ABNORMAL SECURITY

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") supplements the agreement for use of the Abnormal Security Corporation ("**Abnormal**") Service ("**Agreement**") entered into by and between Abnormal and the Customer identified on the signed or accepted Order Form or Agreement ("**Customer**"). Abnormal and Customer may each be referred to separately as, a "**Party**," or together as, the "**Parties**."

Customer has purchased a Subscription to the Service pursuant to the Agreement that involves the Processing of Personal Data subject to Data Protection Laws.

is incorporated into and forms part of the agreement for Customer's use of Abnormal's services The Parties agree as follows:

1. Definitions. All capitalized terms used but not otherwise defined in this Section 1 or within the body of this Addendum have the respective meanings given to them in the Agreement.

"**CCPA Personal Information**" means the "personal information" (as defined in the CCPA) that Abnormal Processes on behalf of Customer in connection with Abnormal's provision of the Service and Support.

"**Controller**" has the meaning given to it in the Data Protection Laws and for the purposes of this Addendum means Customer.

"**Data Protection Laws**" means the following laws, including any amendments to such laws: (i) the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "**Privacy Directive**") and the General Data Protection 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, and repealing Directive 95/46/EC ("**GDPR**"); (ii) the UK Data Protection Act 2018 as supplemented by Schedule 21, the Keeling Schedule ("**UK GDPR**"); (iii) to the extent applicable to the Service and/or Support, any other EU or EU Member State data protection laws with respect to the processing of Personal Data under the Agreement; (iv) the following laws applicable to processing of personal information of citizens of Australia and New Zealand respectively, the *Privacy Act 1988* (Cth) and the *Privacy Act 1993* (NZ) (together "**ANZ Privacy Law**"), and (v) any United States laws or regulations protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the Processing of Personal Data, including the California Consumer Privacy Act of 2018 and any binding regulations promulgated thereunder ("**CCPA**").

"Data Subject" means a "consumer" (as defined in the CCPA), a "data subject" as defined in the GDPR and in the UK GDPR), or an "individual" as defined in ANZ Privacy Law, as applicable.

"**GDPR Personal Data**" means the "personal data" (as defined in the GDPR and the UK GDPR) that Abnormal Processes on behalf of Customer in connection with Abnormal's provision of the Service.

"**Personal Data**" means any information relating to a Data Subject which is subject to the Data Protection Laws and which Abnormal Processes on behalf of Customer as described in Section 4 of this Addendum, including CCPA Personal Information, GDPR Personal Data, and UK GDPR Personal Data.

"**Personal Data Breach**" means a breach of security leading to accidental or unlawful destruction, loss, or alteration, unauthorized disclosure of, or access to, Personal Data Processed by Abnormal on behalf of Customer.

"**Process**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by

automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

"**Processor**" has the meaning given to it in the Data Protection Laws and for the purposes of this Addendum means Abnormal.

"**Standard Contractual Clauses"** means, (i) where the GDPR applies, the terms attached to this Addendum as Exhibit 1 and promulgated pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on standard contractual clauses for the transfer of personal data to Processors established in third countries which do not ensure an adequate level of data protection ("**GDPR SCCs**"), and (ii) where the UK GDPR applies, the terms attached to this Addendum as Exhibit 2 and issued by the Information Commissioner under s 119A(1) of the DPA 2018 and in force 21 March 2022 ("**UK GDPR SCCs**").

2. Compliance with laws. Each Party will comply with the Data Protection Laws as applicable to it, including with respect to the Processing of Personal Data.

3. Customer obligations. Customer as Controller undertakes that all instructions for the Processing of Personal Data under the Agreement or this Addendum or as otherwise agreed will comply with the Data Protection Laws, and such instructions will not in any way cause Abnormal to be in breach of any Data Protection Laws. Customer is solely responsible for ensuring the accuracy, quality, and legality of Personal Data Processed by Abnormal including the means by which Customer acquired Personal Data.

4. Data Processing. Abnormal will Process the Personal Data for the sole purpose of providing the Service and Support to Customer. Abnormal will Process the Personal Data in accordance with Customer's instructions as documented in the Agreement and this Addendum for the term of the Agreement. Abnormal will not access, use or otherwise Process such Personal Data, except as necessary to provide the Service and Support.

Unless prohibited by applicable law, Abnormal will notify Customer if in its opinion, an instruction infringes any Data Protection Laws to which it is subject, in which case Abnormal will be entitled to suspend performance of such instruction, until Customer confirms in writing that such instruction is valid under Data Protection Laws. Any additional instructions regarding the manner in which Abnormal Processes the Personal Data will require prior written agreement between Abnormal and Customer.

Abnormal will not disclose Personal Data to any government, except as necessary to comply with applicable law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If Abnormal receives a binding order from a law enforcement agency for Personal Data, Abnormal will notify Customer of the request it has received so long as Abnormal is not legally prohibited from doing so.

Abnormal will ensure that individuals with access to or involved in the Processing of Personal Data are subject to appropriate confidentiality obligations and/or are bound by related obligations under Data Protection Laws or other applicable laws.

5. Requirements for GDPR Personal Data. This Section 5 shall only apply to Abnormal's Processing of GDPR Personal Data as permitted by the Agreement. This Addendum, together with the Agreement, serves as the binding contract referred to in Article 28(3) of the GDPR and Section 59 of the UK GDPR that sets out the subject matter, duration, nature, and purpose of the Processing, the type of Personal Data and categories of data subjects as well as the obligations and rights of the Controller. In the provision of the Service and Support by Abnormal to Customer pursuant to the Agreement, Customer acts as Controller and Abnormal acts as Processor with respect to the Personal Data. Abnormal may process Personal Data in connection with its provision of the Service and Support in countries that have different data protection regulations than the GDPR and the UK GDPR ("**Third Countries**"). In such event, subject to the terms of this Addendum, the Standard Contractual Clauses in the form provided in Exhibit 1 and Exhibit 2 of this Addendum (as applicable) will govern the transfer of Personal Data to such Third Countries, including to Subprocessors in such Third Countries, unless the transfer of Personal Data occurs via an alternative means permitted by relevant Data Protection Laws.

6. Requirements for CCPA Personal Information. This Section 6 shall only apply to Abnormal's Processing of CCPA Personal Information as permitted by the Agreement. For the purposes of the CCPA, Abnormal and Customer acknowledge and agree that Abnormal will act as a "service provider" (as defined in the CCPA) in its performance of its obligations under the Agreement. Abnormal shall not retain, use or disclose CCPA Personal Information for any purpose other than for the specific purposes of providing the Service and Support, or as otherwise permitted by the CCPA. Abnormal acknowledges and agrees that it shall not retain, use or disclose CCPA Personal Information for a commercial purpose other than providing the Service and Support, generating Threat

Intelligence Data, and performing its obligations under the Agreement. Processing CCPA Personal Information outside the scope of this Addendum or the Agreement will require prior written agreement between the Customer and Abnormal on additional instructions for Processing. Abnormal will not "sell" (as defined in the CCPA) any CCPA Personal Information.

7. Technical and organizational security measures. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Abnormal will in relation to the Personal Data implement appropriate technical and organizational measures to ensure a level of security of the Personal Data appropriate to the risk presented by Processing, as further described on Annex II to Exhibit 1 of this Addendum.

In assessing the appropriate level of security, Abnormal will take into account in particular the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

8. Data Subjects rights. Abnormal will assist Customer in responding to Data Subjects' requests exercising their rights under the Data Protection Laws. To that effect, Abnormal will (i) to the extent permitted by applicable law, promptly notify Customer of any request received directly from Data Subjects to access, correct or delete its Personal Data without responding to that request, and (ii) upon written request from Customer, provide Customer with information that Abnormal has available to reasonably assist Customer in fulfilling its obligations to respond to Data Subjects exercising their rights under the Data Protection Laws.

9. Data Protection Impact Assessments. If Customer is required under the Data Protection Laws to conduct a data protection impact assessment, then upon written request from Customer, Abnormal will assist where reasonably possible in the fulfilment of the Customer's obligation as related to its use of the Service and Support, to the extent Customer does not otherwise have access to the relevant information. If required under Data Protection Laws Abnormal will provide reasonable assistance to Customer in the cooperation or prior consultation with the Data Protection Authorities in relation to any applicable data protection impact assessment.

10. Audit of Technical and Organizational Measures. Abnormal will make available all information necessary to demonstrate its compliance with data protection policies and procedures implemented as part of the Service. To this end, upon written request (not more than once annually) Customer may, at its sole cost and expense, verify Abnormal's compliance with its data protection obligations as specified in this Addendum by: (i) submitting a security assessment questionnaire to Abnormal; and (ii) if Customer is not satisfied with Abnormal's responses to the questionnaire, then Customer may conduct an audit in the form of meetings with Abnormal's information security experts on a mutually agreeable date. Such interviews will be conducted with a minimum of disruption to Abnormal's normal business operations and subject to Abnormal's agreement on scope and timing. The Customer may perform the verification described above either itself or by a mutually agreed upon third party auditor, provided that Customer or its authorized auditor executes a mutually agreed upon non-disclosure agreement. Customer will be responsible for any actions taken by its authorized auditor. All information disclosed by Abnormal under this Section 10 will be deemed Abnormal Confidential Information, and Customer will not disclose any audit report to any third party except as obligated by law, court order or administrative order by a government agency. Abnormal will remediate any mutually agreed, material deficiencies in its technical and organizational measures identified by the audit procedures described in this Section 10 within a mutually agreeable timeframe.

11. Breach notification. If Abnormal becomes aware of a Personal Data Breach that results in unlawful or unauthorized access to, or loss, disclosure, or alteration of the Personal Data, which is likely to cause a risk to the fundamental rights and freedoms of the Data Subjects, then Abnormal will notify Customer without undue delay after becoming aware of such Personal Data Breach and will cooperate with the Customer and take such commercially reasonable steps as agreed with Customer to assist in the investigation, mitigation and remediation of such Personal Data Breach. Abnormal will provide all reasonably required support and cooperation necessary to enable Customer to comply with its legal obligations in case of a Personal Data Breach pursuant to Data Protection laws, including Articles 33 and 34 of the GDPR and Sections 67 and 68 of the UK GDPR.

12. Subprocessing. Customer agrees that Abnormal may appoint either Abnormal affiliated companies or third party providers as sub-Processors under the Agreement and this Addendum ("**Subprocessors**") and hereby authorizes Abnormal to engage such Subprocessors in the provision of the Service and Support. Abnormal will restrict the Processing activities performed by Subprocessors to only what is strictly necessary to provide the Service to Customer pursuant to the Agreement and this Addendum. Abnormal will impose appropriate contractual obligations in writing upon the Subprocessors that are no less protective than this Addendum, and

Abnormal will remain responsible for the Subprocessors' compliance with the obligations under this Addendum.

Abnormal maintains a list of all Subprocessors at www.abnormalsecurity.com/trust which is also set forth in Annex III to Exhibit 1 hereto (together, the "**Subprocessors List**") and Abnormal may amend the Subprocessors List by adding or replacing Subprocessors at any time. Customer will be entitled to object to a new Subprocessor by notifying Abnormal in writing the reasons of its objection. Abnormal will work in good faith to address Customer's objections. If Abnormal is unable or unwilling to adequately address Customer's objections to its reasonable satisfaction, then Customer may terminate this Addendum and the Agreement in accordance with Section 4.2 of the Agreement.

13. Return or Deletion of Personal Data. Abnormal will delete or return, in Customer's discretion and upon Customer's written request, Personal Data within a reasonable period of time following the termination or expiration of the Agreement.

14. Entire Agreement; Conflict. Except as amended by this Addendum, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this Addendum, the terms of this Addendum will control. In the event of any conflict between the Addendum and the Standard Contractual Clauses in Exhibit 1 or 2, the Standard Contractual Clauses shall prevail.

EXHIBIT 1 (GDPR SCCs)

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:

1. 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
2. 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:

1. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
2. 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);
3. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
4. Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
5. Clause 13;
6. Clause 15.1(c), (d) and (e);
7. Clause 16(e);
8. Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Optional Docking clause removed

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

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

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

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

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

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

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:

The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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. 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 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

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 (GDPR SCCs)

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: The named "Customer" on the signed or accepted Order Form or Agreement.

Address: The address associated with Customer on the signed or accepted Order Form or Agreement.

Contact person's name, position and contact details: The contact details associated with the Customer on the signed or accepted Order Form or Agreement.

Activities relevant to the data transferred under these Clauses: See Description of Transfer below.

Signature and date: Refer to the signed or accepted Order Form or Agreement.

Role (controller/processor): Controller

Data importer(s):

1. Name: Abnormal Security Corporation

Address: 185 Clara Street, Suite 100, San Francisco, CA 94107, United States

Contact person's name, position and contact details: The contact details associated with Abnormal on the signed or accepted Order Form or Agreement.

Activities relevant to the data transferred under these Clauses: See Description of Transfer below.

Signature and date: Refer to the signed or accepted Order Form or Agreement.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Individual users of Data Controller's email system, as well as individuals sending messages to or receiving messages from such user accounts.

Categories of personal data transferred

First and Last Name

Email address

IP address

Personal Data contained in email message body or attachments

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.

N/A

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

Ongoing as determined by the Controller

Nature of the processing

For the provision of the Service under the Agreement

Purpose(s) of the data transfer and further processing

Scanning of email contents and metadata for malicious signatures

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

During the Term and as specified under the Agreement

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

During the Term and as specified under the Agreement

C. COMPETENT SUPERVISORY AUTHORITY

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

The competent supervisory authority will be determined in accordance with the GDPR.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES

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

Abnormal has taken and will maintain the appropriate administrative, technical, physical and procedural security measures, for the protection of the Personal Data, including the measures set forth below or otherwise made reasonably available by Abnormal.

Policy Controls:

- Abnormal has established an information security policy.
- A framework of security standards has been developed, which supports the objectives of the security policy.
- Procedures and systems exist for requesting, establishing, issuing, suspending, deleting, and closing user accounts and associated access privileges, e.g. system access is granted based upon position, job function, and manager approval.
- Abnormal prevents unauthorized internal access to customer data by limiting access to only employees who need access to offer and improve the Service
- Multi-Factor Authentication, including biometric fingerprint verification, is required to access Abnormal systems and Customer Data.
- Access to Abnormal offices is controlled via card key access, and is under 24/7 CCTV monitoring.
- No Customer Data is stored on premise.

Collection of Data:

- The Service processes Customer Data on an in-memory basis within Customer's email system.
- Data that is processed and identified as malicious by the Service is transferred to Abnormal servers that support the Service and stored for 180 days. Such data is then automatically deleted at the end of the 180-day period.
- All Customer Data is encrypted at rest using multi-factor encryption with a per-file key and AES-256 block cipher, with keys managed by AWS Key Management Service.

Backup Copies:

- Procedures for backup and retention of data and programs have been documented and implemented.
- Data and programs are backed up regularly and replicated between geographically diverse data centers.

Computers and Access Terminals:

- New employees are required to sign a non-disclosure agreement relating to proprietary software and confidentiality of information relating to customers.
- New employees are required to acknowledge receipt of Abnormal's Information Security Policy.
- Access to the production environment is authorized by the Chief Technology Officer and is based on business need. A multi-factor secure remote access is required for all access to the production systems.
- Customer Data is processed in memory and is not available for printing. All print services are disabled by default on all production servers

Access Controls:

- All Data Importer employees and contractors are provided with unique userIDs
- Access is only granted to employees whose role requires it
- Access is disabled upon role reassignment or termination.
- Access is revoked on termination.

Security while transferring and processing:

- Isolated network environment using Amazon VPC
- Default blocked firewall policies
- Limited number of integration-related endpoints are accessible via public internet. Majority of services protected by firewalls as private endpoints.
- Public endpoints utilize Application Load Balancers, and are resilient to dynamic changes in query load/throughput
- Data in transit encrypted using TLS 1.2 sessions with a 2048-bit RSA asymmetric key
- HTTPS required for all web traffic
- Encrypted connectors for databases using SSL

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors: The sub-processors located on the agreed list available at www.abnormalsecurity.com/trust. As of the effective date, the current list of sub-processors is:

1. Name: Amazon Web Services

Address: United States

Contact person's name, position and contact details: N/A

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Data hosting services for the Abnormal Security SaaS platform

EXHIBIT 2 (UK GDPR SCCs)

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		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	The named "Customer" on the signed or accepted Order Form or Agreement and Affiliates of the Customer established in the UK The address associated with Customer on the signed or accepted Order Form or Agreement	Abnormal Security Corporation 185 Clara Street, Suite 100, San Francisco, CA 94107, United States Official registration number (if any) (company number or similar identifier): N/A
Key Contact	The contact details associated with the Customer on the signed or accepted Order Form or Agreement.	The contact details associated with Abnormal on the signed or accepted Order Form or Agreement.
Signature (if required for the purposes of Section 2)	Refer to the signed or accepted Order Form or Agreement.	Refer to the signed or accepted Order Form or Agreement.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	**X** - The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Effective Date of the MSA. Reference (if any): As set out in Exhibit 1 of the MSA

Table 3: Appendix Information

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

Annex 1A: List of Parties: As listed in Annex 1 of the Approved EU SCCs found in Exhibit 1 of the MSA
Annex 1B: Description of Transfer: As described in Annex 1 of the Approved EU SCCs found in Exhibit 1 of the MSA
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As described in Annex 1 of the Approved EU SCCs found in Exhibit 1 of the MSA
Annex III: List of Sub processors (Modules 2 and 3 only): As listed in Annex 1 of the Approved EU SCCs found in Exhibit 1 of the MSA

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 **X** - Neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. 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.

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 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

3. 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.

4. 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.

5. 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.

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

7. 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.

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 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 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.

11. 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

12. 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.

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 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

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 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 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.

19. 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.

20. 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.