TRANSMIT SECURITY DATA PROTECTION ADDENDUM FOR CLOUD SERVICES

Effective Date: *November 14, 2025*

This Data Protection Addendum (this **"Addendum**") supplements and forms part of the Transmit Security Agreement for Cloud Services ("**Agreement**") entered into between You and Transmit Security. Except as modified in this Addendum, the terms of the Agreement shall remain in full force and effect and defined terms under the Agreement shall have the same meaning in this Addendum, unless defined differently in this Addendum. If there is a conflict between the Agreement and this Addendum, the terms of this Addendum will prevail. For the avoidance of doubt, this Addendum is in force as at the earlier of (each as applicable) (i) the effective date of the Agreement, or (ii) the commencement of processing of End User Personal Data through the Cloud Services, and will remain in effect until termination of the Agreement; or the last processing of End User Personal Data under the Agreement and this Addendum.

1. **Definitions.** In this Addendum, the following words and expressions have the following meanings:

   a. "**Controller**", "**Data Subject**", "**Personal Data Breach**", "**Processor**", "**Supervisory Authority**" and "**processing**" all have the meanings given to those terms in the GDPR (and related terms such as "**process**", **"processes**" and "**processed**" shall have corresponding meanings).

   b. "**Data Protection Laws**" means all laws and regulations relating to data protection and privacy as applicable to the parties and/or to the processing of Custom Personal Data under this Addendum, including without limitation, the EU General Data Protection Regulation 2016/679 ("**EU GDPR**"), the EU GDPR in such form as incorporated into the laws of the United Kingdom by virtue of the European Union (Withdrawal) Act 2018 ("**UK GDPR**", together with the EU GDPR, the "**GDPR**"), the UK Data Protection Act 2018, and any associated implementing legislation and regulations, in each case, as in force and applicable, and as amended, supplemented or replaced from time to time. "**EU Standard Contractual Clauses**" means the Annex to the European Commission's decision of 4 June 2021 on Standard Contractual Clauses for transfer of personal data to third countries which do not ensure an adequate level of data protection pursuant to the GDPR.

   c. "**End User Personal Data**" means End User Data to the extent such data consists of Personal Data;

   d. "**Identity Network End User Personal Data**" means Identity Network End User Data to the extent such data consists of Personal Data.

   e. "**UK Addendum**" means the International Data Transfer Addendum to the Standard Contractual Clauses, issued by the UK Information Commissioner for parties making restricted transfers, which entered into force on 21 March 2022.

   f. "**Sub-Processor**" means another Processor engaged by Transmit Security whilst acting as a Processor for carrying out processing activities in respect of End User Personal Data.

2. **Transmit Security as Controller**.

   a. Transmit Security and Customer shall each be independent Controllers in relation to any Identity Network End User Personal Data processed by it for all purposes, including, in the case of Transmit Security, to provide authentication services to the End User in relation to third party technology platforms, provided that Transmit Security shall remain a Processor in relation to any use of Identity Network End User Personal Data to provide authentication services relating to the End User to the Customer. Each party shall comply with Data Protection Laws applicable to its processing of Identity Network End User Personal Data, including by:

      i. implementing and maintaining throughout the period in which Identity Network End User Personal Data is being processed technical and organizational measures to ensure a level of security appropriate to the risks which may occur as a result of processing the Identity Network End User Personal Data, including to protect against Personal Data Breaches; and

      ii. providing notice to End Users as to how it will use the Identity Network End User Personal Data and obtaining any necessary consents from End Users.

   b. When acting as Controller of the Identity Network End User Personal Data, Customer shall also:

      i. provide reasonable assistance to Transmit Security if required for: (A) exercising of Data Subject Rights; (B) providing notice to Data Subjects; and (C) notifying Data Subjects and Supervisory Authorities about Personal Data Breaches; and

      ii. notify Transmit Security without undue delay upon: (A) receiving a request form a Data Subject relating to the Identity Network End User Personal Data; (B) receiving any claim, complaint or allegation relating to the processing of Identity Network End User Personal Data from any Supervisory Authority or third party; and (C) becoming aware of a Personal Data Breach affecting the Identity Network End User Personal Data.

   c. Customer authorizes Transmit Security to copy, anonymize, create derivative works of and otherwise process End User Personal Data, in whole or in part, for the purpose of deriving statistical and usage data, and data related to the functionality of Transmit Security's products and services and combine or incorporate End User Personal Data with or into other similar data and information available, derived or obtained from other customers, licensees, users or other sources for improving Transmit Security's existing products and services and developing new Transmit Security products and services. Transmit Security is a

Controller for such processing and will process the End User Personal Data in accordance with Data Protection Laws applicable to the processing of such data.

3. **Transmit Security as Processor.**

   a. Other than as set out in Section 2, Transmit Security shall be a Processor in relation to End User Personal Data and this Section 3 shall apply.

   b. **Processing mandate and Controller instructions:** Transmit Security will carry out the processing of End User Personal Data derived from the provision of the Cloud Services contracted by Customer in accordance with the Agreement, limiting itself to carrying out the actions that are necessary to provide Customer with the Cloud Services relating to the processing of the End User Personal Data and otherwise perform its obligations and the Customer's instructions in accordance with this Addendum and its Appendices. Specifically, Transmit Security undertakes to carry out the processing of the End User Personal Data in accordance with the instructions given at all times by Customer, as well as with the provisions of Data Protection Laws, including with regard to transfers of End User Personal Data to a third country or an international organization, unless Transmit Security is obliged to do so by virtue of Data Protection Laws of the UK, EEA or EEA Member State law applicable to it, in which case Transmit Security shall inform Customer of this legal requirement prior to the processing unless prohibited from doing so by applicable law. Where Transmit Security believes that an instruction would result in a violation of any applicable Data Protection Laws, Transmit Security shall notify Customer thereof.

   c. **Details of Processing**. The details of the processing activities to be carried out by Transmit Security in respect of the Cloud Services are specified in **Appendix 1.**

   d. **Data Subjects Rights**. Taking into account the nature of the processing, Transmit Security shall assist Customer, by using appropriate technical and organizational measures, insofar as this is possible, in the fulfillment of Customer's obligations to respond to requests by Data Subjects in exercising their rights under Data Protection Laws.

   e. **Confidentiality**. Transmit Security shall ensure that its personnel engaged in the processing of End User Personal Data are bound by a binding confidentiality undertaking.

   f. **Personal Data Breach**. Transmit Security must notify Customer without undue delay of any Personal Data Breach affecting End User Personal Data.

   g. **Record of processing activities**. Transmit Security shall maintain up-to-date written records of its processing activities carried out on behalf of Customer under this Section 3 and as required under Data Protection Laws.

   h. **Sub-Processors**. Customer acknowledges and agrees that Transmit Security may engage any of the Sub-Processors listed in **Appendix 2** to provide the Cloud Services to Customer, which Transmit Security may update from time to time. If Transmit Security appoints a new Sub-Processor not identified in **Appendix 2**, Transmit Security shall notify Customer of such appointment within 10 business days prior to using the new Sub-Processor for the Cloud Services. If no objection is provided by Customer within such 10 business days or the objection is not reasonably founded on the lack of necessary guarantees regarding compliance with Data Protection Laws by the Sub-Processor, such Sub-Processor will be considered as approved by the Customer. Transmit Security shall ensure that prior to permitting any Sub-Processor to process End User Personal Data, the Sub-Processor has entered into a binding written agreement with Transmit Security which imposes obligations substantially equivalent and no less protective than the obligations imposed on Transmit Security under this Addendum (to the extent applicable to the nature of the services provided by such Sub-processor). Where that Sub-Processor fails to fulfil its data protection obligations concerning End User Personal Data, Transmit Security shall remain fully liable to Customer for the performance of that Sub-Processor's obligations.

   i. **Assistance**. Transmit Security will reasonably assist Customer in ensuring compliance with Customer's obligations related to the security of the processing, notification and communication of a Personal Data Breach affecting End User Personal Data, conduct of data protection impact assessments by Customer, and prior consultations with a relevant Supervisory Authority in connection with data protection impact assessments.

   j. **Information**. Transmit Security will make available to Customer, upon request, information necessary to demonstrate compliance with Transmit Security's obligations set forth in this Section 3.

   k. **Audits**. Upon Customer's reasonable request (but no more than once every 12-month period), Transmit Security shall cooperate with audits and inspections of its compliance with the requirements and obligations herein and/or under Data Protection Laws as relates to End User Personal Data. Such audits and inspections may be conducted by Customer or by any reputable third party designated by Customer subject to confidentiality obligations. Transmit Security's obligations under this audit section are subject to Customer:

      i. Giving Transmit Security reasonable prior notice of such audits and/or inspections being required by Customer;

      ii. Ensuring that all information obtained or generated by Customer or its representatives in connection with such audits and/or inspections is kept strictly confidential (save for disclosure to relevant Supervisory Authorities or as otherwise required by applicable laws; and

iii. Ensuring that such audits and/or inspections are undertaken during normal business hours, with, so far as reasonably practicable, minimal disruption to Transmit Security's business and the business of other customers of Transmit Security.

l. **Technical and Organizational Measures**.

i. Transmit Security shall implement and maintain appropriate technical and organizational measures in relation to the processing of End User Personal Data to ensure a level of security that is appropriate for dealing with and protecting against risks to the rights and freedoms of the Data Subjects which may occur as a result of the processing of such End User Personal Data, and as required in order to avoid accidental or unlawful destruction, loss, alteration or unauthorized disclosure of, or access to Custom Personal Data and/or as otherwise required pursuant to Data Protection Laws, including, *inter alia*, the measures set forth in **Appendix 3**. When complying with the above obligations, Transmit Security shall take into consideration the state of technological development existing at the time and the nature, scope, context and purposes of processing as well as the aforementioned risks.

ii. Transmit Security shall ensure that all persons acting under its authority or on its behalf and having access to the End User Personal Data, do not process the End User Personal Data except as instructed by Customer and permitted herein.

m. **International Transfers of UK/EEA Personal Data.**

i. Where You are contracting with Transmit Security, Inc under the Agreement, the parties acknowledge that the End User Personal Data will be transferred by You to Transmit Security in the United States of America (US), and that the US is a country not deemed adequate for the transfer of Personal Data by the European Commission (in relation to transfers subject to the EU GDPR) or the UK government (in relation to transfers subject to the UK GDPR) ("**Non-Adequate Country**"). To the extent the End User Personal Data is subject to the GDPR, and is not provided directly by the End Users to Transmit Security, the parties agree that such data transfer shall be governed by *Module Two: Controller to Processor* of the EU Standard Contractual Clauses which are hereby incorporate into and form part of this Addendum in the form set out in **Appendix 4**, and the parties hereby conclude and agree to be bound by such EU Standard Contractual Clauses. To the extent the End User Personal Data is subject to the UK GDPR and as required by the UK GDPR, the EU Standard Contractual Clauses shall be supplemented by the UK Addendum, set out in **Appendix 6.**

ii. To the extent Personal Data made available to You by Transmit Security is subject to the GDPR and You are based outside of the EEA or the UK, in a Non-Adequate Country, the parties agree that any transfer of Personal Data from Transmit Security to You shall be governed by Module Four: Processor to Controller of the EU Standard Contractual Clauses which are hereby incorporated into and form part of this Addendum in the form set out in **Appendix 5**, and the parties hereby conclude and agree to be bound by such EU Standard Contractual Clauses. To the extent the Personal Data is subject to the UK GDPR and as required by the UK GDPR, the EU Standard Contractual Clauses shall be supplemented by the UK Addendum, set out in **Appendix 6.**

iii. Transmit Security shall not transfer End User Personal Data to any party outside of the EEA and UK in a Non-Adequate Country (including permitting access to Custom Personal Data from any party in such countries) without the prior written consent of Customer, unless the transfer/access is in compliance with Data Protection Laws (including having in place appropriate transfer safeguards as applicable).

n. **Return and Deletion of Personal Data**. On Customer's request, Transmit Security shall return or destroy the End User Personal Data except as required to be retained by the laws of the UK, EEA or EEA Member State (as applicable).

o. **Obligations of Customer.** Customer will ensure that the End User Personal Data provided to Transmit Security is obtained and transferred to Transmit Security in compliance with Data Protection Laws. Customer hereby represents that it is solely responsible for the accuracy, quality and legitimacy of the End User Personal Data and the means through which they were collected.

4. **Complete agreement and amendments.** This Addendum and its Appendices constitute the complete and entire agreement between the parties in relation to the subject matter hereof and supersedes all prior or contemporaneous agreements and contracts or negotiations in relation thereto.

Appendix 1 – Processing Details

Nature and purpose of the processing. Transmit Security will process End User Personal Data as necessary to perform the Cloud Services contracted by the Customer under the Agreement, and as further instructed by Customer in accordance with the Agreement, the Order Form, and this Addendum.

Duration of processing. Transmit Security will process End User Personal Data for the duration of the Agreement (or as otherwise agreed upon by the parties in writing), and in accordance with Transmit Security's retention obligations under this Addendum and the Agreement, provided that End User Personal Data shall not be processed for longer than is necessary for the purpose for which it was collected or is being processed (except where a statutory exception applies).

Categories of Data Subjects. End Users.

Types of Personal Data. Customer may request the processing of End User Personal Data for the provision of the Cloud Services which may include, but is not limited to the following categories of Personal Data.

Types of Data
End-user IP address, User agent
Optional Data Types (subject to Customer Choice): End-user email, End-user phone number, Custom data (any additional information Customer configures)
Optional Data Types - subject to the Platform capabilities being used by Customer: Transaction Sum, Payee, Payment Requester, End-User Location, Device Information (e.g., bound devices), First Name, Last Name, Middle Name, Date of Birth, Profile Picture Link, Preferred Language, Network Information, Hardware and Software Attributes, Application Journey Details, Interaction Events, Unique Identifier, Country, ID Document Details (document number, document photo, details on ID), Selfie Photo
Retention Policy: All data is saved by default for ninety (90) days unless Customer specifies a different retention period.

Appendix 2 - Sub-Processors & Sub-Contractors

Depending on (a) the geographic location of a Customer or their End Users, and (b) the nature of the Cloud Services provided, as indicated below, Transmit Security may also use Sub-processors to provide the Services to Customer.

Sub-Processor Entity	Brief Description of Processing	Location of Sub-Processor	Applies to Following Products:
Amazon Web Services, Inc.	Hosting	US, EU	Entire Cloud Platform[1]
		Canada, Australia, Singapore	Mosaic
		Brazil	FlexID Cloud
MongoDB Atlas	Database as a Service	US, EU	Entire Cloud Platform
		Canada, Singapore	Mosaic
		Canada, Brazil	FlexID Cloud
Google Cloud Platform	Hosting, End User Logging	US, EU	Entire Cloud Platform
		Canada, Australia, Singapore	Mosaic
		Canada	FlexID Cloud
Coralogix	System monitoring and logs	EU	Entire Cloud Platform
Sentry	Admin Portal Monitoring	US	Mosaic
Movate	Provide Tier 2 Support Services	India and Costa Rica	Entire Platform[2]
Bright Inventions	Provide Escalated Support Services and Production Maintenance	Poland	Mosaic
Cloudflare	Network Routing and Protection	Local[3]	Entire Cloud Platform
Veriff[4]	Identity Verification Vendor	US, EU	Mosaic - Identity Verification Services
Salesforce	Customer Relations and Support	US	Entire Platform

[1]Entire Cloud Platform: FlexID Cloud, BindID, Mosaic
[2]Entire Platform: FlexID, FlexID Cloud, BindID, Mosaic
[3]Cloudflare routes traffic to Worldwide Data Centers that are closest to the user's location.
[4]Veriff is relevant only to Mosaic Identity Verification Services.

Appendix 3- Technical and Security Measures

SECURITY DOMAIN	DESCRIPTION OF THE MEASURE
General Security Measures	• SOC2 Compliance • IT Security and operational policies and procedures • DevOps/IT Monitoring Policies and Tools • Auditing and SIEM • Data Encryption (at rest and in transit) • Multi Tenancy and Segregations • DDoS prevention • Multi Factor Authentication • WAF (Web Application Firewall) • Penetration Tests and Vulnerability Checks • Secured SDLC with automated security testing • Access Control based on least privileges principal with JIT (Just-In-Time) access • Annual Risk Assessment • EDR (Endpoint Detection and Response) • CSPM (Cloud Security Posture Management) • Infrastructure as Code (IaC) for secure deployments • MDM (Mobile Device Management) • Third-Party and Vendor Security Assessments • Business Continuity and Disaster Recovery with defined RPO/RTO • Security awareness training program
Standards	SOC2 Type II GDPR
Policies	SOC2 required policies
Records	All customer data records are encrypted at rest.
Metrics	• Vulnerabilities Data • Employee completion for security trainings • Performance and availability metrics • Device inventory and update • Malware Prevention • Exception tracking
Training and Awareness	Annual Training and Awareness for all employees and subcontractors
Physical and Environmental Safety	According to physical and Environmental Safety policies
Communications Security	According to Transmit Security's Communications Security Policy
Security of Operations	Included in SOC2 policies
Access Control (Physical and logical	Included in SOC2 policies
Acquisition, Development and Maintenance of the software	Included in SOC2 policies
Incident Management	Included in SOC2 policies
Business Continuity	According to company's Business Continuity policy
Procedures	Security, IT, and Engineering Operational Procedures

Appendix 4- EU Standard Contractual Clauses (Controller to Processor)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of and on the free movement of such data (General Data Protection Regulation) for the transfer of Custom 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 Custom Personal Data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the Custom 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 Custom Personal Data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8.1(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 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 Custom Personal Data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I. B.

Clause 7

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

(a) The data importer shall process the Custom 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 Custom 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 Custom 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 Custom 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 Custom 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 Custom 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 Custom 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 "Custom 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 Custom 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 Custom 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 Custom Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a Custom Personal Data breach concerning Custom 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 Custom 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 Custom 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 Custom 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, 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) 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 10 business 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 , 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 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 Custom 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 Custom Personal Data by the data importer, including any requirements to disclose Custom 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 Custom 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 Custom 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 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 Custom 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 transferred pursuant to these Clauses; such notification shall include

information about the Custom 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 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 Custom 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 Custom 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 Custom Personal Data under these Clauses, where:

(i) the data exporter has suspended the transfer of Custom 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) Custom 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 Custom 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 Custom 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 Custom 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 Belgium.

Clause 18

Choice of forum and jurisdiction

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

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

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

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

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name and Address: the name and address of the "Customer" (as defined in the Agreement).

Contact person's name, position and contact details: Customer key contact as communicated by the Customer to Transmit Security in writing from time to time.

Activities relevant to the data transferred: receipt of the Cloud Services provided by Transmit Security pursuant to the Agreement.

Role: controller.

Data importer(s):

Name and Address: Transmit Security, Inc, 201 Washington Street, Suite 2600, Boston, Massachusetts, 02108, United States.

Contact person's name, position and contact details:

Name: Mickey Boodaei

Role: Data Protection Officer

Contact details: privacy@transmitsecurity.com

EU/UK Representative details: Name: Adam Desmond. Contact details: adam.desmond@transmitsecurity.com

Activities relevant to the data transferred: provision of the Services to Customer pursuant to the Agreement.

Role: processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose data is transferred:

The data subjects concerned as identified in Appendix 1 (Processing Details) of the Addendum above.

Categories of Personal Data transferred:

The categories concerned as identified in Appendix 1 (Processing Details) of the Addendum above.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

The special categories of data as identified in Appendix 1 (Processing Details) of the Addendum above.

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

Continuous.

Nature of the processing:

The nature of the processing as identified in Appendix 1 (Processing Details) of the Addendum above.

Purpose(s) of the data transfer and further processing:

The purpose of the processing as identified in Appendix 1 (Processing Details) of the Addendum above.

The period for which the Custom Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:

The duration of the processing as identified in Appendix 1 (Processing Details) of the Addendum above.

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

The subject matter, nature and duration of processing as identified in Appendix 1 (Processing Details) of the Addendum above.

C. COMPETENT SUPERVISORY AUTHORITY

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

As determined in accordance with Clause 13.

ANNEX II

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

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

The technical and organisational measures as identified in Appendix 3 (Technical and Security Measures) of the Addendum above.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorized the use of the following sub-processors: the Sub-Processors as identified in Appendix 2 (Sub-Processors & Sub-Contractors) of the Addendum above.

Appendix 5
EU Standard Contractual Clauses (Processor to Controller)
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)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 13;

(iv) Clause 15.1(c), (d) and (e);

(v) Clause 16(e);

(vi) Clause 18.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies

(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

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

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

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

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

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

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data,[2] the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

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

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

8.3 Documentation and compliance

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

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

Clause 10

Data subject rights

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

Clause 11

Redress

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

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

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

---

[2] This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[3];

(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 15(d) and (e) shall apply.

---

[3] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Clause 15

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

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

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

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

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

(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 13(e) and Clause 15 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 13(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 13(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 collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Belgium.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Belgium.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name and Address: the name and address of the applicable Transmit Security entity as set out in the Agreement.

Contact person's name, position and contact details:

Name: Mickey Boodaei

Role: Data Protection Officer

Contact details: privacy@transmitsecurity.com

EU/UK Representative details: Name: Adam Desmond. Contact details: adam.desmond@transmitsecurity.com

Activities relevant to the data transferred: provision of the Identity Network services provided by Transmit Security pursuant to the Agreement

Role: processor.

Data importer(s):

Name and Address: The name and address of the "Customer" (as defined in the Agreement)

Contact person's name, position and contact details: Customer key contact as communicated by the Customer to Transmit Security in writing from time to time.

Activities relevant to the data transferred: receipt of the Identity Network services provided by Transmit Security pursuant to the Agreement

Role: controller.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose data is transferred:

The data subjects concerned as identified in Appendix 1 (Processing Details) of the Addendum above; end users of other customers.

Categories of Personal Data transferred:

The categories concerned as identified in Appendix 1 (Processing Details) of the Addendum above.

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):

Continuous.

Nature of the processing:

Transmit Security will process and transfer Personal Data to Customer as necessary to perform the Cloud Services contracted by the Customer under the Agreement, and as further instructed by Customer in accordance with the Agreement, the Order Form, and the Addendum.

Purpose(s) of the data transfer and further processing:

Transmit Security will process and transfer Personal Data to Customer as necessary to perform the Cloud Services contracted by the Customer under the Agreement, and as further instructed by Customer in accordance with the Agreement, the Order Form, and the Addendum. **The period for which the Custom Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:**

The parties will process Personal Data for the duration of the Agreement (or as otherwise agreed by the parties in writing), and in accordance with the parties' retention obligations under this Addendum, the Agreement and the applicable provided that Personal Data shall not be processed for longer than is necessary for the purpose for which it was collected or is being processed (except where a statutory exception applies).

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

The subject matter, nature and duration of processing as identified in Appendix 1 (Processing Details) of the Addendum above.

Appendix 6 - International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

The Parties confirm that the UK Addendum to the EU Standard Contractual Clauses (or "**Clauses**") as set out and populated below (**"UK Addendum"**) shall apply to the transfer of End User Personal Data originating from the UK to (a) Transmit Security as Processor in the US or (b) to Customer as Controller, and by executing the EU Standard Contractual Clauses and this UK Addendum, the Parties agree to be bound by the UK Addendum. Unless expressly stated below, any optional clauses contained within the UK Addendum shall not apply. The Parties shall work together, in good faith, to enter into any updated version of the UK Addendum as issued by the Information Commissioner's Office from time to time or negotiate an alternative solution to enable transfers of Custom Personal Data originating from the UK to Transmit Security in the US in compliance with UK Data Protection Laws and related binding guidance issued by the Information Commissioner's Office.

Background:

This Addendum has been issued by the Information Commissioner for the 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

Start Date

The UK Addendum is effective from the date the Addendum comes into force.

Table 1: Parties

Controller to Processor

Exporter and key contact	As set out in Annex I of the EU Standard Contractual Clauses in Appendix 4
Importer and key contact:	As set out in Annex I of the EU Standard Contractual Clauses in Appendix 4

Processor to Controller

Exporter and key contact	As set out in Annex I of the EU Standard Contractual Clauses in Appendix 5
Importer and key contact:	As set out in Annex I of the EU Standard Contractual Clauses in Appendix 5

Table 2: Selected SCCs, Modules and Clauses

Controller to Processor

Addendum EU SCCs	Module 2 of the EU Standard Contractual Clauses as set out in Appendix 4

Processor to Controller

Addendum EU SCCs	Module 4 of the EU Standard Contractual Clauses as set out in Appendix 5

Table 3: Appendix Information

As set out in Annex I and Annex II of the of the EU Standard Contractual Clauses in Appendices 4 and 5

PART 2

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 I.A 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 Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs as set out in Appendix 4, including the Appendix Information.
Appendix Information	As set out in Annex I to the Standard Contractual Clauses included in Appendix 4.
Appropriate Safeguards	The standard of protection over the Custom 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 Custom 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 EU 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 Custom 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 Custom 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 Custom 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, and the Processor 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 the Processor has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then the Processor may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the Controller 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.