Data Processing Addendum for the Onit Companies

This Data Processing Addendum ("Addendum") is entered into by and between Onit, Inc. ("Company") and the Customer named in the Order (each, a "Party" as applicable, and collectively, the "Parties") and is effective as of the Effective Date of the Order by virtue of the Parties accepting and executing the Order, together with the Onit Subscription and Services Agreement referenced in the Order ("Terms"). The Order, together with the Terms, is collectively referred to in this Addendum as the "Agreement". This Addendum amends and is incorporated into the terms of the Agreement between the Parties but only to the extent such Agreement provides for Company to access, collect, acquire, receive, transfer, process, and/or use the customer Personal Data (as defined below) of Customer. All capitalized terms not otherwise defined in this Addendum will have the meaning given to them in the Agreement. If you are accepting these terms, you warrant that: (a) you have full legal authority to bind Customer to this Addendum; (b) you have read and understand this Addendum; and (c) you agree, on behalf of Customer, to this Addendum. Company and Customer agree as follows:

1. **Definitions**. For purposes of this Addendum:

   a. **"Data Privacy Laws**" means all applicable laws, regulations, and other legal requirements in the jurisdictions in which Company operates relating to privacy, data protection, data security, communications secrecy, breach notification, or the Processing of Personal Data that are applicable to Company's provision of its services to its general customer base, without regard for Customer's specific use of those services, including without limitation, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* and the General Data Protection Regulation, Regulation (EU) 2016/679 ("**GDPR**") and the United Kingdom of Great Britain and Northern Ireland ("**UK**") Data Protection Act of 2018.

   b. **"Data Processor**" means Company receiving or accessing Personal Data of Customer for purposes of Processing under the Agreement.

   c. "**Data Subject**" means an identified or identifiable natural person about whom Personal Data relates, as set forth in **Annex 1**. "**Annex 1**" is also deemed to be "**Annex I**" for purposes of the Standard Contractual Clauses.

   d. "**Personal Data**" means Customer data that identifies an individual or is reasonably capable of being associated with an identified individual or device and includes "personal data," "personal information," and "personally identifiable information," and as such terms will have the same meaning as defined by the applicable Data Privacy Laws. Any Personal Data which has been de-identified or anonymized will not be considered Personal Data.

   e. "**Process**" and "**Processing**" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction within the production environments hosted by Company.

   f. "**Security Breach**" means any unauthorized and/or accidental destruction, loss, alteration, disclosure of, access to, or unlawful acquisition of Personal Data caused by Company.

   g. "**Security Measures**" mean appropriate administrative, technical, physical, and organizational measures designed to protect Personal Data, as set forth in **Annex 2**, as may be modified from time to time by Company provided that any such modifications will be adequate alternative measures and not materially degrade the Security Measures. "**Annex 2**" is also deemed to be "**Annex II**" for purposes of the Standard Contractual Clauses.

   h. "**Standard Contractual Clauses**" or "SCCs" means the terms under the GDPR setting forth the obligations for the transfer of Personal Data to Data Processors established in third countries adopted by the European Commission decision of June 4, 2021, attached hereto as **Annex 4**.

   i. **"Subcontractor"** means any entity that Company utilizes to fulfill any part of the Agreement with Customer and has access to Customer's Personal Data, including those set forth in **Annex 3**. "**Annex III**" is also deemed to be "**Annex 3**" for purposes of the Standard Contractual Clauses.

   j. **"UK Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office under S119A(1) Data Protection Act 2018 VERSION B1.0, in force 21 March 2022, for Restricted Transfers, attached hereto as **Annex 5**.

2. **Scope and Purposes of Processing**. Company will:

   a. Process Personal Data as set forth in this Addendum, as outlined in the Agreement, and in compliance with Data Privacy Laws applicable to Company as a Data Processor.

   b. Process Personal Data as may be mutually agreed in writing by Customer and Company from time to time.

   c. Process Personal Data as required by Data Privacy Laws to which Company is subject. In such case, and unless applicable law prohibits Company from doing so, Company will inform Customer of such legal requirement before such Processing.

3. **Personal Data Processing Requirements**. Company will:

   a. Require that the persons it authorizes to Process the Personal Data are subject to appropriate confidentiality obligations or are under an appropriate statutory obligation of confidentiality.

   b. Upon written request of Customer, assist Customer in the fulfilment of Customer's obligations to respond to verifiable requests by Data Subjects (or their representatives) for exercising their rights under Data Privacy Laws (such as rights to access or delete Personal Data).

c. Promptly notify Customer of (i) any third-party or Data Subject requests or complaints regarding the Processing of Personal Data; or (ii) any government or Data Subject requests for access to or information about Company's Processing of Personal Data on Customer's behalf, unless prohibited by Data Privacy Laws.

d. Provide reasonable assistance to and cooperation with Customer for Customer's consultation with regulatory authorities in relation to the Processing, including complying with any obligation applicable to Company under Data Privacy Laws.

4. **Data Security**. Company will implement appropriate administrative, technical, physical, and organizational measures designed to protect Personal Data, as set forth in Annex 2.

5. **Security Breach**. Company will notify Customer promptly of any Security Breach. Company will comply with the Security Breach-related obligations directly applicable to Data Processors under Data Privacy Laws and will assist Customer in Customer's compliance with its Security Breach-related obligations, including without limitation, by:

a. Providing Customer with details of the Security Breach to the extent known, which may include the nature of the Security Breach, the circumstances and the categories and approximate number of Data Subjects and Personal Data records involved; and

b. Addressing the Security Breach and where appropriate, mitigating possible adverse effects of the Security Breach to reduce the risk to Data Subjects whose Personal Data was involved, at Company's expense subject to the terms of the Agreement. Data Processor's liability under this Addendum shall be limited to one times the amount of fees paid by Customer to Company in the previous year.

6. **Subcontractors**.

a. Customer acknowledges and agrees that Company may use Company affiliates and other Subcontractors to Process Personal Data in accordance with the provisions of this Addendum and Data Privacy Laws, a copy of such list of Subcontractors which may be provided to Customer upon request.

b. Where Company subcontracts any of its rights or obligations concerning Personal Data, Company will (i) take steps to select and retain Subcontractors that are capable of maintaining appropriate privacy and security measures to protect Personal Data consistent with this Addendum; and (ii) enter into a written agreement with each Subcontractor that imposes obligations on the Subcontractor that are no less restrictive than those imposed on Company under this Addendum.

c. Company will maintain an up-to-date list of its Subcontractors which Company will provide to Customer upon request. In the event Customer objects to a new Subcontractor, Company will use reasonable efforts to make available to Customer a change in the services or recommend a commercially reasonable change to Customer's use of the services to avoid Processing of Personal Data by the objected-to Subcontractor without unreasonably burdening Customer and Company. Customer may, in its sole discretion, terminate the Agreement at any time and with thirty days' prior notice in the event that it objects to a Subcontractor and Company is unable to change the services to satisfy Customer.

7. **Data Transfers**. The Parties agree to be bound by the Standard Contractual Clauses to the extent that Company Processes Personal Data of Data Subjects to processors established in third countries which do not ensure an adequate level of data protection. The Standard Contractual Clauses will not apply with respect to Personal Data that Company Processes in the European Economic Area or in a country that the European Commission has decided provides adequate protection for Personal Data. The transfers of Personal Data of Data Subjects located in the UK to and from the UK and subsequent onward transfers shall be subject to the UK Data Protection Act of 2018 and the UK Addendum. In the event Standard Contractual Clauses apply, the Standard Contractual Clauses set forth in Annex 4 have be completed for Module Two: Transfer Controller to Processor as follows:

a. The Data Exporter is the Customer, and the Data Exporter's contact information is set forth in the Agreement.
b. The Data Importer is Company, and Company's contact information is set forth in the Agreement.
c. For the purposes of this DPA and the Agreement, Module Two (Transfer Controller to Processor) applies.
d. Clause 7 (Optional Docking Clause) does not apply.
e. Clause 8.9 (Documentation and compliance): the Parties agree that audits and requests for audits pursuant to Clause 8.9 shall be done in accordance with Section 8 (Audits) of this DPA.
f. Clause 9(a) (Use of Sub-processors): the Parties elect Option 2 (General Written Authorisation) with a 10-day notice period. Data Exporter consents to Data Importer's engagement of Sub-processor(s) in accordance with Section 6 (Subcontractors) of this DPA.
g. Clause 11(a) (Redress): the optional section does apply.
h. Clause 13 (Supervision) subclause (a): the third option shall be applicable.
i. Clause 17 (Governing Law): the Parties elect Option 2 and agree that the Clauses shall be governed by the law of Belgium.
j. Clause 18(b) (Choice of Forum and Jurisdiction): the Parties agree that any dispute arising from the Clauses shall be resolved by the courts of Belgium.
k. Annex 1 (Description of Processing) will apply to Annex I of the Standard Contractual Clauses.
l. Annex 2 (Technical and Organizational Security Measures) will apply to Annex II of the Standard Contractual Clauses.
m. Annex 3 (Subcontractors) will apply to Annex III of the Standard Contractual Clauses
n. Annex 5 (UK Addendum) will apply to Processing UK Personal Data.

8. **Audits**. Upon at least fifteen (15) business days advance notice once per calendar year, Customer may request Company to make available to Customer appropriate information necessary to demonstrate compliance with this Addendum, including to provide Customer with inspections conducted by Customer or its third-party provider, which will be subject to the strictest confidentiality obligations set forth in any of the Agreements and which will survive in accordance with the terms of the applicable Agreement, notwithstanding any termination of this Addendum. Any such audit will be conducted during regular business hours in such a way that the audit does not disrupt Company's business. If the scope of the audit has been addressed in a SSAE 18 Type 1 or Type 2 or similar audit report performed by a qualified third party auditor within the prior twelve (12) months, and

Company confirms there are no known material changes in the controls audited, Customer agrees to accept those reports in lieu of requesting an additional audit of the controls covered by the report.

9. **Return or Destruction of Personal Data**. Except to the extent required otherwise by Data Privacy Laws, Company will, at the choice of Customer, return to Customer and/or securely destroy all Personal Data upon (a) written request of Customer (excessive requests will incur reasonable fees for the administrative costs to comply with such request); or (b) in accordance with the terms of the applicable Agreement. Except to the extent prohibited by Data Privacy Laws, Company will inform Customer if it is not able to return or delete the Personal Data.

10. **Term**. The Addendum will be effective as of the Effective Date and remain in effect for so long as the Agreement between the Parties remains in effect. Upon expiration or termination of the Agreement then in effect between the parties, the Addendum and the obligations hereunder will automatically terminate.

11. **Governing Law**. This Addendum will be governed by the law governing the Agreement, provided that if this Addendum is applicable to more than one Agreement with more than one governing law set forth in the various Agreements, the laws of Delaware will apply.

12. **Conflicts**. To the extent of any conflict or inconsistency between the Agreement and the terms of this Addendum, then as it relates to data protection or processing, the terms of this Addendum shall govern and control except to the extent that the Order Form specifically modifies this Addendum by reference to this Addendum.

Annex 1:
Description of Processing

A. List of Parties

1. The Data Exporter is the Customer, and the Data Exporter's contact information is set forth in the Agreement.

2. The Data Importer is Company, and Company's contact information is set forth in the Agreement.

B. Description of Transfer

Categories of Data Subjects: The Personal Data transferred concern the following categories of Data Subjects (please specify):

Employees and contractors of Customers and those of Customers' vendors and other business partners.

Categories of Data: The Personal Data transferred concern the following categories of data (please specify):

Business contact information (such as name, email, location), employment related information, and other commercial information.

Sensitive Categories of Data (if appropriate): The Personal Data transferred concern the following special categories of data (please specify):

The data in each special category IS NOT automatically or routinely captured in most instances. Only when the information needed is subject to or part of an on-going litigation or investigation and is needed to further the litigation or investigation will this information be collected, transferred and/or stored. Generally most of the matter data collected is commercial in nature and will not involve this type of data.

Frequency: Continuous.

Nature of Processing: Scoping, implementing, and supporting software as a service that hosts a platform for in-house legal and other departments

Purpose: In house legal and other departments manage their matters and process invoices from vendors (e-billing) and manage other business processes or as otherwise specified in the Agreement.

Period of Data Retained: For the term of the Agreement.

Transfers to Sub-processors: The same terms as set forth above.

C. **Competent Supervisory Authority**: Belgian Data Protection Authority (APD) Autorité de protection des données in French or GBA, Gegevensbeschermingsautoriteit)

Annex 2: Security Measures

1. **Access Control to Hosted Facilities.** Measures must be taken to prevent unauthorized physical access to hosted facilities holding personal data. Measures may include:

- Access control system
- Uninterruptible power supply (UPS)
- Issuance of keys
- Door locking (electric door openers etc.)
- Surveillance facilities
- Alarm system, video/CCTV monitor
- Logging of facility exits/entries
- Use of ISO 27001 certified hosting providers

2. **Access Control to Systems.** Measures must be taken to prevent unauthorized access to IT systems. These must include the following technical and organizational measures for user identification and authentication:

- Password procedures (such as special characters, minimum length, forced change of password)
- No access for guest users or anonymous accounts
- Central management of system access
- Access to IT systems subject to approval from HR management and IT system administrators
- Multi-Factor Authentication wherever available.

3. **Access Control to Data.** Measures must be taken to prevent authorized users from accessing data beyond their authorized access rights and prevent the unauthorized input, reading, copying, removal, modification, or disclosure of data. These measures may include:

- Measures to prevent the use of automated data-processing systems by unauthorized persons using data communication equipment
- Access rights defined according to duties
- Automated log of user access via IT systems
- Differentiated access rights

4. **Disclosure Control.** Measures must be taken to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged. These measures may include:

- Compulsory use of encrypted connections for all data transfers
- Limited use of portable media
- Multi Factor Authentication for remote access, transport and communication of data
- Creating an audit trail of data transfers

5. **Input Control.** Measures must be put in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained. Measures should include:

- Ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment
- Logging user activities on IT systems
- Ensure that it is possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input

6. **Job Control.** Measures should be put in place to ensure that data is processed strictly in compliance with the data importer's instructions. These measures must include:

- Unambiguous wording of contractual instructions
- Monitoring of contract performance

7. **Availability Control.** Measures should be put in place to ensure that data are protected against accidental destruction or loss. These measures must include:

- Ensuring that installed systems may, in the case of interruption, be restored
- Ensure systems are functioning, and that faults are reported
- Ensure stored personal data cannot be corrupted by means of a malfunctioning of the system
- Business Continuity procedures
- Remote storage
- Anti-virus/firewall systems

8. **Segregation Control.** Measures should be put in place to allow data collected for different purposes to be processed separately. These should include:

- Restriction of access to data stored for different purposes according to staff duties.
- Segregation of business IT systems
- Segregation of IT testing and production environments

ANNEX 3
LIST OF SUBPROCESSORS

Those Subcontractors listed at www.Onit.com/sub-processors, as may be updated from time to time. Customer agrees to subscribe to the email update service set forth on the URL and maintain an up-to-date email address to receive updates.

ANNEX 4
STANDARD CONTRACTUAL CLAUSES

[MODULE TWO: Transfer controller to processor]

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 2016on 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 – Optional- **Not Applicable***

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

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.

Clause 9

Use of sub-processors

(a)OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

(c)Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its 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

(a) 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

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

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

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

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

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

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

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

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

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

Clause 15

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

15.1 **Notification**

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

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

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

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

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

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

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

15.2 **Review of legality and data minimisation**

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

(i)the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii)the data importer is in substantial or persistent breach of these Clauses; or

(iii)the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.
(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
(e)Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

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

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

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

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

APPENDIX

EXPLANATORY NOTE:
It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. **LIST OF PARTIES**

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*
1.Name: .....

Address: .....
Contact person's name, position and contact details: .....
Activities relevant to the data transferred under these Clauses: .....
Signature and date: .....
Role (controller/processor): .....

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*
1.Name: .....

Address: .....
Contact person's name, position and contact details: .....
Activities relevant to the data transferred under these Clauses: .....
Signature and date: .....
Role (controller/processor): .....

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred
.....
Categories of personal data transferred
.....
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
.....
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
.....
Nature of the processing
.....
Purpose(s) of the data transfer and further processing
.....
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
.....
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
.....

C. **COMPETENT SUPERVISORY AUTHORITY**

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

ANNEX II

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

EXPLANATORY NOTE:
The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.
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.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
Measures for user identification and authorisation
Measures for the protection of data during transmission
Measures for the protection of data during storage
Measures for ensuring physical security of locations at which personal data are processed
Measures for ensuring events logging
Measures for ensuring system configuration, including default configuration
Measures for internal IT and IT security governance and management
Measures for certification/assurance of processes and products
Measures for ensuring data minimisation
Measures for ensuring data quality
Measures for ensuring limited data retention
Measures for ensuring accountability
Measures for allowing data portability and ensuring erasure]
For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III

LIST OF SUB-PROCESSORS

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

1.Name: .....

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

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):
.....
.....

Annex 5:
UK ADDENDUM

Information Commissioner's Office

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

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	Effective Date	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: See Annex I.A of the EU SCCs Trading name (if different): Main address (if a company registered address): See Annex I.A of the EU SCCs Official registration number (if any) (company number or similar identifier):	Full legal name: See Annex I.A of the EU SCCs Trading name (if different): Main address (if a company registered address): See Annex I.A of the EU SCCs Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): See Annex I.A of the EU SCCs Job Title: Contact details including email:	Full Name (optional): See Annex I.A of the EU SCCs Job Title: Contact details including email:
Signature (if required for the purposes of Section 2)	See Annex I.A of the EU SCCs	See Annex I.A of the EU SCCs

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: The date of the last signature in Annex I.A of the EU SCCs

	Reference (if any): Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

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: Annex I.A of the EU SCCs
Annex 1B: Description of Transfer: Annex I.B of the EU SCCs
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Annex II of the EU SCCs
Annex III: List of Sub processors (Modules 2 and 3 only): Annex III of the EU SCCs

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 19: ☐ Importer ☐ Exporter ☒ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this

	Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so

far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

"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";

c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the

revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

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 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.