against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster.
2. **Organisational Measures**
    a) Designate a security officer or other person responsible for overseeing the security program; this person shall drive and be responsible for continuous improvement of the Information Security Program.
    b) All security personnel must be adequately trained and qualified.
    c) Establish and implement a process and written policies and rules to ensure the appropriate and secure processing of personal data, including, in particular, incident response and acceptable use policies. This shall also include without limitation policies or specific rules for regularly testing, assessing, and evaluating the effectiveness of physical, technical and organizational measures for ensuring the security of the processing of personal data and preventing leakage, loss or damage of personal data.
    d) Information Security Training and Awareness shall be conducted and provided to all staff on a yearly basis at minimum; Recommended topics to address include but are not limited to Business Email Compromise, Phishing, Safe Web Browsing, Mobile Device and Cloud Security.
    e) Provide employee and contractor training to ensure ongoing capabilities to carry out the security measures established in the written policies.

f) Account for all the risks that are presented by processing, such as from accidental or unlawful destruction, loss, or alteration, unauthorized or unlawful storage, processing, access or disclosure of personal data.

3. Technical Measures

a) Access Management:

1. Ensure that the personal data can be accessed only by authorized personnel for the purposes set forth in the Data Processing Terms. Authorized personnel are to be based on the "need to know" principle.
2. User Account Management must include processes for granting, denying, canceling, terminating and deactivating/decommissioning access to information systems. Regular review, at least yearly, of existing users and authorizations must be performed.
3. User Access Management must include use of strong passwords or pass phrases (recommended 12 characters or longer). For all remote access connections, a VPN and multifactor authentication must be used. Internal multifactor authentication is highly recommended.

b) Network Security and Data Encryption:

1. External data transmissions of personal data must be encrypted using non-deprecated security protocols (example: use TLS1.2 or higher, do not use TLS 1.0 or 1.1). Weak and obsolete cipher suites like RC2, RC4, DES, IDEA and TDES/3DES should not be used.
2. Use Network Intrusion Detection or Network Intrusion Prevention technology.
3. Key Management – well defined key management and key escrow procedures must be implemented. Server certificates must be managed and secured, and these processes be clearly understood by technical personnel within data importer/exporter.

c) Operating System Security: Operating systems must be protected with anti-malware/virus protection software. Server and cloud operating systems must be deployed using a secure build process.

1. Security Logging is enabled per vendor recommendations for all desktop, server, and network infrastructure OS.
2. Next Generation Endpoint protection/EDR with advanced ransomware protection settings is recommended.
3. Operating System versions must not be end-of-life.
4. Anti-virus signatures must be updated regularly.

d) System Configuration: Use hardened systems, to include but not limited to:

1. Eliminate or disable needless system applications, drivers, permissions, database services, ports, user accounts, and other features not necessary for the functioning of the application.
2. Keep the operating system and application patched and updated.
3. Regularly update 3rd party software that's needed for the application (example, Java).
4. Use long and strong passwords, especially for administrative and privileged accounts.
5. Automatically lock user accounts after several unsuccessful (recommended 5 to 7) login attempts.
6. Disable USB Ports at boot.
7. Use multifactor authentication for all externally accessible systems (MFA for internal systems housing sensitive data is recommended).
8. Use local firewalls and antivirus/malware software.
9. Encrypt sensitive data at rest and in transit using state-of-the-art encryption as agreed on with data exporter.
10. Limit system access to only necessary permissions needed (Role Based Access recommended).

Recommended: configure systems in alignment with NIST SP 800-123 or leverage Computer Information Security (CIS) Center for Internet Security configuration baselines.

e) Incident Response:

1. Maintain an Enterprise Information Security Incident Response plan that is tested at least annually.
2. Implement and maintain technology that allows to detect malicious activity, vulnerabilities and security incidents generally on your systems, such as Network Intrusion Detection.

f) Event Logging:

1. Implement appropriate IT systems designated to detect fraudulent or harmful activity (e.g., an attack).
2. Maintain logs on relevant events, including a personal data breach log.

g) Control/Audit Trails:

1. Use built in system and audit trails. Use of a centralized read-only logging system such as a System Information and Event Management system with the capacity to store 6 months of log data per application is recommended. Recommended minimum configuration is timestamp, who (identity of the operator), what (information about the event), source system.

2. Conduct audits of your systems and data security measures on a no less than annual basis.

h) Data Retention and Data Subject Rights:

1. Set a data retention policy limiting the need for protecting data that is no longer needed.
2. Implement controls and systems that allow to comply with data retention policy and data subject rights requests within statutory and contractual timelines. For instance, have systems in place to automatically detect relevant personal data that is the subject of a data portability / erasure request, and has systems in place to ensure automatic deletion/transmission to the data subject or a third party of choice.
3. Have controls and systems in place to segregate personal data from other data, including when processed (e.g.: multiple controller support, sandboxing).

i) Vulnerability Management:

1. Perform routine (at least quarterly) scanning or penetration testing of your systems. Remediate all critical and severe items in a timely manner (less than 3 months). For items that cannot be remediated quickly, implement compensating controls to reduce the risk of the vulnerability.

j) Patch Management:

1. Perform routine (at least quarterly) maintenance on operating systems and applications to keep security patches current.

k) Pseudonymization/Encryption:

1. Ensure pseudonymization and/or encryption of personal data, where appropriate and/or as agreed on with between the data importer and exporter.
2. Where personal data is or should be encrypted, encryption should be state-of-the-art, and the encryption standard must be commensurate to the risk involved in the processing.
3. Personal data must be encrypted in transit and at rest, save as otherwise agreed between the data importer and exporter.

l) Availability Control: Maintain the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

1. Establish a high availability solution for systems to maintain resiliency or a recovery plan based on the SLAs or similar contractual commitments that establishes the availability of the data and business requirements.
2. Have encryption enabled at the database and/or storage layer as well as in transit.
3. Have a Disaster Recovery Plan in place that protects the data from cyberattacks, natural site disasters and site disasters. Annual tests should

be done to ensure the recovery plan is working as expected and meets the business requirements.

4. Maintain the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
5. Policy and procedures should be in place to follow best practices for system backups and recovery. There should also be SLAs in place for those applications. Establish a practice to test the backup and recovery to ensure that the solution is operating as expected and SLAs are met.
6. Seller should have obtained and maintain in good standing at least the following security certificates: SOC2 and ISO 27001.

m) Data Minimization and Quality:

1. Implement measures to ensure data minimization, i.e., to ensure only the minimum amount of personal data necessary are being processed and shared with third
2. outside data importer/exporter.
3. Implement technical controls, measures and internal policies to facilitate and allow you to comply with data quality requirements under applicable data protection laws.

4. Subcontractors:

a) Undertake due diligence on sub-contractors to ensure only subcontractors that are capable of maintaining security consistent with this Annex II and of complying with applicable data protection laws are appointed.

5. Monitor Compliance:

a) Implement suitable measures to monitor system administrators and ensure that they act according to the instructions received and data protection laws; individually designate system administrators and keep their access logs secure, accurate and unmodified for at least six months; and yearly audit system administrators' activity to assess compliance with assigned tasks, instructions received and data protection laws, keep an updated list with identification details (e.g. name, surname, function or organizational area and tasks assigned), and provide it promptly to data exporter upon request.

b) Monitor compliance to measures stated above on an ongoing basis to ensure measures implemented are still state-of-the-art and commensurate to the risk involved in the processing.

6. Accountability:

a) Maintain records in line with the Standard Contractual Clauses for all personal data processing activities.

b) Maintain adequate consent logs (where applicable) for all data processing activities.

Where Buyer is Data Importer:

The data importer has implemented the following technical and organisational measures to ensure a level of security in line with the nature, scope, context, and purpose of the processing and the risks the processing presents for the rights and freedoms of natural persons:

***Measures of pseudonymisation and encryption of personal data**:*

- All applicable data is encrypted with strong encryption solution, at rest and in transit.

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

- Firewalls are updated, supported, managed and maintained by a third party, SOC certified vendor.
- MDR – Managed Detection & Response, MVM – Managed Vulnerability Management are in place through a third party, SOC certified vendor, and is globally implemented in phases.
- Patch management and global infrastructure visibility provided by endpoint management solution, and is centrally managed with limited access delegation globally.
    - This endpoint management produced is also used for vulnerability remediation.
- Endpoint malware protection centrally managed with limited access delegation globally.
- ISO 27001 certification pending approval for our corporate offices.
- Bergneustadt plant is TISAX certified. Meschede plant's certification pending approval.
- Cyber security training delivered to staff globally via Learning Management System.
- Phishing campaigns and associated mandatory training in place.
- Information Security Policies are maintained and updated regularly.

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

- Enterprise backup solution in place. Backups are taken regularly in accordance with established backup policies.
- Backup team members are responsible for the maintenance and verification of both backup and recovery.
- Our backup solution meets the minimum recovery point objective and recovery time objective as per company policy.

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

- Internal and third-party audits, including vulnerability and penetration testing assessments, are performed regularly to validate the effectiveness of organizational security controls.
- Annual internal penetration testing
- Quarterly external penetration testing

***Measures for user identification and authorisation**:*

- Identification and authorization, dedicated per individual user/account, is subject to security controls including but not limited to two-factor authentication, segregation of duties, identify access management policy, and remote access management.

***Measures for the protection of data during transmission**:*

- Security controls are in place for removable devices, such as USB flash drives.
- Data shared with both internal and external parties via authorized secure file transfer protocols (SFTP).

***Measures for the protection of data during storage**:.*

- Sensitive data at rest, is encrypted based on business case requirements, aligning with company security policies, where applicable.

***Measures for ensuring physical security of locations at which personal data are processed**:*

- Physical measures are implemented as necessary to ensure the security of personal information, including implementing:
    - RFID badge and readers
    - CCTV surveillance
    - Alarm systems
    - Locked filing cabinets
    - Clean-desk policy

***Measures for ensuring events logging**:*

- Managed Detection & Response solution is in place, and we are actively monitoring available event logs, ensuring visibility to detect any breach of personal data.
- We maintain a personal data breach log.

***Measures for ensuring system configuration, including default configuration**:*

- Security policies are in place to enforce best practices on password policies, application control, and access management.
- Change management processes are also in place to ensure approval is obtained for any configuration or software installation.

***Measures for internal IT and IT security governance and management**:*

- Security governance is based on internal IT organizational hierarchy, to support the business and protect personal data.

Measures for ensuring data minimisation*:*

- We collect only the necessary information required to provide our products and services.

Measures for ensuring data quality*:*

- Policies are in place to keep personal information accurate and up to date .

Measures for ensuring limited data retention.:

Measures for ensuring accountability*:*

- Dedicated personal Data Protection and IT Security Officer is responsible for applicable sensitive data held by the organization, including personal information transferred to third party for processing.

Measures for allowing data portability and ensuring erasure*:*

- Commonly accepted ways are in place to irreversibly destroy the media which stores personal information, so that personal information cannot be reconstructed or recovered in any way.

Measures for handling and responding to data subject rights' requests*:*

We have internal guidelines in place for responding to requests from data subjects in accordance with our Global Data Protection Policy

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

Deliberately left blank