DATA TRANSFER ADDENDUM FOR CUSTOMERS

This Data Transfer Addendum (including its Exhibits) ("**DTA**") forms part of and is subject to the agreement between Customer ("**You"** or "**Your**") and Company ("**We**," "**Us**," or "**Our**") under which Company provides the Customer with Products and Services (the "**Agreement**") and supplements the Data Processing Agreement for Customers ("**DPA**") by and between Customer and the Company entity providing Products and Services to the Customer. Company and Customer may each be referred to in this DTA and DPA as a "**Party**" or together as the "**Parties**."

This DTA reflects the Parties' commitment to abide by Applicable Laws concerning the transfer of Personal Data originating from Argentina, the European Economic Area, Switzerland, and/or the United Kingdom to a country that has not been found to provide an adequate level of protection under Applicable Laws. Capitalized terms not defined in this DTA (including its Exhibits) shall have the meaning set forth in the DPA or, if not defined in the DPA, in the Agreement. If and to the extent this DTA or any of its Exhibits conflicts with the Agreement or the DPA, this DTA shall control.

1.   DEFINITIONS

Argentine Model Clauses: means the Model Agreement of International Transfer of Personal Data for the case of Provision of Services (*Contrato modelo de transferencia internacional de datos personales con motivo de prestación de servicios*) (reference: EX-2016-00311578- -APN-DNPDP#MJ- Anexo II) approved by the *Dirección Nacional de Protección de Datos Personales* on 2 November 2016 together with the Annex attached hereto as *Exhibit A*.

EU Standard Contractual Clauses means the Standard Contractual Clauses for the transfer of personal data to third countries issued by the European Commission under Commission Implementing Decision (EU) 2021/914 of 4 June 2021, or such alternative as may be approved by the European Commissioner from time to time.

Transfer Mechanism: means the Argentine Model Clauses, the EU Standard Contractual Clauses, and the UK Addendum, as defined herein.

UK Addendum means version B1.0 of the document entitled "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" as issued by the UK Information Commissioner under s119A(1) of the UK Data Protection Act 2018, in force 21 March 2022, or such alternative as may be approved by the UK Information Commissioner from time to time.

2.   Restricted Transfer from Argentina

If Personal Data originating from Argentina is Transferred by You from Argentina to Us in a country that has not been found to provide an adequate level of protection under Applicable Laws, the Parties agree that the transfer shall be governed by the Argentine Model Clauses, the terms of which are incorporated herein by reference.

3.   Restricted Transfers from EEA, Switzerland, and/ or the United Kingdom

a.   Data Transfer Impact Assessment Questionnaire. We have provided responses to the Data Transfer Impact Assessment Questionnaire attached hereto as Exhibit B, and the Parties acknowledge that the responses set forth therein may be used for compliance with Clause 14 of the EU Standard Contractual Clauses.

b.   EEA, Swiss, and UK Standard Contractual Clauses. If Personal Data originating from the European Economic Area or Switzerland is Transferred by You to Us in a third country that has not been found to provide an adequate level of protection under Applicable Laws, the Parties agree that the transfer shall be governed by the EU Standard Contractual, Module Two (controller-to-processor transfers) attached hereto as Exhibit C and incorporated herein by reference. If Personal Data originating from the United Kingdom is Transferred by You to Us in a third country that has not been found to provide an adequate level of protection under Applicable Laws in the UK, the Parties agree that the transfer shall

be governed by the EU Standard Contractual Clauses as supplemented and amended by the UK Addendum, attached hereto as Exhibit D, and incorporated herein by reference. For purposes of the EU Standard Contractual Clauses and the UK Addendum, the Parties agree that Customer is the 'data exporter' (as Controller) and Company is the 'data importer' (as Processor), and that:

(i)   the audit described in Clause 8.9 of the EU Standard Contractual Clauses shall be carried out in accordance with Section 7 of the DPA;

(ii)   the information required under Clause 15.1(c) will be provided upon Your written request;

(iii)   notwithstanding anything to the contrary, You will reimburse Us for all costs and expenses incurred by Us in connection with the performance of Our obligations under Clause 15.1(b) and Clause 15.2 of the EU Standard Contractual Clauses without regard for any limitation of liability set forth in the Agreement; and

(iv)   to the extent transfers of Personal Data originate from Switzerland, the Parties agree that, for purposes of the EU Standard Contractual Clauses: (1) the term 'member state' shall be interpreted to include Switzerland and, for the avoidance of doubt, the term 'data subject' includes residents of Switzerland; (2) references to the EU Regulation 2016/679 (General Data Protection Regulation, "**GDPR**") are to be interpreted as including a reference to the Swiss Federal Data Protection Act ("**Swiss FDPA**"); and (3) for data transfers subject solely to the Swiss FDPA, the Swiss Federal Data Protection Authority is the competent supervisory authority, and disputes arising from such transfers may be brought in the courts of Switzerland.

4.   Miscellaneous

In the event of inconsistencies between the provisions of the Transfer Mechanisms and this DTA, DPA, or the Agreement, the applicable Transfer Mechanism shall take precedence to the extent required by Applicable Laws. In the event that any Transfer Mechanism attached as an Exhibit hereto is amended, replaced, or repealed under Applicable Laws, Company may amend such Transfer Mechanism as required by Applicable Laws to enable the continued transfer of Personal Data under this DTA.

EXHIBIT A
DATA TRANSFER ADDENDUM

Annex A of the Argentine Model Clauses

This Exhibit A forms part of the DTA. As stated in Section 2 of the DTA, the Parties have agreed that the Argentine Model Clauses have been incorporated into the DTA by reference. This Exhibit A sets forth the content of Annex A of the Argentine Model Clauses (Description of the Transfer and Intended Services, *Descripción de la Transferencia y Servicios Previstos*). The Parties agree that Customer is the Data Exporter (*exportador de datos*) and Company is the Data Importer (*importador de datos*).

Titulares de los datos	Data Owners
Los datos personales transferidos se refieren a las siguientes categorías de titulares de los datos:	The personal data transferred concern the following categories of data owners:
Consulte la descripción de la transferencia adjunta.	*The response set forth in the Data Transfer Impact Assessment Questionnaire shall apply mutatis mutandis to Transfers that are subject to the Argentine Model Clauses.*

Características de los datos	Characteristics of the data
Los datos personales transferidos se refieren a las siguientes categorías de datos:	The personal data transferred concern the following categories of data:
Consulte la descripción de la transferencia adjunta.	*The response set forth in the Data Transfer Impact Assessment Questionnaire shall apply mutatis mutandis to Transfers that are subject to the Argentine Model Clauses.*

Tratamientos previstos y finalidad	Purpose of the data processing to be conducted:
Los datos personales transferidos serán sometidos a los siguientes tratamientos y finalidades:	The transferred personal data will be subject to the following processing and purposes:
Consulte la descripción de la transferencia adjunta.	*The response set forth in the Data Transfer Impact Assessment Questionnaire shall apply mutatis mutandis to Transfers that are subject to the Argentine Model Clauses.*

DATA TRANSFER ADDENDUM

Data Transfer Impact Assessment Questionnaire

This Exhibit B forms part of the DTA. Capitalized terms not defined in this Exhibit B have the meaning set forth in the DTA, the DPA, or the Agreement.

1. What countries will 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.

Answer: Personal Data may be stored in or accessed from Australia, Canada, Chile, China, Colombia, Dominican Republic, Egypt, the European Economic Area, India, Israel, Jamaica, Japan, Malaysia, Mexico, New Zealand, Norway, Philippines, Serbia, Singapore, South Africa, South Korea, Switzerland, Turkey, United Arab Emirates, the United Kingdom, United States and Vietnam.

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

Answer: Data Subjects whose Personal Data is processed under the Agreement are Customer's end users, including, but not limited to, Customer's employees, contractors, contingent workers, business partners, vendors, and any other end users that receive access to the Products and Services through Customer.

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

Answer: The categories of Personal Data that are processed under the Agreement are data that are used to provide the Products and Services: details about Customer end users' computers, devices, applications, and networks, including internet protocol (IP) address, cookie identifiers, mobile carrier, Bluetooth device IDs, mobile device ID, mobile advertising identifiers, MAC address, IMEI, Advertiser IDs, and other device identifiers that are automatically assigned to computers or devices of Customer end users when accessing the Internet, browser type and language, language preferences, battery level, on/off status, geo-location information, hardware type, operating system, Internet service provider, pages that Customer end users visit before and after using the Products and Services, the date and time of site visits, the amount of time end users spend on each page, information about the links Customer end user click and pages viewed within the Products and Services, and other actions taken through use of the Products and Services such as preferences.

4. Will any 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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures?

Answer: Not to our knowledge.

5. What business sector is the Company involved in?

Answer: Cybersecurity.

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

Answer: We provide cybersecurity services. Personal Data is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom in order to provide the Products and Services. This includes, but is not limited to, the following processing activities: (i) processing Personal Data to provide information technology services to Customer employees; (ii) processing Personal Data to provide security and data protection Products and Services; and (iii) processing Personal Data to enhance Company threat defenses.

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

Answer: We will retain Personal Data in accordance with the Agreement.

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

Answer: Personal Data is transferred to Us on a continuous basis via Customer's use of the Products and Services.

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

Answer: All Personal Data that is transmitted to Us is protected in accordance with *Exhibit A* of the DPA.

10.   Please list the third-party Sub-Processors that will have access to Personal Data that is transferred outside of the European Economic Area, Switzerland, and/or the United Kingdom:

Answer: Our list of Sub-processors includes those parties set forth at the following URL: https://www.skyhighsecurity.com/en-us/about/legal.html

11.   Is the Company subject to any laws in a country outside of the European Economic Area, Switzerland, and/or the United Kingdom where Personal Data is stored or accessed from that would interfere with Us fulfilling our obligations under the EU Standard Contractual Clauses? For example, FISA 702 or U.S. Executive Order 12333. If yes, please list these laws.

Answer: As of the effective date of the DPA, no court has found Us to be eligible to receive process issued under the laws contemplated by Question 11, including FISA Section 702 and no such court action is pending.

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

Answer: No.

13.   Have We ever received a request from public authorities to access Personal Data of individuals located in European Economic Area, Switzerland, and/or the United Kingdom? If yes, please explain.

Answer: No.

14.   What safeguards will We apply during transmission and to the processing of 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?

Answer: Those safeguards set forth in the DPA and this DTA.

EXHIBIT C

DATA TRANSFER ADDENDUM

This Exhibit C forms part of the DTA.

EU STANDARD CONTRACTUAL CLAUSES - SECTION I

Clause 1	**Purpose and Scope**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding 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 the United Kingdom General Data Protection Regulation as supplemented by terms in the Data Protection Act 2018.

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 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) 2016/67 9.

Clause 3	**Third-Party Beneficiaries**

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

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

    (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii)	Clause 9(a), (c), (d) and (e);
(iv)	Clause 12(a), (d) and (f);
(v)	Clause 13;
(vi)	Clause 15.1(c), (d) and (e);
(vii)	Clause 16(e);
(viii)	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 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* | **Docking Clause** |

Omitted

OBLIGATIONS OF THE PARTIES - SECTION II

| *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 organizational 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 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 organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, 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 organizational 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 authorized 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, 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 defense of legal claims in the context of specific administrative, regulatory, or judicial proceedings; or

(iv)   the onward transfer is necessary 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 consider 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**

MODULE TWO:	**Transfer Controller to Processor**

(a)   The data importer has the data exporter's general authorization 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 ten (10) 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** |

| *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 authorized 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 organizational 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 authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

| *MODULE TWO:* | **Transfer Controller to Processor** |

(a) 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.

(b) 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.

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

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

(e)   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** |

<div style="background:blue;color:white">MODULE TWO: Transfer Controller to Processor</div>

(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** |

<div style="background:blue;color:white">MODULE TWO: Transfer Controller to Processor</div>

(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 behavior 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.

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

Clause 14   Local Laws and Practices affecting Compliance with the Clauses

MODULE TWO: Transfer Controller 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 authorizing 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 authorizing access by such authorities – relevant considering the specific circumstances of the transfer, and the applicable limitations and safeguards;

  (iii)   any relevant contractual, technical, or organizational 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 organizational 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, in so far 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**

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 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 Minimization**

(a)   The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the

applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

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

FINAL PROVISIONS - SECTION IV

Clause 16   Non-Compliance with the Clauses and Termination

MODULE TWO: Transfer Controller to Processor

(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**

MODULE TWO: Transfer Controller 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

(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.

| **A.** | **LIST OF PARTIES** |

MODULE TWO: **Transfer Controller to Processor**

Data Exporter: Customer (name, address, and contact details as set forth in the Agreement)

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

Signature and Date: As per the Agreement.

Role: Controller

Data Importer: Company (name, address, and contact details as set forth in the Agreement)

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

Signature and Date: As per the Agreement.

Role: Processor

| **B.** | **DESCRIPTION OF TRANSFER** |

MODULE TWO: **Transfer Controller to Processor**

Categories of data subjects whose personal data is transferred

(As set forth in Exhibit B of the DTA.)

Categories of personal data transferred

(As set forth in Exhibit B of the DTA.)

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

(As set forth in Exhibit B of the DTA.)

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 of the DTA.)

Nature of the processing

(As set forth in Exhibit B of the DTA.)

Purpose(s) of the data transfer and further processing

(As set forth in Exhibit B of the DTA.)

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 of the DTA.)

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

(As set forth in Exhibit B of the DTA.)

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer Controller to Processor

The supervisory authority mandated by Clause 13 is 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 to Exhibit C
TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer Controller to Processor

Description of the technical and organizational 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.

The technical and organizational measures can be found at the following link: https://trellix.com/en-us/assets/docs/legal/technical-and-organisational-measures.pdf

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

ANNEX III to Exhibit C
LIST OF SUB-PROCESSORS

Available at the following link: https://www.skyhighsecurity.com/en-us/about/legal.html

EXHIBIT D
UK ADDENDUM TO THE EU STANDARD CONTRACTUAL CLAUSES

VERSION B1.0, IN FORCE 21 MARCH 2022

This Exhibit D forms part of the DTA.

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 start date of this DTA	
The Parties	**Exporter(s) (who send the Restricted Transfer)**	**Importer(s) (who receive the Restricted Transfer)**
Parties' details	**Full legal name:** (That of the Customer, as set forth in Exhibit C, Annex I, Part A of this DTA.) **Trading name (if different):** (That of the Customer, as set forth in Exhibit C, Annex I, Part A of this DTA.) **Main address (if a company registered address):** (That of the Customer, as set forth in Exhibit C, Annex I, Part A of this DTA.) **Official registration number (if any) (company number or similar identifier):** See the Agreement.	**Full legal name:** (That of the Company, as set forth in Exhibit C, Annex I, Part A of this DTA.) **Trading name (if different):** (That of the Company, as set forth in Exhibit C, Annex I, Part A of this DTA.) **Main address (if a company registered address):** (That of the Company, as set forth in Exhibit C, Annex I, Part A of this DTA.) **Official registration number (if any) (company number or similar identifier):** See the Agreement.
Key Contact	**Full Name (optional), Job Title, and Contact details including email:** (Those of the Customer, as set forth in Exhibit C, Annex I, Part A of this DTA.)	**Full Name (optional), Job Title, and Contact details including email:** (Those of the Company, as set forth in Exhibit C, Annex I, Part A of this DTA.)

Table 2:	**Selected SCCs, Modules and Selected Clauses**

Addendum EU SCCs	☒ <u>**The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:**</u>
	Date: the date of this DTA
	Reference (if any): -
	Other identifier (if any): -
	Or
	☐ The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	-	-	-	-	-	-
2	-	-	-	-	-	-
3	-	-	-	-	-	-
4	-	-	-	-	-	-

Table 3:	**Appendix Information**

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

Annex 1A: List of Parties:	(As set forth in Exhibit C, Annex I, Part A of this DTA.)
Annex 1B: Description of Transfer:	(As set forth in Exhibit C, Annex I, Part B of this DTA.)
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 of this DTA.)
Annex III: List of Sub processors (Modules 2 and 3 only):	(As set forth in Exhibit C, Annex III of this DTA.)

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

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ **Importer** ☐ Exporter ☐ neither Party

PART 2: MANDATORY CLAUSES

Entering into this Addendum

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.

-End-