Vendor Data Processing Agreement

This Data Processing Agreement ("**DPA**"), effective as of by and between Koch Business Solutions, LP ("**Company**") and and its Affiliates ("**Vendor**") sets forth the terms and conditions relating to the privacy, confidentiality, security and protection of Personal Data (as defined below) associated with services rendered by, and/or products provided by, Vendor to Company (and/or its Affiliates or customers pursuant to any agreement between Vendor and Company (and/or its Affiliates) (collectively, Company and Vendor are the "**Parties**"), regardless of whether such agreement exists as of or after the Effective Date (such agreement as applicable, the "**Services Agreement**", which, together with this DPA, the "**Agreement**").

1. Definitions

"***Affiliates***" means any entity that now or in the future directly or indirectly controls, is controlled by, or is under common control or ownership for as long as such control exists, where "control" (including the terms "controlled by" and "under common control with") means the possession, directly or indirectly, of the power to direct, influence or cause the direction of the management policies of an entity, whether through the ownership of voting securities, by contract, or otherwise.

"***Data Controller***" means the entity which determines the purposes and means of Processing Personal Data.

"***Data Processor***" means the entity which Processes Personal Data on behalf of the Data Controller.

"***Data Protection Laws***" means, as applicable to the Parties all laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective relating in any way to the privacy, confidentiality, security or protection of Personal Data, including without limitation, the GDPR, the UK Data Protection Act 2018, the UK GDPR, the Swiss Federal Act on Data Protection, as amended, replaced or superseded, LGPD and any such laws, rules, regulations, directives and governmental requirements in the United States (including the California Consumer Privacy Act of 2018 ("CCPA"), Cal. Civ. Code §§ 1798.00, et seq., its implementing regulations, and similar laws passed in other states as they become effective).

"***Data Subject***" means an identified or identifiable natural person to which the Personal Data pertains.

"***Europe***" or the "***EU***" means the European Economic Area plus Switzerland.

"***GDPR***" means collectively the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 as amended or replaced from time to time (the "EU GDPR"), and the "UK GDPR" (the EU GDPR as incorporated into UK law by the UK Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, (each as amended or replaced from time to time))).

"***LGPD***" means the Federal Law n. 13,709 or August 14, 2018 for Brazil ("Lei Geral de Proteção de Dados").

"***Personal Data***" means any data, information or record that is Processed in connection with the Services Agreement (i) relating to an identified or identifiable natural person, or (ii) that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household, regardless of the media in which it is maintained.

"***Personal Data Breach***" means the breach of security leading or reasonably expected to lead to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Personal Data Processed under the Services Agreement.

"***Process***", "***Processing***" or "***Processed***" means 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.

"***Sell***" or "***Selling***" shall have the meaning ascribed to it in the applicable Data Protection Law.

"***Standard Contractual Clauses***" or "***SCCs***" means the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, and implemented by the European Commission decision 2021/914, dated 4 June 2021.

"***Subprocessor***" means other processors used by Vendor to process Personal Data.

"***Supervisory Authority***" means (i) an independent public authority which is established by an EU member state pursuant to Article 51 of the EU GDPR; (ii) the Information Commissioner's Office for the purposes of the UK; or (iii) a government regulator or enforcement authority which has regulatory or enforcement authority with respect to the privacy, confidentiality, security or protection of Personal Data.

2. Nature of Data Processing

2.1 *Processing Limitations.* Vendor will only Process Personal Data in accordance with (i) Company's written instructions as set forth in, or pursuant to, the Services Agreement and (ii) Annex I to the SCCs, if applicable. Vendor will not use or otherwise Process Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes including Selling, or (c) any other purpose. If applicable law requires Vendor (or, for avoidance of doubt, any Subprocessor) to conduct Processing that is or could be construed as inconsistent with Company's instructions, Vendor will promptly notify Company of such inconsistency prior to commencing (or continuing) the Processing, unless notification is prohibited by law.

2.2 *Role of the Parties.* Company and Vendor agree that Company is the Controller of Personal Data and Vendor is the Processor. Vendor agrees that the Agreements (including any applicable updates), are Company's complete documented instructions to Vendor for the Processing of Personal Data.

3. Compliance with Applicable Law

Vendor will comply with laws and regulations applicable to its performance under the Service Agreement, including Data Protection Laws. This DPA is not meant to reduce the level of protections applicable to each Data Subject. In the event of any conflict or inconsistency between the DPA terms and any other terms in the Services Agreements, the DPA terms shall prevail. As required by clause 5 of the SCCs (if applicable), the SCCs prevail over any other term of this DPA and terms of the Services Agreement.

4. Subprocessors

4.1 *Appointment of Subprocessors.* Vendor may engage Subprocessors, including its Affiliates to provide services on its behalf. When engaging a Subprocessor, Vendor will ensure via a written agreement that (i) the Subprocessor may access and use Personal Data only to deliver the services Vendor has retained them to provide and is prohibited from using Personal Data for any other purpose and (ii) that Subprocessor provides for, in substance, the same data protection obligations as those binding Vendor under this DPA and (if applicable) the SCCs. Vendor agrees to oversee Subprocessors to ensure these contractual obligations are met.

If Vendor engages new Subprocessors, Vendor will give Company notice of any new Subprocessor (in accordance with clause 9(a) of the SCCs if applicable). If Company raises a commercially reasonable objection to a new Subprocessor in writing, and Vendor is unable to resolve that objection in a reasonable amount of time, then Company may terminate the affected services by providing, before the end of the relevant notice period, written notice of termination, and shall be entitled to prorata refunds for fees paid for the applicable terminated services.

Where the SCCs apply: (i) the Parties agree to use "Option 2" in clause 9 and (ii) Vendor warrants and represent that it will agree a third-party beneficiary clause with its Subprocessor(s) whereby, in the event that Vendor has factually disappeared, ceased to exist in law or has become insolvent, Company and/or its Affiliates acting as data exporter(s), have the right to terminate the Subprocessor contract and to instruct the Subprocessor to erase or return the Personal Data.

4.2 *Liability.* Vendor is responsible for its Subprocessors compliance with Vendor's obligations as outlined in the DPA and Vendor shall remain fully liable for Subprocessors' acts or omissions that result in a breach of the DPA.

5. Security

5.1 *Security Measures.* Vendor will implement and maintain appropriate technical and organizational security measures including, as appropriate: (i) encryption and pseudonymisation; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of those measures. If applicable, Vendor represents and warrants it has implemented the security measures described in the attached Annex II to the SCCs to protect Personal Data.

5.2 *Access to Personal Data and Confidentiality.* Vendor will ensure that Personal Data is only available to those who have a legitimate business need to access the Personal Data, who are bound by legally enforceable confidentiality obligations, and who will only Process Personal Data in accordance with Company's instructions. Vendor shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to Personal Data in accordance with applicable Data Protection Laws and industry standards.

5.3 *Personal Data Breach Response and Notification.* If Vendor becomes aware of a Personal Data Breach affecting Personal Data while Processed by Vendor, Vendor will promptly and within forty-eight (48) hours (i) notify Company of the Personal Data Breach ; (ii) investigate the Personal Data Breach and provide Company with detailed information about the Personal Data Breach; and (iii) take reasonable steps to mitigate effects and to minimize any damage resulting from the Personal Data Breach. Notification(s) of Personal Data Breaches must be sent to Company's point of contact by email at: kiicompeth@kochind.com. If according to the Company's assessment, a Personal Data Breach affecting Personal Data should be disclosed or reported to a third party, including Data Subjects, Supervisory Authorities or governmental authorities, Vendor will fully cooperate with and assist Company in such reporting or disclosure.

6. Audits/Inspections

Vendor will conduct audits of its security controls applied to processing Personal Data (and, if applicable, of the Processing activities covered by the SCCs), as follows:

- Each audit will be performed according to the rules of the accreditation body for each applicable control standard or framework.
- Each audit will be performed by qualified, independent, third-party security auditors at Vendor's selection and expense.

Each audit will result in the generation of an audit report ("Vendor Data Protection Audit Report"), which Vendor will make available upon request. The Vendor Data Protection Audit Report will be Vendor's Confidential Information. If Company requests, Vendor will provide Company with each Vendor Data Protection Audit Report. The Vendor Data Protection Audit Report will be subject to non-disclosure and distribution limitations of Vendor and the auditor.

To the extent Company's audit requirements under the SCCs or Data Protection Laws cannot reasonably be satisfied through the Vendor Data Protection Audit Reports, any other audit reports or other information Vendor makes generally available to Company, Vendor will promptly respond to Company's additional audit instructions.

Before the commencement of an audit, Company and Vendor will mutually agree upon the scope, timing, duration, control and evidence requirements. Company agrees that the audit will be conducted without unreasonably interfering with Vendor's (or Vendor's Subprocessor's) business activities, during regular business hours with reasonable advance notice, and subject to Vendor's (or the applicable Subprocessor's) security policies and confidentiality procedures. Where on site audits of physical data centers are not permitted, Company will work with Vendor (and Subprocessor if applicable) to reach a mutually agreeable resolution sufficient to provide information necessary for Company to comply with the applicable Data Protection Laws.

7. Vendor's Cooperation Obligation

7.1 *Cooperation*. Vendor will provide assistance to Company to allow Company to comply with its own obligations under Data Protection Laws with respect to Personal Data. Such assistance may include, without limitation, (i) responding to Data Subjects' requests to exercise their rights under Data Protection Laws; (ii) assistance with Company's performance of a data protection impact assessment and, if necessary, prior consultation with the competent supervisory authority, with respect to the Processing of Personal Data under this DPA; and (iii) responding to requests or investigations of Company by a Supervisory Authority, with respect to the Processing of Company's Personal Data under the Services Agreement.

7.2 *Third-Party Access Requests and Complaints; Data Subject Requests.* Vendor will not disclose or provide access to Personal Data except: (i) as Company directs, (ii) as described in this DPA; or (iii) as required by law, and in any event in accordance with the relevant clauses of the SCCs (where applicable). In connection with a product or service for which Company is the Controller Vendor will promptly notify Company within forty-eight (48) hours of any request or complaint from a Supervisory Authority, public authority, Data Subject or other third party relating to Personal Data or Company's obligations under Data Protection Laws unless prohibited by law. Vendor will attempt to redirect the third party to request the Personal Data directly from Company and will provide Company with a copy of the request unless legally prohibited from doing so. If unable to redirect the request, Vendor will reject it unless required by law to comply, exercising any challenges as may be applicable to the request before responding (i.e. overbroad). If applicable, Vendor will act in accordance with clauses 14 and 15 of the SCCs in handling requests.

Vendor will make available to Company in a manner consistent with the functionality of the products or services, the ability to fulfill Data Subject requests to exercise their rights under Data Protection Laws. Vendor shall comply with requests by Company to assist with Company's response to such a Data Subject request.

8. Data Retention, Return and Deletion

8.1 *Retention.* Vendor will not retain Personal Data any longer than is reasonably necessary to accomplish the intended purposes for which the Personal Data was Processed pursuant to the Service Agreement.

8.2 *Return and Deletion.* When Personal Data is no longer necessary for the purposes set forth in the applicable Services Agreement or promptly upon the expiration or termination of the Services Agreement, whichever is earlier, or at an earlier time as Company requests in writing, Vendor will (i) return to Company, in the format and on the media requested by Company, all the Personal Data; and (ii) destroy all the Personal Data in Vendor's possession or control. The foregoing obligations will also apply to Personal Data held by Subprocessors. Vendor will provide a certification of destruction and a detailed report summarizing the sanitized or destroyed items if requested. If applicable law does not permit Vendor to comply with the return or destruction of Personal Data, Vendor agrees such retained Personal Data shall remain subject to the terms of this DPA and the SCCs and it shall return or destroy such Personal Data when permitted by applicable law.

9. International Data Transfers

9.1 *Transfer Mechanism.* If the services and/or products provided by Vendor under the Services Agreement involve an international transfer of Personal Data between the Parties such transfer shall be in compliance with applicable Data Protection Laws. If the Personal Data transferred is governed by the GDPR, such transfer shall only occur subject to the conditions set out in section 9.2 and 9.3 below.

9.2 *SCCs.* Depending on the circumstances of the transfer of Personal Data, the Parties agree:

> to enter into the SCCs as set out in Attachment 1, for transfers of Personal Data from Company or its Affiliates established in the EEA or Switzerland, as a data controller, to Vendor established in a country outside the EEA, as a data processor as set out in Module II of the European Commission decision 2021/914, dated 4 June 2021 ("Controller to Processor SCCs" or "Module II"). The Controller to Processor SCCs will only apply to Personal Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for Personal Data. Personal Data that Vendor processes on Company's behalf may only be disclosed to a third party located outside the EEA in accordance with clause 8.8 of the Controller to Processor SCCs.

9.3 *International Transfer Assessments.* In cases where Personal Data is being transferred outside the EEA, Vendor represents it is aware of the requirement for a data transfer impact assessment. Vendor represents it has reviewed and analyzed the ruling of the Court of Justice for the European Union dated July 16, 2020 ("**Schrems II ruling**"), clause 14 of the SCCs, and the European Data Protection Board recommendations on supplementary measures for data transfers. After taking into account all relevant circumstances of the transfer, legislation and practices that potentially may apply to Vendor, transferred data, and Vendor's supply chain, Vendor represents that it has no reason to believe that Vendor or its Subprocessors will be prevented from complying with the SCCs.

10. Indemnification by Vendor; Liability

Vendor will defend, indemnify and hold Company, its Affiliates and their respective officers, directors, employees, agents, customers and representatives (collectively, the "**Company Indemnified Parties**") harmless from and against any liability, damages, costs, and expenses, including without limitation reasonable attorneys' fees, fines and penalties or investigative costs arising from or relating to a Personal Data Breach, or Vendor's failure to comply with this DPA or the SCCs . Vendor's obligations under this section will not be subject to any exclusions or limitations on liabilities, damages, costs or expenses with respect to amounts payable to the Company Indemnified Parties by Vendor.

Monetary damages for breach of the obligations in this DPA or the SCCs are not subject to any limitation of liability provisions in the Services Agreement. In the event Vendor breaches any of its obligations under this DPA, Company will have the right to immediately suspend Vendor's continued processing of any Personal Data, and subject to a thirty (30) day cure period, terminate the Agreement thereafter if the issue remains unresolved without penalty upon notice to Vendor.

11. Miscellaneous

11.1 *Changes in Data Protection Law.* Vendor will amend this DPA or enter into any further agreement reasonably requested by Company for purposes of compliance with Data Protection Laws.

11.2 *Counterparts/Electronic Signature.* This DPA may be executed in counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument. This DPA or any counterpart may be exchanged electronically or stored electronically as a photocopy (such as in .pdf format). The Parties agree such electronically exchanged or stored copies will be enforceable as original documents. The Parties hereby consent to the use of electronic and/or digital signatures for the execution of this DPA and further agree the use of electronic and/or digital signatures will be binding, enforceable and admissible into evidence in any dispute regarding this DPA.

Signing the DPA, the SCCs (if applicable), and the Annex 1 of the SCCs (if applicable) on behalf of Company (data exporter):

Koch Business Solutions, LP

Name

Chris Meitler

Signature

Chris Meitler

Title

Director, Global Privacy

Date

February 15, 2022

Signing the DPA, the SCCs (if applicable), and the Annex 1 of the SCCs (if applicable) on behalf of Vendor (data importer):

Vendor Name

Name

Signature

Title

Date

Attachment 1 – The Standard Contractual Clauses

Execution of the DPA by Vendor includes execution of this Attachment 1, which is countersigned by Company.

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 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.

[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, 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 2021/915.

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

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

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

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

Clause 4
Interpretation

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

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

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

Clause 5
Hierarchy

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

Clause 6
Description of the transfer(s)

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

Clause 7 – Optional
Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

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

MODULE TWO: Transfer controller to processor

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable

to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

MODULE THREE: Transfer processor to processor

8.1 Instructions

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

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

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

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

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[3].

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

[3] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article29(4) of Regulation (EU) 2018/1725.

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of theEuropean Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

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

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

Clause 9
Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 days in advance, or other reasonable time period based on the service licensed by the data exporter, 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.[5] 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 fulfill its obligations under that contract.

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

MODULE THREE: Transfer processor to processor

(a) GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub- processors at least 14 days in advance, or other reasonable time period based on the service licensed by the data exporter, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

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

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

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

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

Clause 10
Data subject rights

MODULE TWO: Transfer controller to processor

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

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

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

MODULE THREE: Transfer processor to processor

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

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

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

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 TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

a. 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;

b. 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 TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

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

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

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

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

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

Clause 13
Supervision

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

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

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

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

Clause 14
Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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[7];

(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[7];

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

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

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

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

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

Clause 15

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

[7] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account 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.

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

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

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

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

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

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

15.2 Review of legality and data minimization

(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 [for Module Three: and the controller] of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Option 2: 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 The Netherlands.

Clause 18
Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

(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.

APPENDIX

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

- Data exporter(s)/Controller:

Company is the data exporter/controller and user of services rendered by, and/or products provided under the DPA and Agreement.

Koch Business Solutions, LP

Address: 4111 E. 37th St. N Wichita, KS 67220

Contact: Global Data Privacy Officer; privacy@kochind.com

Name of DPO and/or Representative in the EU: Koch Business Solutions –Europe S.à r.l.

- Data importer(s)/Processor:

Vendor is the data importer/Processor and provider of the services and/or products provided under the DPA and Agreement.

Vendor Name: _____

Address: _____

Contact person's name, position and contact details: _____

MODULE THREE: Transfer processor to processor

- Data exporter(s)/:

Company is the data exporter/processor and user of services rendered by, and/or products provided under the DPA and Agreement.

Company Name:

Address:

Contact:

Name of DPO and/or Representative in the EU:

- Data importer(s)/Subprocessor:

Vendor is the data importer/Subprocessor and provider of the services and/or products provided under the DPA and Agreement.

Vendor Name:

Address:

Contact person's name, position and contact details:

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Categories of Data Subjects Whose Personal Data is Transferred:

Data subjects include the data exporter's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by data importer. Vendor acknowledges that, depending on Company's use of the product and or services, Company may elect to include personal data from any of the following types of data subjects in the Personal Data:

- Employees, contractors and temporary workers (current, former, prospective) of data exporter;
- Dependents of the above;
- Data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users (e.g., customers, clients, patients, visitors, etc.) and other data subjects that are users of data exporter's services;
- Partners, stakeholders or individuals who collaborate, communicate or otherwise interact with employees of the data exporter and/or use communication tools such as apps and websites provided by the data exporter;
- Minors; or
- Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Categories of Personal Data Transferred:

The Personal Data transferred that is included in email, documents and other data in an electronic form in the context of the products or services. Vendor acknowledges that, depending on Company's use of the products or services, Company may elect to include Personal Data from any of the following categories in the Personal Data:

- Basic personal data (for example place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone, telephone number, first name, last name, initials, email address, gender, date of birth), including personal data about family members and children;
- Contact information (for example addresses, email, telephone numbers, and emergency contact details);
- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
- Authentication data (for example username and password);
- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, payment behavior, and creditworthiness);

- Commercial information (for example history of purchases, special offers, and payment history);
- Biometric information (for example DNA and fingerprints);
- Location data (for example, Cell ID, geo-location network data, location data derived from use of Wi-Fi access points);
- Photos, video, and audio;
- Device identification (for example IMEI-number, SIM card number, MAC address);
- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, and benefits);
- Education data (for example education history, current education, and grades and results);
- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, and residency or work permit information);
- Data processed for the performance of a task carried out in the public interest or in the exercise of an official authority; or
- Any other personal data identified in Article 4 of the GDPR.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to 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.

- Special categories of data as set forth in Article 9 of the GDPR if applicable to the products or services. Technical and Organizational Security Measures in Annex II are applied to all Personal Data regardless of sensitivity.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

- The duration of data processing shall be so long as Vendor processes Personal Data for the term designated under the applicable Agreement between data exporter and the Vendor to which these Standard Contractual Clauses are annexed ("Company"). The objective of the data processing is the performance of products or services.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Nature of the processing

- For products or services, data importer will only act upon data exporter's instructions as conveyed by data exporter.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Purpose(s) of the data transfer and further processing

- The purpose of processing Personal Data is described in this DPA.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

- Upon expiration or termination of data exporter's use of products or services, Company may extract Personal Data and data importer will delete Personal Data, each in accordance with the DPA terms applicable to the Agreements.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

- In accordance with the DPA, the data importer may leverage subprocessors or hire other companies to provide limited services on data importer's behalf. Any such subprocessors or subcontractors will be permitted to obtain Personal Data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Personal Data for any other purpose.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

If the data exporter is established in an EU Member State, then that Member State's supervisory authority will be responsible for ensuring compliance by the data exporter with GDPR as regards the data transfer and will act as competent supervisory authority in the context of this DPA.

If the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR (i.e., Article 3(2) GDPR) and has appointed a representative in the EU (i.e., Article 27(1) GDPR), then the supervisory authority of the Member State in which the representative is established will act as competent supervisory authority in the context of this DPA.

If the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR without however having to appoint a representative in the EU, then the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under the Controller to Processor SCCs in relation to the offering of goods or services to them, or whose behavior is monitored, are located, will act as competent supervisory authority. In the context of this DPA, the competent supervisory authority is the Netherlands.

ANNEX II

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Vendor has implemented the following administrative, physical, technical and organizational security measures, at a minimum, to protect all Personal Data Processed under the DPA:
Use box to insert a link to additional measures.

Subject Matter	**Measures**
Organization of Information Security	Vendor has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. Vendor personnel with access to Personal Data are subject to confidentiality obligations. Vendor personnel receive data security training at least annually.
Operations	Vendor maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel. At least weekly, Vendor creates backup copies of production data to enable data recovery. Vendor stores backup copies of data in a different location from where the production data is located. Vendor has anti-malware controls designed to help avoid malicious software gaining unauthorized access to Personal Data, including malicious software originating from public networks. Vendor encrypts, or enables Company to encrypt, Personal Data that is transmitted over public networks.
Asset Management	Vendor classifies Personal Data to help identify it and to allow for access to it to be appropriately restricted.
Physical and Environmental Security	Vendor uses industry standard processes to delete Personal Data when it is no longer needed. Vendor uses industry standard systems to protect against loss of data due to power supply failure or line interference.
Access Control	Vendor maintains a record of security privileges of individuals having access to Personal Data. Vendor maintains and updates a record of personnel authorized to access Vendor systems that contain Personal Data.

Subject Matter	Measures
	Vendor identifies personnel who may grant, alter or cancel authorized access to data and resources. Technical support personnel are only permitted to have access to Personal Data when needed. Vendor restricts access to Personal Data to only those individuals who require such access to perform their job function. Vendor instructs Vendor personnel to disable administrative sessions when leaving premises Vendor controls or when computers are otherwise left unattended. Vendor uses industry standard practices to identify and authenticate users who attempt to access information systems. Where authentication mechanisms are based on passwords, Vendor requires that the passwords are changed regularly. Where authentication mechanisms are based on passwords, Vendor requires the password to be at least eight characters long. Vendor maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. Vendor uses industry standard password protection practices. Vendor has controls designed to avoid individuals assuming access rights they have not been assigned to gain access to Personal Data they are not authorized to access.
Security Incident Management	Vendor maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, to whom the breach was reported, and the procedure for recovering data. For each security breach that is a Personal Data Breach, notification by Vendor will be made without undue delay and, in any event, within 48 hours. Vendor tracks, or enables Company to track, disclosures of Personal Data, including what data has been disclosed and to whom.
Business Continuity Planning	Vendor maintains emergency and contingency plans for the facilities in which Vendor information systems that process Personal Data are located. Vendor's procedures for recovering data are designed to attempt to reconstruct Personal Data in its original or last-replicated state from before the time it was lost or destroyed. Vendor reviews data recovery procedures at least annually.

2. **Data Subject Access Requests**

As required by Clause 10(b) Vendor will handle data subject requests in compliance with Section 7 of the DPA.

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

The Parties agree to use "Option 2" in clause 9(a) of the SCCs (i.e., Company's general written authorization for the engagement of Vendor's Subprocessors from an agreed list).

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

1. **Name:**
   Address:
   Contact person's name, position and contact details:

   Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized):

2. **Name**
   Address:
   Contact person's name, position and contact details:

   Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized):

3. **Name:**
   Address:
   Contact person's name, position and contact details:

   Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized):

4. **Name:**
   Address:
   Contact person's name, position and contact details:

   Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized):

5. **Name:**
   Address:
   Contact person's name, position and contact details:

   Description of processing (including a clear delimitation of responsibilities in case several subprocessors are authorized):