bugcrowd

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") forms part of the master services agreement or other overarching agreement (i.e. consulting agreement, vendor agreement, subscription agreement, etc.) (the "**Agreement**") between Bugcrowd, Inc. ("**Company**") and the entity listed and that signs as "**Service Provider**" on the signature page of this Agreement (Service Provider, together with Bugcrowd, are collectively referred to as the "**Parties**").

1. Subject Matter and Duration.

a) Subject Matter. This Addendum reflects the Parties' commitment to abide by Data Protection Laws concerning the Processing of Company Personal Data in connection with Service Provider's execution of the Agreement. All capitalized terms that are not expressly defined in this Addendum will have the meanings given to them in the Agreement. If and to the extent language in this Addendum or any of its Exhibits conflicts with the Agreement, this Addendum shall control.

b) Duration and Survival. This Addendum will become legally binding upon the effective date of the Agreement or upon the date that the Parties sign this Addendum if it is completed after the effective date of the Agreement. Service Provider will Process Company Personal Data until the relationship terminates as specified in the Agreement. Service Provider's obligations and Company's rights under this Addendum will continue in effect so long as Service Provider Processes Company Personal Data.

2. Definitions.

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

a) "**Company Personal Data**" means Personal Data Processed by Service Provider on behalf of Company. The Company Personal Data and the specific uses of the Company Personal Data are detailed in **Exhibit A** attached hereto.

b) "**Data Protection Laws**" means all applicable data privacy, data protection, and cybersecurity laws, rules and regulations to which the Company Personal Data are subject. "Data Protection Laws" shall include, but not be limited to, the California Consumer Privacy Act of 2018 ("**CCPA**"), the California Privacy Rights Act of 2020 ("**CPRA**") once in effect (the CCPA and CPRA are referred to collectively as the "**California Privacy Laws**"), and the EU General Data Protection Regulation 2016/679 ("**GDPR**"); the Swiss Federal Act on Data Protection; the United Kingdom General Data Protection Regulation; and the United Kingdom Data Protection Act 2018 (in each case, as amended, adopted, or superseded from time to time.

c) "**Personal Data**" shall have the meaning assigned to the terms "personal data" and/or "personal information" under Data Protection Laws and shall, at a minimum, include any information relating to an identified or identifiable natural person.

d) "**Process**" or "**Processing**" means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

e) "**Security Incident(s)**" means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Company Personal Data.

f) "**Services**" means any and all services that Service Provider performs under the Agreement.

g) "**Third Party(ies)**" means Service Provider's authorized contractors, agents, vendors and third party service providers (i.e., sub-processors) that Process Company Personal Data.

3. Data Use and Processing.

a) Documented Instructions. Service Provider and its Third Parties shall Process Company Personal Data solely for the purpose of providing the Services to Company, and solely to the extent necessary to provide the Services to Company, in each case, in accordance with the Agreement, this Addendum and Data Protection Laws. Service Provider will, unless legally prohibited from doing so, inform Company in writing if it reasonably believes that there is a conflict between Company's instructions and applicable law or otherwise seeks to Process Company Personal Data in a manner that is inconsistent with Company's instructions.

b) Authorization to Use Third Parties. To the extent necessary to fulfill Service Provider's contractual obligations under the Agreement or any Statement of Work, Company hereby authorizes (i) Service Provider to engage Third Parties and (ii) Third Parties to engage sub-processors.

c) Service Provider and Third Party Compliance. Service Provider shall (i) enter into a written agreement with Third Parties that imposes on such Third Parties (and their sub-processors) data protection and security requirements for Company Personal Data that are at least as restrictive as the obligations in this Addendum; and (ii) remain responsible to Company for Service Provider's Third Parties' (and their sub-processors if applicable) failure to perform their obligations with respect to the Processing of Company Personal Data. Service Provider shall flow down all obligations in this Addendum to Third Parties (and their sub-processors) regarding, among other things: (i) Company Personal Data and (ii) all Company's and Company's regulator's rights regarding review and audit (including Company's right to appoint an independent third party to perform such review or audits).

d) Right to Object to Third Parties. Service Provider shall make available to Company a list of Third Parties that Process Company Personal Data upon reasonable request. Prior to engaging any new Third Parties that Process Company Personal Data, Service Provider will notify Company via email

and allow Company thirty (30) days to object. If Company has legitimate objections to the appointment of any new Third Party, the Parties will work together in good faith to resolve the grounds for the objection for no less than thirty (30) days, and failing any such resolution, Company may terminate the part of the Service performed under the Agreement that cannot be performed by Service Provider without use of the objectionable Third Party. Service Provider shall refund any pre-paid fees to Company in respect of the terminated part of the Service.

e) Confidentiality. Any person or Third Party authorized to Process Company Personal Data must contractually agree to maintain the confidentiality of such information or be under an appropriate statutory obligation of confidentiality.

f) Personal Data Inquiries and Requests. Service Provider agrees to provide reasonable assistance and comply with all reasonable instructions from Company related to any requests from individuals exercising their rights in Company Personal Data granted to them under Data Protection Laws (e.g., access, rectification, erasure, data portability, etc.). If a request is sent directly to Service Provider, Service Provider shall promptly notify Company within five (5) days of receiving such request and shall not respond to the request unless Company has authorized Service Provider to do so.

g) Sale of Company Personal Data Prohibited. Service Provider shall not sell Company Personal Data as the term "sell" is defined by the applicable California Privacy Laws. Service Provider shall not disclose or transfer Company Personal Data to a Third Party or other parties that would constitute "selling" as the term is defined by the applicable California Privacy Laws.

h) Data Protection Impact Assessment and Prior Consultation. Service Provider agrees to provide reasonable assistance at Company's expense to Company where, in Company's judgement, the type of Processing performed by Service Provider requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

i) Demonstrable Compliance. Service Provider agrees to keep records of its Processing in compliance with Data Protection Laws and provide any necessary records to Company to demonstrate compliance with this Addendum upon reasonable request.

4. Cross-Border Transfers of Personal Data.

a) Cross-Border Transfers of Personal Data. Company authorizes Service Provider and its Third Parties to transfer Company Personal Data across international borders, including from the European Economic Area, Switzerland, and/or the United Kingdom to the United States, provided that such transfer complies with Data Protection Laws.

b) Data Transfer Impact Assessment Questionnaire. Service Provider agrees that it has provided true, complete, and accurate responses to the Data Transfer Impact Assessment Questionnaire attached hereto as **Exhibit B**. Service Provider will notify Company if there are material changes to the responses originally provided by Service Provider following the effective date of this Addendum.

c) Standard Contractual Clauses. If Service Provider or its Third Parties Process Company Personal Data originating in the European Economic Area, Switzerland, and/or United Kingdom in a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws, the parties agree that the Standard Contractual Clauses attached hereto as **Exhibit C** shall apply. Where the Standard Contractual Clauses are applicable and Company acts as a controller of Company Personal Data with Service Provider acting as a processor of Company Personal Data, each party shall comply with its obligations under Module Two of the Standard Contractual Clauses. Where the Standard Contractual Clauses are applicable and Company acts as a processor of Company Personal Data with Service Provider also acting as a processor of Company Personal Data, each party shall comply with its obligations under Module Three of the Standard Contractual Clauses. Service Provider agrees that Company shall be an intended third-party beneficiary of Service Provider's Third Party agreements as contemplated by Clause 9(e) of the Standard Contractual Clauses and, where applicable, such provisions are intended to inure to the benefit of the Company. Without limiting the foregoing, if the conditions contemplated by Clause 9(e) of the Standard Contractual Clauses apply, Company will be entitled to enforce Service Provider's agreement(s) with its Third Parties as contemplated by Clause 9(e) of the Standard Contractual Clauses as if Company were a signatory to such Third Party agreements. Each party's signature to this Addendum shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder.

d) Data Transfer Impact Assessment Outcome. Taking into account the information and obligations set forth in this Addendum and, as may be the case for a party, such party's independent research, to the parties' knowledge, the Company Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom that is transferred pursuant to the attached Standard Contractual Clauses to a country that has not been found to provide an adequate level of protection under applicable Data Protection Laws is afforded a level of protection that is essentially equivalent to that guaranteed by applicable Data Protection Laws.

5. **Information Security Program.**

a) Service Provider agrees to implement and maintain appropriate technical and organizational measures to protect Company Personal Data (the "**Information Security Program**"). At a minimum, such measures shall include:

i) Pseudonymisation of Company Personal Data where appropriate, and encryption of Company Personal Data

in transit and at rest;

ii) The ability to ensure the ongoing confidentiality, integrity, availability of Service Provider's Processing and Company Personal Data;

iii) The ability to restore the availability and access to Company Personal Data in the event of a physical or technical incident;

iv) A process for regularly evaluating and testing the effectiveness of the Service Provider's Information Security Program to ensure the security of Company Personal Data from reasonably suspected or actual accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

6. Security Incidents.

a) Security Incident Procedure. Service Provider will deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents including procedures to (i) identify and respond to reasonably suspected or known Security Incidents, mitigate harmful effects of Security Incidents, document Security Incidents and their outcomes, and (ii) restore the availability or access to Company Personal Data in a timely manner.

b) Notice. Service Provider agrees to provide prompt written notice without undue delay (but in no event longer than twenty-four (24) hours) to Company's Designated POC if it knows or reasonably suspects that a Security Incident has taken place. Such notice will include all available details required under Data Protection Laws for Company to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

c) Remediation. Company has the right to participate in the investigation and response to the Security Incident and Service Provider agrees to cooperate fully in the investigation and remediation of any harm or potential harm caused by the Security Incident. To the extent that a Security Incident gives rise to a need, in Company's sole judgment to: (i) provide notification to public and/or regulatory authorities, individuals, or other persons, or (ii) undertake other remedial measures (including, without limitation, notice, credit monitoring services and the establishment of a call center to respond to inquiries – collectively, "**Remedial Action**"), at Company's request and direction, and at Service Provider's cost, Service Provider agrees to undertake such Remedial Actions. Company shall have sole discretion to control and direct the timing, content and manner of any notices, including but not limited to communication with Company customers and/or employees, regarding the same. If Company chooses to carry out the Remedial Action itself, Service Provider agrees to reimburse Company for its costs.

7. Audits.

a) Right to Audit; Permitted Audits. In addition to any other audit rights described in the Agreement, Company and its regulators shall have the right to an on-site audit of Service Provider's architecture, systems, policies and procedures relevant to the security and integrity of Company Personal Data, or as otherwise required by a governmental regulator:

i) Following any notice from Service Provider to Company of an actual or reasonably suspected Security Incident involving Company Personal Data;

ii) Upon Company's reasonable belief that Service Provider is not in compliance with Data Protection Laws, this Addendum or its security policies and procedures under the Agreement;

iii) As required by governmental regulators; and

iv) For compliance purposes, once annually.

b) Audit Terms. Any audits described in this Section shall be:

i) Conducted by Company or its regulator, or through a third party independent contractor selected by one of these parties;

ii) Conducted during reasonable times;

iii) To the extent possible, conducted upon reasonable advance notice to Service Provider; and

iv) Of reasonable duration and shall not unreasonably interfere with Service Provider's day-to-day operations.

c) Third Parties. In the event that Company conducts an audit through a third party independent auditor or a third party accompanies Company or participates in such audit, such third party shall be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect Service Provider's and Service Provider's customers' confidential and proprietary information. For the avoidance of doubt, regulators shall not be required to enter into a non-disclosure agreement.

d) Audit Results. Upon Service Provider's request, after conducting an audit, Company shall notify Service Provider of the manner in which Service Provider does not comply with any of the applicable security, confidentiality or privacy obligations or Data Protection Laws herein. Upon such notice, Service Provider shall make any necessary changes to ensure compliance with such obligations at its own expense and without unreasonable delay and shall notify Company when such changes are complete. Notwithstanding anything to the contrary in the Agreement, Company may conduct a follow-up audit within six (6) months of Service Provider's notice of completion of any necessary changes. To the extent that a Service Provider audit and/or Company audit identifies any material security vulnerabilities, Service Provider shall remediate those vulnerabilities within fifteen (15) days of the completion of the applicable audit, unless any vulnerability by its nature cannot be remedied within such time, in which case the remediation must be completed within a mutually agreed upon time not to exceed sixty (60) days.

8. Data Storage and Deletion.

a) Data Storage. Service Provider will abide by the following with respect to storage of Company Personal Data:

i) Service Provider will not store or retain any Company

bugcrowd

Personal Data except as necessary to perform the Services under the Agreement.

b) Data Deletion. Service Provider will abide by the following with respect to deletion of Company Personal Data:

i) Within thirty (30) calendar days of the Agreement's expiration or termination, or sooner if requested by Company, Service Provider will securely destroy (per subsection (iii) below) all copies of Company Personal Data (including automatically created archival copies).

ii) Upon Company's request, Service Provider will promptly return to Company a copy of all Company Personal Data within thirty (30) days and, if Company also requests deletion of the Company Personal Data, will carry that out as set forth above.

iii) Company Personal Data shall be disposed of in a method that prevents any recovery of the data in accordance with industry best practices for shredding of physical documents and wiping of electronic media (e.g., NIST SP 800-88).

iv) Upon Company's request, Service Provider will provide a "Certificate of Deletion" certifying that Service Provider has deleted all Company Personal Data. Service Provider will provide the "Certificate of Deletion" within thirty (30) days of Company's request.

9. Indemnification.

a) Service Provider shall indemnify, defend, and hold harmless Company and its officers, directors, employees and agents from and against any claims, disputes, demands, liabilities, damages, losses, fines, and costs and expenses, including, without limitation, reasonable attorneys' fees arising out of or relating to: (i) a Security Incident; (ii) Service Provider's negligence or willful misconduct related to Company Personal Data; and/or (iii) Service Provider's breach of this Addendum.

10. Contact Information.

a) Company and Service Provider agree to designate a point of contact for urgent privacy and security issues (a "**Designated POC**"). The Designated POC for both parties are:

- Company Designated POC:_____
- Service Provider Designated POC: _____

BUGCROWD, INC.

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

SERVICE PROVIDER
Entity Name: _____

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

Exhibit A to the Data Processing Addendum

1.1 Subject Matter of Processing	The Processing will involve Processing for: The subject matter of Processing is the Services pursuant to the Agreement.
1.2 Duration of Processing	The Processing will continue until the expiration or termination of the Agreement.
1.3 Categories of Data Subjects	Includes the following: Data subjects whose Company Personal Data is Processed pursuant to the Agreement.
1.4 Nature and Purpose of Processing	Includes the following: The purpose of Processing of Company Personal Data by Service Provider is the performance of the Services pursuant to the Agreement.
1.5 Types of Personal Information	Includes the following: Company Personal Data Processed pursuant to the Agreement.

Exhibit B to the Data Processing Addendum

Data Transfer Impact Assessment Questionnaire

This Exhibit B forms part of the Addendum. Capitalized terms not defined in this Exhibit B have the meaning set forth in the Addendum.

1. What countries will Company Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom be stored in or accessed from? If this varies by region, please specify each country for each region.

    a. **Answer:** [Service Provider to insert response].

2. What are the categories of data subjects whose Company Personal Data will be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

    a. **Answer:** [Service Provider to insert response].

3. What are the categories of Company Personal Data transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

    a. **Answer:** [Service Provider to insert response].

4. Will any Company 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 be transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom? If so, are there any 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?

    a. **Answer:** [Service Provider to insert response].

5. What business sector is Service Provider involved in?

    a. **Answer:** [Service Provider to insert response].

6. Broadly speaking, what are the services to be provided and the corresponding purposes for which Company Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom?

    a. **Answer:** [Service Provider to insert response].

7. What is the frequency of the transfer of Company Personal Data outside of outside of the European Economic Area, Switzerland, and/or the United Kingdom? E.g., is Company Personal Data transferred on a one-off or continuous basis?

    a. **Answer:** [Service Provider to insert response].

8. When Company Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom to Service Provider, how is it transmitted to Service Provider? Is the Company Personal Data in plain text, pseudonymized, and/or encrypted?

    a. **Answer:** [Service Provider to insert response].

9. What is the period for which the Company Personal Data will be retained, or, if that is not possible, the criteria used to determine that period?

    a. **Answer:** [Service Provider to insert response].

10. Please list the Third Parties that will have access to Company Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom:

Name of Third Party	Subject matter, nature, and duration of processing	Location (Country)	Adequacy Mechanism Supporting Transfer
[Service Provider to complete].			

11. Is Service Provider subject to any laws in a country outside of the European Economic Area, Switzerland, and/or the United Kingdom where Company Personal Data is stored or accessed from that would interfere with Service Provider fulfilling its obligations under the attached Standard Contractual Clauses? For example, FISA Section 702. If yes, please list these laws.

    a. **Answer:** [Service Provider to insert response].

12. Has Service Provider ever received a request from public authorities for information pursuant to the laws contemplated by Question 11 above (if any)? If yes, please explain.

    a. **Answer:** [Service Provider to insert response].

13. Has Service Provider ever received a request from public authorities for Personal Data of individuals located in European Economic Area, Switzerland, and/or the United Kingdom? If yes, please explain.

    a. **Answer:** [Service Provider to insert response].

14. What safeguards will Service Provider apply during transmission and to the processing of Company Personal Data in countries outside of the European Economic Area, Switzerland, and/or the United Kingdom that have not been found to provide an adequate level of protection under applicable Data Protection Laws?

    a. **Answer:** Those safeguards set forth in the Addendum.

Exhibit C to the Data Processing Addendum

This Exhibit C forms part of the Addendum.

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.

(e) To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the Parties' processing of personal data that is subject to the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection.

(f) To the extent applicable hereunder, these Clauses, as supplemented by Annex III, also apply mutatis mutandis to the Parties' processing of personal data that is subject to UK Data Protection Laws (as defined in Annex III).

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) 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)

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

(iv) Clause 12 – 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 Two and Three: Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional

Docking clause – Omitted

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE TWO: Transfer controller to processor

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (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.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. 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 thirty (30) days 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 TWO: Transfer controller to processor

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

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

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

MODULE THREE: Transfer processor to processor

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

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

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

Clause 11

Redress

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

(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 TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

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

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

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

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

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

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Where the data exporter is established in an EU Member State, the following section applies: 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 following section applies: 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 following section applies: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

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

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

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

Clause 15

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

15.1 Notification

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

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

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

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

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

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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 Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

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

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

APPENDIX

ANNEX I

A. **LIST OF PARTIES**

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Data exporter(s):

1. .....Name: Company.

.....Address: As set forth in the Notices section of the Agreement.

.....Contact person's name, position and contact details: Company's Designated POC.

.....Activities relevant to the data transferred under these Clauses: As set forth in Exhibit B.

.....Role (controller/processor): Controller.

Data importer(s):

1. .....Name: Service Provider.

.....Address: As set forth in the Notices section of the Agreement.

.....Contact person's name, position and contact details: Service Provider's Designated POC.

.....Activities relevant to the data transferred under these Clauses: As set forth in Exhibit B.

.....Role (controller/processor): Processor.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred

.....As set forth in Exhibit B.

Categories of personal data transferred

.....As set forth in Exhibit B.

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.

.....As set forth in Exhibit B.

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

.....As set forth in Exhibit B.

Nature of the processing

.....As set forth in Exhibit B.

Purpose(s) of the data transfer and further processing

.....As set forth in Exhibit B.

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

.....As set forth in Exhibit B.

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

.....As set forth in Exhibit B.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

.....The supervisory authority mandated by Clause 13. If no supervisory authority is mandated by Clause 13, then the Irish Data Protection Commission (DPC), and if this is not possible, then as otherwise agreed by the parties consistent with the conditions set forth in Clause 13.

ANNEX II

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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.

Data importer shall implement and maintain appropriate technical and organisational measures that protect personal data in accordance with the Addendum.

Pursuant to Clause 10(b), data importer will provide data exporter assistance with data subject requests in accordance with the Addendum.

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 UK 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 of the Addendum.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Company. Main address (if a company registered address): As set forth in the Notices section of the Agreement.	Full legal name: Service Provider. Main address (if a company registered address): As set forth in the Notices section of the Agreement.
Key Contact	Contact details including email: Company Designated POC.	Contact details including email: Service Provider Designated POC.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	[x] The version of the Approved EU SCCs which this UK Addendum is appended to, detailed below, including the Appendix Information: Date: The effective date of the 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 UK Addendum is set out in:

Annex 1A: List of Parties: As set forth in Exhibit C, Annex I.
Annex 1B: Description of Transfer: As set forth in Exhibit C, Annex I.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set forth in Exhibit C, Annex II.

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

Ending this UK Addendum when the Approved UK Addendum changes	Which Parties may end this UK Addendum as set out in Section 19: Exporter.

Part 2: Mandatory Clauses

Entering into this UK Addendum

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

2. 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 UK 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 UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this UK Addendum

3. Where this UK 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 EU SCCs	The version(s) of the Approved EU SCCs which this UK 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 UK 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 Addendum	This International Data Transfer Addendum which is made up of this UK Addendum incorporating the Addendum EU SCCs.
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.

4. This UK 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.

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

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

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

8. 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 UK Addendum has been entered into.

Hierarchy

9. 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.

10. Where there is any inconsistency or conflict between the Approved UK Addendum and the UK Addendum EU SCCs (as applicable), the Approved UK 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 UK Addendum.

11. Where this UK 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 UK Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This UK 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 UK 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.

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

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

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

a. References to the "Clauses" means this UK 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 UK Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this UK Addendum

16. 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.

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

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

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

    b. reflects changes to UK Data Protection Laws;

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

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

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

    b. its risk under the UK 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 UK 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 UK Addendum.

20. The Parties do not need the consent of any third party to make changes to this UK 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 UK 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.