Data Protection Agreement

This Data Protection Agreement ("**Agreement**") is made by and between:

A. **[Entity Name] [and its affiliates, subsidiaries, and/or operating companies] ([collectively] "Company A"), having a place of business at [Address of principle place of business]; and**

B. **Teletrac Navman (UK) Ltd.,** company organized under the laws of The United Kingdom and having its principal place of business at K1 Kents Hill Business Park, Milton Keynes, MK7 6BZ, United Kingdom ("**Company B**"), (each a "**Party**"**,** together, "**the Parties**"), as of the date of the last signature thereof below.

IT IS AGREED:

1. Data processing roles

In relation to the data processing activities to which this Agreement applies, the Parties will be performing the following roles:

Party	**Data processing role**
Company A	☐ **Independent Controller/Business** ☒ **Processor or Subprocessor on behalf of Company B** ☐ **Processor or Subprocessor on behalf of a third party Controller**
Company B	☒ **Independent Controller/Business** ☐ **Processor or Subprocessor on behalf of Company A** ☐ **Processor or Subprocessor on behalf of a third party Controller**

2. Definitions

For the purpose of this Agreement, the following words and phrases shall have the following meaning unless the context otherwise requires:
"**Aim**" has the meaning given to it in Clause 15.a.

"**Business**" or "**Controller**" means an entity that determines the purposes and means of processing Personal Data or Personal Information.

"**Contract**" means the [**Commercial Agreement Name**] between Company A and Company B dated [**Date of Commercial Agreement**].

"**Controller Personal Information**" has the meaning given to it in Clause 15.a below.

"**Data**" means the Processor Personal Information and/or Controller Personal Information, as the content requires.

"**Data Exporter**" has the meaning set out in the EU Standard Contractual Clauses.

"**Data Importer**" has the meaning set out in the EU Standard Contractual Clauses.

"**Data Discloser**" has the meaning given to it in Clause 3.b.

"**Data Receiver**" has the meaning given to it in Clause 3.b.

"**Data Protection Laws**" means all laws, regulations, legislative and regulatory requirements, and legally binding rules, codes and guidelines applicable to the Processing, privacy, integrity, security, confidentiality and use of the Data, Company A and/or Company B including, without limitation and where applicable (i) the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") together with national implementing laws in any Member State of the EEA; (ii) the GDPR as it is incorporated into the laws of the United Kingdom; (iii) the Data Protection Act of 2018 of the United Kingdom; (iv) the Swiss DPA; (v) United States regulation, including, but not limited to the California Consumer Privacy Act ("**CCPA**") and the California Privacy Rights Act ("**CPRA**") and the Section 5(a) of the Federal Trade Commission Act (15 U.S.C. § 45) (vi) the Lei Geral de Proteção de Dados; (vii) the Protection of Personal Information Act 2013 of South Africa; and any legislation that supplements, amends or supersedes the foregoing.

"**EU Standard Contractual Clauses**" means the clauses, approved in the European Commission Implementing Decision (EU) 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, (a copy of which can be found in Schedule 4) as amended, updated or replaced by the European Commission.

"**Party One**" has the meaning given to it in Clause 3.a.

"**Party Two**" has the meaning given to it in Clause 3.a.

"**Permitted Purpose**" means the purpose(s) for which the Controller Personal Information may be Processed as set out in Part B of Schedule 1.

"**Processor**" means a natural or legal person, public authority, agency or other body engaged by a Controller to Process Personal Data and/or Personal Information, and includes a Service Provider as defined under the CCPA and CPRA.

"**Processor Personal Information**" means all Personal Information and Personal Data, in whatever form or medium, which is Processed by Party Two for and on behalf of Party One and/or the Third Party Controller (as applicable) whether or not such Personal Information and Personal Data is supplied to (by transfer or access), and/or produced collected or generated by or on behalf of Party Two in connection with the Contract or this Agreement, including as set out in Part A of Schedule 1.

"**Services**" shall have the meaning given to it under the Contract or where this term is not defined means the services described in the Contract and agreed between Company A and Company B from time to time.

"**Subprocessor**" means a natural or legal person, public authority, agency or other body engaged by another Processor to Process Personal Data and/or Personal Information.

"**Supervisory Authority**" means any competent data protection or privacy authority in any jurisdiction in which Company A, Company B or the Third Party Controller (if applicable) is established, in which the Services are delivered or received, or in which the Processor Personal Information is Processed.

"**Swiss DPA**" shall mean the Swiss Data Protection Act of 19 June 1992 or, as soon as in force, the Swiss Data Protection Act adopted by the Swiss parliament on 25 September 2020, or, where applicable, the provisions of the relevant Cantonal data protection laws.

"**Third Party Controller**" has the meaning given to it in Clause 3.a.ii.

"**UK Addendum**" means the Addendum in Schedule 5.

"**Data Subject**", "**Personal Data**", "**Service Provider**", "**Personal Information**", "**Personal Data Breach**", "**Processing**", "**Sensitive Personal Information**" (or "**Special Categories of Personal Data**"), "**Sell**", and "**Share**" all have the meanings given to those terms in applicable Data Protection Laws (and related terms, such as "Process", have corresponding meanings). If any of these terms is not defined under applicable Data Protection Laws, the term shall have the meaning given to it under the GDPR or CCPA or CPRA.

3. Application of this Agreement

a. If either of the Parties are listed as a Processor or Subprocessor in Clause 1, the terms of Part A and Part C shall apply, such that:

   i. If one Party is listed as an Independent Controller/Business and the other Party is listed as a Processor or Subprocessor on behalf of that Party, the Controller/Business party is "**Party One**" and the Processor or Subprocessor party is "**Party Two"**; or

   ii. If one Party is listed as a Processor or Subprocessor on behalf of a third party Controller ("**Third Party Controller**") and the other Party is listed as a Processor or Subprocessor on behalf of that Party, the Third-Pary Controller party is "**Party One**" and the Processor or Subprocess party is "**Party Two**".

b. If both Parties are listed as an **Independent** Controller/Business in Clause 1, the terms of Part B and Part C shall apply such that:

   i. the Party or Parties sharing the Controller Personal Information are "**Data Disclosers**" and each a "**Data Discloser**"; and

   ii. the Party or Parties receiving the Controller Personal Information are "**Data Receivers**" and each a "**Data Receiver**".

Part A: Processor terms

4. Appointment and role of the Parties

a. Party One appoints Party Two to Process the Processor Personal Information on its behalf (or on behalf of the Third Party Controller, as applicable) as is necessary for the provision of the Services and performance of the Contract.

b. Where, in Clause 1 Party One is a Processor or Subprocessor on behalf of a Third Party Controller, Party One warrants that it has obtained prior authorization and all applicable consents and licenses from the Third Party Controller to appoint Party Two as a Processor.

5. Details of the Processing

a. Processing of the Processor Personal Information by Party Two under this Agreement shall be for the: (a) subject-matter; (b) duration; (c) nature and purpose; and (d) categories of Data Subjects, set out in Part A of Schedule 1.

b. Other than as set out herein, the Processor shall not Process the Processor Personal Information for any other incompatible purpose.

6. Complying with Data Protection Law

a. Party One shall have the right to take reasonable and appropriate steps to help ensure that Party Two uses the Processor Personal Information in a manner consistent with Party One's and the Third Party Controller's (if applicable) obligations under the Data Protection Laws.

b. Party One shall have the right, upon notice to Party Two, to take reasonable and appropriate steps to stop and remediate unauthorized use of the Processor Personal Information.

7. Acting on Party One 's documented instructions

a. Subject to Clause 7.b, Party Two shall Process Processor Personal Information only on the documented instructions of Party One including as set out in this Agreement and the Contract.

b. Notwithstanding Clause 7.a, Party Two also has the right to Process the Processor Personal Information:

   i. to the extent required by law, following Party Two's prior notification to Party One, except where mandatory applicable law prohibits such notification; and

   ii. if Party Two is also listed as an Independent Controller/Business in respect of any Processor Personal Information that is also Controller Personal Information.

c. Party Two shall promptly notify Party One if in Party Two's reasonable opinion any instruction from Party One infringes Data Protection Law, with such notification to include an explanation of why Party Two has formed such an opinion

d. Party Two acknowledges that it is prohibited from:

i. selling or sharing Processor Personal Information unless otherwise permitted under the Data Protection Laws or this Agreement;

ii. retaining, using, or disclosing Processor Personal Information for any purpose other than for the purpose(s) specified in Part A of Schedule 1 or as otherwise permitted under Data Protection Laws; or

iii. combining Processor Personal Information with Personal Data and/or Personal Information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the Data Subject, unless otherwise permitted under the Data Protection Laws or this Agreement.

8. Taking appropriate technical and organizational measures, including for security

a. Party Two shall implement appropriate technical and organizational measures:

i. designed to assist Party One and/or the Third Party Controller (if applicable) in responding to requests from Data Subjects to exercise their rights under Data Protection Law; and

ii. designed to ensure a level of security for the Processor Personal Information appropriate to the risk posed by the Party Two's Processing of such Processor Personal Information, to protect it from unauthorized, accidental or unlawful disclosure, or access, loss or alteration and shall include the measures set out in Schedule 2 at a minimum.

9. Data breach notification and assistance

a. Party Two shall notify Party One in writing without undue delay if it becomes aware that it has suffered a Personal Data Breach affecting the Processor Personal Information (a "**Data Breach**"), and provide Party One, as soon as reasonably practicable with the following information relating to the Data Breach:

i. the nature of the Processor Personal Information affected;

ii. the categories and number of Data Subjects concerned;

iii. the number of Processor Personal Information records concerned;

iv. measures taken to address the Data Breach; and

v. the possible consequences and adverse effect of the Data Breach.

b. Party Two, at its own cost, shall provide Party One and/or the Third Party Controller (if applicable) with all reasonable assistance in relation to Party One's and/or the Third Party Controller's (if applicable) compliance with Articles 32-34 of the GDPR or equivalent requirements of other Data Protection Laws. Party Two shall provide such assistance in a

timely manner and in accordance with any time frames set out in the Data Protection Laws.

10. Subcontracting

a. Party One hereby authorizes Party Two to engage only the third parties listed in Schedule 3 to perform Processing activities in respect of Processor Personal Information on behalf of the Party One ("**Authorized Subprocessors**"). Party Two shall notify Party One in writing in advance if it intends to replace or add to the Authorized Subprocessors and Party One shall have a right, acting reasonably, to reject to such replacement or additional subprocessor. If Party One does not notify Party Two in writing of its objection to the additional or replacement subprocessor within 20 days of being notified of such addition or replacement, Party Two may proceed with engaging the additional or replacement subprocessor to Process the Processor Personal Information. If Party One notifies Party Two of its objection in accordance with this Clause, the Parties shall work in good faith to find a resolution to the issue. If the Parties cannot reach a resolution within 30 days of Party One's objection, either Party has the right to terminate this Agreement and the Contract on 30 days' written notice to the other.

b. Party Two shall enter into a written agreement with each Authorized Subprocessor that contains obligations that are consistent with and no less onerous than those set out in this DPA.

c. Party Two shall promptly provide, on request from Party One, the relevant details of any such written agreements between Party Two and its Authorized Subprocessors.

d. Party Two shall remain fully liable to Party One for any non-compliance with the terms of this Agreement by any Authorized Subprocessor.

11. Cross Border Transfers of Processor Personal Information

a. Party Two shall not, and shall procure that any Authorized Subprocessor shall not, receive or transfer any Processor Personal Information to any country or territory outside the Processor Personal Information's country or territory of origin, without first obtaining the express written consent of Party One and ensuring that appropriate safeguards are in place to protect the Processor Personal Information, in accordance with the requirements of Data Protection Laws and subject to Clause 22. For the purposes of this Clause, the locations set out in Part A of Schedule 1 and Schedule 3 are hereby approved by Party One, subject to Clause 21.a2.

12. Deleting or returning of Processor Personal Information

a. Party Two shall promptly and in any event within thirty (30) days: (a) of termination or expiry of the Contract, for whatever reason; (b) after the end of the provision of the relevant Services related to the Processing; or (c) if earlier, as soon as Processing by Party Two of any Processor Personal Information is no longer required for Party Two's performance of its obligations under the Contract, cease all use of such Processor Personal Information and shall either securely destroy or return to Party One(at Party One's direction) all such Processor Personal Information.

13. Records and audit

a. Party Two shall maintain complete, accurate and up to date written records of all Processing activities carried out on the Processor Personal Information and shall make available to Party One, on written request, such records and any other information as is reasonably required by Party One to demonstrate compliance by Party Two with its obligations under this Agreement and applicable Data Protection Laws.

b. Party One has the right to conduct, by itself or by an independent third party acting under Party One's direction that is not a competitor of Party Two, at Party One's cost, an inspection, including an audit, of Party Two's data security and privacy procedures relating to the Processing of Processor Personal Information and compliance with this Agreement. Such inspection or audit may only occur once per calendar year, during Party Two's normal business hours following receipt by Party Two of 30 days prior written notice of such inspection and audit. For the avoidance of doubt, such inspection or audit shall not cause unreasonable disruption to Party Two's business and shall not include an inspection or audit which compromises Personal Information, Personal Data or confidential information Processed by Party Two on behalf of third parties.

14. Informing Party One of complaints, enquiries and third party access requests

a. To the extent not prohibited by applicable law, Party Two shall inform Party One without undue delay of any enquiry, complaint, notice or other communication it receives from any Supervisory Authority or any Data Subject in connection with Party Two's Processing of the Processor Personal Information. Party Two shall provide all reasonable assistance to Party One to enable Party One to respond to such enquiries, complaints, notices or other communications and to comply with Data Protection Laws. For the avoidance of doubt, Party Two shall not respond to any such enquiry, complaint, notice or other communication without the prior written consent of Party One unless it is required to do so under applicable law.

b. Subject to Clause g, Party Two shall notify Party One without undue delay if it:

    i. receives a request from a public authority, including judicial authorities, for the disclosure of Processor Personal Information ("**Public Authority Request**"); such notification shall include, but is not limited to, information about the Processor Personal Information requested, the requesting authority, the legal basis for the request and Party Two's proposed response; or

    ii. becomes aware of any direct access by public authorities to Processor Personal Information; such notification shall include all information available to Party Two about such access, including but not limited to, the timing and method of the access, the Processor Personal Information accessed, the reason for the access and all communications with the public authority about such access (if any).

c. Party Two shall review the legality of the Public Authority Request, in particular whether it is within the powers granted to the requesting public authority, and if, after careful assessment by or on behalf of Party Two:

i. Party Two concludes that there are reasonable grounds to consider that the Public Authority Request is unlawful, Party Two must challenge the request; or

ii. Party Two concludes that the Public Authority Request is lawful, Party Two must pursue possible grounds of appeal.

d. When challenging a Public Authority Request, Party Two shall use best efforts to seek interim measures with a view to suspending the effects of the Public Authority Request until the competent judicial authority has decided on the merits of the Public Authority Request. Party Two shall not disclose the Processor Personal Information requested until required to do so under the applicable legal procedural rules.

e. Party Two shall document the assessment set out in Clause c and any challenge to or appeal against the Public Authority Request and, to the extent not prohibited by law, make such documentation available to Party One on request.

f. Party Two shall provide the minimum amount of Processor Personal Information permissible when responding to a Public Authority Request, based on a reasonable interpretation of the request.

g. If Party Two is legally prohibited from notifying Party One in accordance with Clause b, Party Two shall use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible about the notifiable matter, as soon as possible, to Party One. Party Two shall document its best efforts in order to be able to demonstrate them on request from Party One.

Part B: Controller terms

15. Scope of Processing.

a. The aim of sharing the Controller Personal Information is to facilitate the provision and receiving of services under the **Contract** (the "**Aim**").

b. The Parties acknowledge that in connection with the Aim, the Data Receiver may receive from the Data Discloser Personal Data and/or Personal Information about or related to certain Data Subjects as more particularly described in Part B of Schedule 1 (collectively "**Controller Personal Information**").

c. The Data Discloser warrants that the Controller Personal Information it provides to the Data Receiver will, to the best of its knowledge, be accurate and agrees to notify the Data Receiver promptly, after being made aware, of any inaccuracies in the Controller Personal Information.

d. The Data Discloser undertakes not to provide the Data Receiver with any Personal Data and/or Personal Information that is not described in Schedule 1.

e. The Data Receiver:
   i. may only process the Controller Personal Information for the Permitted Purpose; and
   ii. shall not Process the Controller Personal Information for any purpose that is

incompatible with the Permitted Purpose.

16. Relationship of the Parties.

a. The Parties acknowledge that each Party shall process the Controller Personal Information as a separate and independent Controller (or Business, where applicable), for its own purposes and in its own right and in the case of the Data Receiver, only for the Permitted Purpose. In no event will the Parties process the Controller Personal Information as joint Controllers (as that term is understood under the GDPR).

b. Nothing in this Agreement shall limit the Data Discloser from collecting or using the Controller Personal Information, or other Personal Data and Personal Information, that Data Discloser otherwise Processes independently of Data Receiver and the Aim.

17. Responsibilities.

a. **Transparency.** Data Discloser shall, prior to sharing any Controller Personal Information with the Data Receiver:

i. provide all necessary disclosures, information or notices to the Data Subjects to satisfy the requirements of Data Protection Laws. Without prejudice to the generality of the foregoing, such disclosure, information or notice shall, at a minimum, include the following information: (i) the type of Controller Personal Information collected, shared, sold or otherwise Processed by Data Discloser and the Permitted Purpose of Processing thereof; (ii) the categories of recipients who will have access to or receive the Controller Personal Information; including the Data Receiver; (iii) where applicable, the legitimate interests pursued by the Data Discloser in Processing the Controller Personal Information, including sharing the Controller Personal Information with the Data Receiver; and (iv) any other information the Data Discloser is required to provide to the Data Subjects under Data Protection Laws to allow it to lawfully disclose the Controller Personal Information to the Data Receiver; and

ii. make available to the Data Receiver, for the Data Receiver's review prior to its use, all such disclosures, information and notices provided to Data Subjects in accordance with clause i. The Data Receiver may terminate this Agreement without prejudice to any rights or remedies if, in the Data Receiver's sole discretion, the Data Receiver concludes that such disclosures, information and notices do not meet applicable Data Protection Laws.

b. **Lawfulness:** If the Data Discloser is relying on the Data Subject's consent to share the Controller Personal Information with the Data Receiver:

i. the Data Discloser will make available to the Data Receiver, for the Data Receiver's review and approval prior to its use, all such permissions and consents. The Data Receiver may terminate this Agreement without prejudice to any rights or remedies if, in the Data Receiver's sole discretion, the Data Receiver concludes that such permissions or consents do not meet applicable Data Protection Laws; and

ii. the Data Discloser will at all times, make available, maintain and make operational a mechanism for Data Subjects to easily withdraw such permissions

and/or consents in accordance with Data Protection Laws.

c. **Consent:** If the Data Receiver is relying on the Data Subjects' consent to Process the Controller Personal Information for some or all of the Permitted Purpose, and such consent is being obtained by the Data Discloser on the Data Receiver's behalf:

i. the Data Discloser warrants that any consent mechanism used to obtain consent from each Data Subject is clear and specific to reasonably ensure that the Data Subject understands the identity of the party or parties to which the Data Subject is consenting to use their Controller Personal Information and the purposes for which such party or parties will use that Controller Personal Information. Without prejudice to the generality of the foregoing, the Data Discloser shall ensure that all such consent mechanisms specifically name the Data Receiver and any third party instructed by the Data Receiver, and the Permitted Purpose for which the Data Receiver is Processing the Controller Personal Information in reliance on the Data Subjects' consent;

ii. the Data Discloser shall maintain a record of all such consents, including the time and date on which consent was obtained, the information presented to Data Subjects in connection with their giving consent, and details of the mechanism used to obtain consent. Data Discloser shall make the aforementioned records available to Data Receiver promptly upon written request;

iii. the Data Discloser shall notify the Data Recipient promptly of any Data Subject who withdraws their consent.; and

iv. the Data Discloser will make available to the Data Receiver, for the Data Receiver's review and approval prior to its use, all such consents mechanisms. The Data Receiver may terminate this Agreement without prejudice to any rights or remedies if, in the Data Receiver's sole discretion, the Data Receiver concludes that such consent mechanism does not meet applicable Data Protection Laws.

d. **Retention.** The Data Receiver shall not retain or process the Controller Personal Information for longer than is necessary to carry out the Permitted Purpose or to comply with any statutory or professional retention periods applicable to the Data Receiver.

18. Cooperation.

a. **Data Subjects' Rights.** Each Party shall, on request by the other Party, provide all reasonable and timely assistance (at their own expense) to enable the other Party to comply with its obligations under Data Protection Laws, specifically in order to enable the other Party to respond to: (i) any request from a Data Subject to exercise any of his or her rights under Data Protection Law in relation to the Controller Personal Information; and (ii) any other correspondence, enquiry or complaint received from a Data Subject, regulator or other third party in connection with the processing of the Controller Personal Information.

b. **Security Incidents and Data Breaches.** Each Party shall, on request by the other Party, provide all reasonable assistance in relation to the other Party's obligations under Data Protection Laws to report or notify a security incident or Personal Data Breach involving the Controller Personal Information. The Parties shall provide such assistance in a timely

manner and in accordance with any time frames set out in the Data Protection Laws (if applicable).

c. If required by Data Protection Law, if a Party suffers a security incident or Personal Data Breach affecting the Controller Personal Information, it shall notify the other Party and provide the other Party with accurate and comprehensive information about such incident or Personal Data Breach in accordance with Data Protection Law.

19. Records and audit

a. Each Party shall maintain complete, accurate and up to date written records of all Processing activities carried out on the Controller Personal Information in connection with this Agreement and shall make available to the other Party ("**Requesting Party**"), on written request, such records and any other information as is reasonably required by the Requesting Party to demonstrate the other Party's compliance with its obligations under this Agreement.

b. The Requesting Party shall have the right to terminate this Agreement without notice if it considers, acting reasonably, that the other Party is not Processing the Controller Personal Information in accordance with this Agreement.

20. Part C: General terms

21. Ensuring employee confidentiality

a. Each Party shall ensure that any person acting under its authority who may have access to, or who otherwise Process, the Data are subject to legally binding obligations of confidentiality, and at all times act in compliance with Data Protection Law, and shall ensure that such persons receive regular and appropriate training on the same.

22. Cross Border Transfers of Data

a. Subject to Clauses 22.c and 22.d (as applicable), if Data originating from the EEA, UK or Switzerland is transferred from Company A to Company B as part of this Agreement and/or the Contract, the relevant module of the EU Standard Contractual Clauses is hereby incorporated into this Agreement and shall apply to Company A as Data Exporter and Company B as Data Importer.

b. Subject to Clauses 22.c and 22.d (as applicable), if Data originating from the EEA, UK or Switzerland is transferred from Company B to Company A as part of this Agreement and/or the Contract, the relevant module of the EU Standard Contractual Clauses is hereby incorporated into this Agreement and shall apply to Company B as Data Exporter and Company A as Data Importer.

c. With respect to Data originating from Switzerland, the EU Standard Contractual shall be amended as follows: (i) references to the term "Member State" shall be substituted for the term "Switzerland" to preserve the rights of data subjects under the Swiss DPA; (ii) references to "Regulation (EU) 2016/679" or "that Regulation" will be understood as references to the Swiss DPA; (iii) the governing law will be the law of the relevant canton;

(iv) the competent authority shall be the Swiss Federal Data Protection and Information Commissioner or, where applicable, the competent Cantonal Data Protection Commissioner; and (v) the footnotes shall be removed.

d. With respect to Data originating from the UK, the EU Standard Contractual Clauses shall be amended in accordance with the UK Addendum.

23. Complying with Data Protection Law

a. Each Party shall in all cases Process the Data in compliance with and shall be individually and separately responsible for complying with, their respective obligations under the Data Protection Laws.

b. If any of the Data Protection Laws in any country to which this Agreement relates conflict, the requirements of the country that necessitates stricter or additional requirements to protect Data Subjects' privacy and Data shall be applied.

c. Neither Party shall cause the other Party, by act or omission, to be in breach of Data Protection Laws.

24. Liability; Indemnification.

a. **No Limit on Liability.** Neither Party excludes or limits its liability for: (a) fraud or fraudulent misrepresentation; (b) death or personal injury caused by its negligence; or (c) any matter for which it would be unlawful for the Party to exclude liability.

b. **Exclusion of Certain Damages**. Notwithstanding and expressly modifying or taking precedence over anything to the contrary in any other agreements between the Parties, neither Party nor its affiliates, licensors, officers, directors, agencies, employees or representatives shall be liable to the other Party or its affiliates, licensors, officers, directors, agencies, employees or representatives under or in connection with this Agreement for indirect, special, incidental, consequential, or punitive damages or penalties (including, without limitation, lost profits, lost business, business interruption, and the like), however it arises, whether for breach of contract or in tort (including negligence), even if a Party has been advised of the possibility of such damages. This Clause **Error! Reference source not found.** shall not be construed to limit the types of claims for which an indemnity is owed.

c. **Indemnity**. Company A agrees to indemnify, keep indemnified and defend at its own expense Company B for all losses, costs, claims, damages and expenses directly incurred by Company B as a result of failure by Company A to comply with any of its obligations under this Agreement and/or Data Protection Laws.

d. Except where the Parties cannot limit or exclude their liability under applicable law, each Party’s liability in the aggregate arising out of or in connection with this Agreement, whether in contract, tort (including negligence), breach of statutory duty or otherwise, is subject to the limitations and exclusions of liability in the Contract, and any reference in

the Agreement to the liability of a Party means the aggregate liability of that Party and all of its Affiliates under the Contract and the Agreement together.

25. General terms

a. This Agreement constitutes the entire agreement between the Parties and supersedes, terminates and extinguishes all previous and contemporaneous agreements, promises, assurances and understandings between them, whether written or oral, relating to its subject matter.

b. Both Parties acknowledge and understand that the Data may be subject to Data Protection Laws that require certain undertakings and/or the entering into of additional agreements, including in relation to the cross-border transfers of the Data. Both parties agree that they shall work together in good faith to enter into any alternative or additional agreements or arrangements or implement any additional measures as may be required under Data Protection Laws in relation to the Processing and/or cross-border transfer of the Data.

c. In the event of any conflict between the provisions of this Agreement, the Contract (if any) and the EU Standard Contractual Clauses, the EU Standard Contractual Clauses shall prevail, then this Agreement, then the Contract.

d. Variation or amendment of this Agreement is only valid upon the signed written agreement of both Parties.

e. Should any provision of this Agreement be invalid or unenforceable, then the remainder of this Agreement shall remain valid and in force. The invalid or unenforceable provision shall either be (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

f. Any disputes or claims (including non-contractual disputes or claims) arising out of or in connection with this Agreement shall be governed by the laws set out in the Contract (if a Contract exists) otherwise they shall be governed by the law of England and Wales.

g. Any disputes or claims (including non-contractual disputes or claims) arising out of or in connection with this Agreement shall be resolved by the courts in the territory set out in the Contract (if a Contract exists) otherwise the courts of England shall have jurisdiction.

IN WITNESS WHEREOF, intending to be legally bound, each of the Parties have caused this Agreement to be executed and effective as of the last date set forth below.

[COMPANY A NAME] **[COMPANY B NAME]**

Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Schedule 1

Part A: Description of processing for Processor Personal Information

1. Subject matter and duration of the Processing of Processor Personal Information

The subject matter of the Processing of the Processor Personal Information is the provision of the Services to Party One. Processor Personal Information will be Processed for the duration of the Contract between the parties, subject to Clause 12 of this Agreement.

2. Nature and purpose of the Processing of Processor Personal Information

Party Two shall host, maintain and otherwise process Processor Personal Information only in connection with the provision of Services pursuant to the terms of the Contract and this Agreement.

3. Types of Processor Personal Information Processed

Personal Information and Personal Data relating the Data Subjects listed below, input by (or at the direction of) Party One or by Data Subjects into Party Two's system or that Party Two otherwise Processes on Party One's behalf in connection with providing the Services pursuant to the terms of the Contract and this Agreement, including:

☒ Name

☒ Contact details

☐ IP address

☐ Cookie ID

☐ Web browsing information

☐ Other: (please specify)……

4. Categories of Data SubjectS to whom the Processor Personal Information Relates

☒ Party One's (or the Third Party Controller's) employees, contractors and other personnel

☐ Party One's (or the Third Party Controller's) end users and/or customers

☐ Party One's Prospective customers

☐ Other: *(please specify)*…….

5. Countries in which the Processor will Process the Controller Personal Information

[To be completed]

Part B: Description of processing for Controller Personal Information

1. **Data Subjects**:

☒ Data Discloser's employees, contractors or other personnel

☐ Data Discloser's end users and/or customers

☐ Prospective customers for the Data Receiver

☐ Other: *(please specify)*……

2. **Types of Controller Personal Information**:

☒ Name

☒ Contact details

☐ IP address

☐ Cookie ID

☐ Web browsing information

☐ Other: (please specify)……

3. **Permitted Purpose(s):**

☒ As contemplated by the Contract

☐ Using the Controller Personal Information for sales, marketing and direct marketing purposes, such as sending marketing communications to the Data Subjects

☐ Disclosing the Controller Personal Information to Data Receiver's third party partners or affiliates for their sales, marketing and direct marketing purposes, such as sending marketing communications to Data Subjects

☐ Other: (please specify)……

Contact points for data protection enquiries

Company A	**Company B**
[To complete]	Privacy and Data Counsels
	privacy@vontier.com

Schedule 2

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

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

Technical Measures

Technical Measures to Ensure Security of Processing	
1. Inventory and Control of Hardware Assets	Actively manage all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
2. Inventory and Control of Software Assets	Actively manage all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
3. Continuous Vulnerability Management	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.
4. Controlled Use of Administrative Privileges	Maintain processes and tools to track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, applications, and data.
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	Implement and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
6. Maintenance, Monitoring, and Analysis of Audit Logs	Collect, manage, and analyze audit and security logs of events that could help detect, understand, or recover from a possible attack.
7. Email and Web Browser Protections	Deploy automated controls to minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems or content.

Technical Measures to Ensure Security of Processing	
8. Malware Defenses	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.
9. Limitation and Control of Network Ports, Protocols, and Services	Manage (track, control, correct) the ongoing operational use of ports, protocols, services, and applications on networked devices in order to minimize windows of vulnerability and exposure available to attackers.
10. Data Recovery Capabilities	Maintain processes and tools to properly back up personal data with a proven methodology to ensure the confidentiality, integrity, availability, and recoverability of that data.
11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches	Implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
12. Boundary Defenses	Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on personal data.
13. Data Protection	Maintain processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the confidentiality and integrity of personal data.
14. Controlled Access Based on the Need to Know	Maintain processes and tools to track, control, prevent, and correct secure access to critical or controlled assets (e.g. information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical or controlled assets based on an approved classification.
15. Wireless Access Control	Maintain processes and tools to track, control, prevent, and correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems.
16. Account Monitoring and Control	Actively manage the life cycle of system and application accounts, their creation, use, dormancy, and deletion in order to minimize opportunities for unauthorized, inappropriate, or nefarious use.

Organizational Measure

Organizational Measures to Ensure Security of Processing	
1. Implement a Comprehensive Information Security Program	Through the implementation of a Comprehensive Information Security Program (CISP), maintain various administrative safeguards to protect personal data. These measures are designed to ensure: •security, confidentiality and integrity of personal data •protection against unauthorized access to or use of (stored) personal data in a manner that creates a substantial risk of identity theft or fraud •that employees, contractors, consultants, temporaries, and other workers who have access to personal data only process such data on instructions from the data controller.
2. Implement a Security Awareness and Training Program	For all functional roles (prioritizing those mission critical to the business, its security, and the protection of personal data), identify the specific knowledge, skills and abilities needed to support the protection and defense of personal data; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.
3. Application Software Security	Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.
4. Incident Response and Management	Protect the organization's information, including personal data, as well as its reputation, by developing and implementing an incident response infrastructure (*e.g.*, plans, defined roles, training, communications, management oversight, retainers, and insurance) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the organization's network and systems.
5. Security and Privacy Assessments, Penetration Tests, and Red Team Exercises	Test the overall strength of the organization's defense (the technology, processes, and people) by simulating the objectives and actions of an attacker; as well as, assess and validate the controls, policies, and procedures of the organization's privacy and personal data protections.
6. Physical Security and Entry Control	Require that all facilities meet the highest level of data protection standards possible, and reasonable, under the circumstances relevant to the facility and the data it contains, process, or transmits.

Schedule 3

AUTHORIZED SUBPROCESSORS – to be completed by Party two

Subprocessor name	Subprocessor registered address	Description of Processing for which Subprocessor engaged	Country in which Processor Personal Information will be stored (including any backups)

Schedule 4

EU STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.
(b) The Parties:
(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')
have agreed to these standard contractual clauses (hereinafter: 'Clauses').
(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

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

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8 – 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

(intentionally left blank)

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE ONE: Transfer controller to controller

8.1 Purpose limitation

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

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

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

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

8.2 Transparency

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

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

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

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

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

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

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

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

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

8.5 Security of processing

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

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

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

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

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of

the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

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

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

8.6 Sensitive data

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

8.7 Onward transfers

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

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

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

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

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

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

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having

informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

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

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without

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

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

8.7 Sensitive data

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

8.8 Onward transfers

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

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

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

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

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

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

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

MODULE THREE: Transfer processor to processor

8.1 Instructions

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

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

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

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

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

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

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

MODULE FOUR: Transfer processor to controller

8.1 Instructions

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

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

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

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

8.2 Security of processing

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

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

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

8.3 Documentation and compliance

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

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

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least fifteen (15) 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. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

MODULE THREE: Transfer processor to processor

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least fifteen (15) in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

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

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

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

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

Clause 10

Data subject rights

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. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.
(b) In particular, upon request by the data subject the data importer shall, free of charge:

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

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

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.
(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of

the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

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

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

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

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

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

MODULE TWO: Transfer controller to processor

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

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

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

MODULE THREE: Transfer processor to processor

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

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

nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

MODULE FOUR: Transfer processor to controller

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

Clause 11

Redress

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

MODULE ONE: Transfer controller to controller
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

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

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

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
(ii) refer the dispute to the competent courts within the meaning of Clause 18.

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

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

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

Clause 12

Liability

MODULE ONE: Transfer controller to controller
MODULE FOUR: Transfer processor to controller

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

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

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

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

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

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

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

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

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

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

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

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

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

Clause 13

Supervision

MODULE ONE: Transfer controller to controller
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

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

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

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

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

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

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

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

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

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

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for

Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

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

15.1 Notification

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

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
(ii) the data importer is in substantial or persistent breach of these Clauses; or
(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

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

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

Clause 17

Governing law

MODULE ONE: Transfer controller to controller
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third- party beneficiary rights. The Parties agree that this shall be the law of the EU Member State in which the data exporter is established.

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 the EU Member State in which the data exporter is established.

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

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

(b) The Parties agree that those shall be the courts of the EU Member State in which the data exporter is established.

(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 the EU Member State in which the data exporter is established.

ANNEX I

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor
MODULE FOUR: Transfer processor to controller

Data exporter(s): The party identified in Clause 22.a or 22.b of the Agreement.

Data importer(s): The party identified in Clause 22.a or 22.b of the Agreement.

B. DESCRIPTION OF TRANSFER
MODULE ONE: Transfer controller to controller

Categories of data subjects whose personal data is transferred
The categories of Data Subjects described in Part B of Schedule 1 of the Agreement to which these Clauses are attached.

Categories of personal data transferred
The categories of Controller Personal Information described in Part B of Schedule 1 of the Agreement to which these Clauses are attached.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
The categories of Controller Personal Information described in Part B of Schedule 1 of the Agreement to which these Clauses are attached.

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

Nature and purpose of the processing
The Permitted Purpose described in Part B of Schedule 1 of the Agreement to which these Clauses are attached.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
The duration specified in Clause 8.5 of these Clauses.

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor
MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred

The categories of Data Subjects described in Part A of Schedule 1 of the Agreement to which these Clauses are attached.

Categories of personal data transferred
The categories of Processor Personal Information described in Part A of Schedule 1 of the Agreement to which these Clauses are attached.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
The categories of Processor Personal Information described in Part A of Schedule 1 of the Agreement to which these Clauses are attached.

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

Nature of the processing
The nature described in Part A of Schedule 1 of the Agreement to which these Clauses are attached.

Purpose(s) of the data transfer and further processing
The purpose described in Part A of Schedule 1 of the Agreement to which these Clauses are attached.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
The duration specified in Clause 8.5 of these Clauses and in Clause 12 of the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
As per the sections above.

C. COMPETENT SUPERVISORY AUTHORITY
MODULE ONE: Transfer controller to controller
MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor
Identify the competent supervisory authority/ies in accordance with Clause 13
The competent supervisory authority shall be the authority of the EU Member State in which the Data Exporter is established.

ANNEX II

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

See Schedule 2 to the Agreement to which these Clauses are attached.

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor
MODULE THREE: Transfer processor to processor

See Schedule 3 to the Agreement to which these Clauses are attached.

Schedule 5:

UK ADDENDUM

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

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

Part 1: Tables

Table 1: Parties

Start date	The Effective Date as set out in the Agreement to which this Addendum is attached or, if no effective date is set out, the date of last signature of the Parties.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	As set out at the top of the Agreement	As set out at the top of the Agreement

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	Means the EU Standard Contractual Clauses as defined in the Agreement to which this Addendum is attached.

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties:	As set out at the top of the Agreement to which this Addendum is attached.
Annex 1B: Description of Transfer:	Schedule 1 of the Agreement to which this Addendum is attached
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	Schedule 2 of the Agreement to which this Addendum is attached
Annex III: List of Sub processors (Modules 2 and 3 only):	Schedule 3 of the Agreement to which this Addendum is attached

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section **Error! Reference source not found.**: ☒ Importer ☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section **Error! Reference source not found.** of those Mandatory Clauses, are hereby incorporated.