CHATLIO LLC ("SERVICE PROVIDER") DATA PROCESSING ADDENDUM ("DPA")

Effective Date: _____

This DPA is incorporated into the Terms of Service (the "Agreement") between _____ ("Company") and Service Provider. The DPA applies to all Processing of Customer Personal Data by Service Provider under the Agreement. Should there be a conflict between this DPA and the Agreement, this DPA will govern.

1 Definitions. In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1 **"Applicable Laws"** means all statutes, laws, rules, regulations, ordinances, and the like of any federal, international, city, state, provincial, or local government or governmental agency applicable to Services under the Agreement including without limitation Data Protection Laws.

1.2 **"Confidential Information"** is defined in the Agreement.

1.3 **"Customer Personal Data"** means any Personal Data provided by or made available by Customer to Service Provider or collected by Service Provider on behalf of Customer, which Service Provider Processes to perform the Services.

1.4 **"Data Breach"** means unauthorized acquisition of, access to, disclosure of, or use of, Customer Personal Data.

1.5 **"Data Protection Laws"** means Applicable Laws relating to privacy, security, or protection of Personal Data, as may be defined by such laws, including, for example and to the extent applicable, the EU General Data Protection Regulation (Regulation 2016/679) ("GDPR"); the California Consumer Protection Act ("CCPA"), regulations and official guidance adopted thereunder, and any subsequent supplements, amendments, or replacements to the same.

1.6 **"Data Subject"** means an identified or identifiable natural person about whom Personal Data is Processed under this Agreement or as otherwise defined (including under similar terms such as "consumer") under Data Protection Laws.

1.7 **"Personal Data"** means data that that relates to an identified or identifiable natural person or as otherwise defined under Data Protection Laws.

1.8 **"Process, processed, or processing"** means the collection, receipt, recording, organization, structuring, alteration, use, transmission, access, sharing, provision, disclosure, distribution, copying, transfer, storage, management, retention, deletion, combination, restriction, summarizing, aggregation, correlation, inferring, derivation, analysis, adaptation, retrieval, consultation, destruction, disposal, or other handling of Personal Data.

1.9 **"Sell"** or **"selling"** means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's Personal Data to another business or a third party for monetary or other valuable consideration.

1.10 **"Services"** means services provided by Service Provider under the Agreement and all schedules, order forms, and statements of work thereunder.

1.11 **"Share"** or **"sharing"** means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data to a third party for cross-context behavioral advertising (as that term is defined in the CCPA), whether or not for monetary or other valuable consideration.

1.12 **"Sub-processor"** means any person or entity engaged by Service Provider that Processes Customer Personal Data.

1.13 The terms "**Controller," "Processor," "Data Processor,"** and **"Business,"** shall have the same meaning as in Data Protection Laws.

2 Data Ownership/Licenses

2.1 **Ownership.** For purposes of this DPA, as between the parties, Customer retains all right, title, and interest in Customer Personal Data.

2.2 **License.** Subject to its compliance with the Agreement and DPA, Customer grants to Service Provider a worldwide, perpetual, fully paid-up right and license under all applicable intellectual property laws to make, use, copy, distribute, display, organize, create derivative works from, and otherwise Process, the Customer Personal Data, and to sublicense all the foregoing rights to Sub-processors, as necessary for the Services, rights, and obligations under the Agreement and this DPA.

3 Scope of Processing

3.1 **Roles of Parties.** The parties acknowledge and agree that with respect to processing of Customer Personal Data, Service Provider is a Processor and a service provider (as that term is defined in Data Protection Laws) and Customer is a Controller and Business, except that if Customer is a Processor in which case Service Provider is a Sub-processor. If Customer is a Processor of Customer Personal Data, Customer represents and warrants that Customer's instructions and Processing of Customer Personal Data, including its appointment of Service Provider as a Sub-processor, have been authorized by the respective Controller.

3.2 **Details of Processing.** Exhibit 1 to this DPA (Description of Processing and Transfer Details) provides information about the subject matter and details of the Processing of Personal Data.

3.3 **Customer Instructions and Restrictions on Processing**

3.3.1 **Instructions.** Service Provider will use, retain, and disclose Company Personal Data solely for the specific business purpose of providing the Services and in accordance with Customer's instructions, which are as set forth in the Agreement, DPA, and other agreements between the parties for the Services. Service Provider will inform Customer if any of Customer's instructions infringes any Data Protection Laws.

3.3.2 **Processing by Service Provider.** Service Provider will Process Customer Personal Data in compliance with Data Protection Laws.

3.3.2.1 Service Provider will not:

3.3.2.1.1 Sell or Share Customer Personal Data;

3.3.2.1.2 use, retain, or disclose Customer Personal Data outside of its direct business relationship with the Customer;

3.3.2.1.3 use, retain, or disclose Company Personal Data for any other purpose (including any other commercial purpose) other than as set forth in the Agreement and DPA, except as authorized by Customer or as required by law or by order of a court or authorized governmental agency (provided that prior notice first be given to the Customer unless such notice is prohibited by law or court order); or

3.3.2.1.4 combine Customer Personal Data with Personal Data that it (a) receives from or on behalf of third parties, or (b) collects from Service Provider's own interactions with Data Subjects unrelated to the Services.

3.3.2.2 Service Provider may Process Customer Personal Data:

as necessary or appropriate:

3.3.2.2.1 to perform its rights and obligations under the Agreement and this DPA;

3.3.2.2.2 to operate, manage, test, maintain and enhance the Services including as part of its business operations;

3.3.2.2.3 to deidentify or aggregate Customer Personal Data in a manner that prevents individual identification of the Customer, or Data Subjects; and

3.3.2.2.4 protect the Service from a threat to the Services, Customers, Customer Personal Data, and Service Provider's systems.

3.3.2.2.5 as otherwise expressly authorized by the Customer.

3.3.3 **Employees and Agents**. Service Provider will take commercially reasonable steps so that all Service Provider employees, contractors, and Sub-processors that Process Customer Personal Data are subject to written confidentiality agreements that provide substantially the same level of protection for Company Personal Data as provided in this DPA and as required by Data Protection Laws.

3.3.4 **Unauthorized Processing**. Customer may take reasonable and appropriate steps to stop unauthorized Processing of Company Personal Data, including without limitation, by instructing Service Provider to cease any such Processing.

3.3.5 **Deidentification**. Where Service Provider is permitted by applicable Data Protection Law or this DPA to use Customer Personal Data for its internal business purposes in a de-identified manner, Service Provider agrees to take reasonable measures designed to ensure that the Personal Data cannot be associated with an individual (or, household, where applicable), publicly commits to maintain and use the information in de-identified form only and make no attempt to re-identify the information except where necessary to test its de-identification processes, and contractually obligates any authorized recipients to comply with these obligations.

4 Data Security

4.1 **Data Security Obligations.** Service Provider will implement and maintain commercially reasonable administrative, technical, and physical safeguards, as described in Exhibit 2.

4.2 **Data Breach.**

4.2.1 If Service Provider learns of a Data Breach affecting Customer Personal Data, Service Provider shall take reasonable, appropriate, and prompt steps to: (a) investigate, mitigate, and remedy the Data Breach; (b) notify Customer of such Data Breach without unreasonable delay consistent with timing under applicable laws; (c) furnish to Customer necessary and relevant details of the Data Breach as may be available; (d) assist Customer, as needed, in its investigation, mitigation, and remedying of the Data Breach; and (e) provide information and assist Customer, as needed, in meeting Customer's legal obligations, including any applicable obligations to notify individuals affected by the Data Breach.

4.2.2 Unless prohibited by Applicable Laws or court order, Service Provider will notify Customer if Service Provider learns of any third-party legal process relating to any Data Breach, including, but not limited to, any legal process initiated by any governmental entity.

4.2.3 Service Provider's cooperation or obligation to report or respond to Data Breaches under this DPA shall not be deemed an acknowledgment by Service Provider of any fault or liability of Service Provider with respect to a Data Breach.

4.2.4 Service Provider shall not be identified in any notifications provided publicly or to third parties (such as to government entities or Data Subjects) unless the contents of the notifications are approved by Service Provider. Service Provider agrees to cooperate in promptly reviewing any notifications and will not unreasonably withhold approval. If such reviews and approvals are expressly prohibited by Applicable Law, Customer can provide them without review and approval.

4.3 **Security Audit.** If and to the extent Service Provider processes, handles, distributes or otherwise makes available, or stores Customer Personal Data as part of the Services, then Service Provider will respond in writing to a security questionnaire as requested by Customer no more than once annually. Customer agrees to treat such information provided by Service Provider in response to request under this Section 4.3 as Service Provider's Confidential Information.

5 **Data Protection Audits and Assistance.** Upon Customer request, but no more than once per year, Service Provider will provide reasonable assistance and information to Customer regarding its Processing of Customer Personal Data to support compliance with its obligations and data protection impact assessments, where the information sought is not provided in the Agreement or this DPA or otherwise accessible to Customer. Service Provider will also provide reasonable assistance and information to Customer to support responses to regulatory enquiries and Data Subject Rights where such means and assistance are not provided in the Agreement or this DPA or otherwise accessible to Customer. No more than once annually, Service Provider will respond in writing to a security questionnaire as requested by Customer.

6 Notice Regarding Third Party Requests and Inquiries Service Provider will take reasonable steps to notify Customer if Service Provider receives the following in connection with its Processing of Customer Personal Data: (i) any requests from a Data Subject, including individual opt-out requests, requests for access and/or deletion and all similar individual rights requests; or (ii) any request from a government entity or regulator provided such notice is not prohibited by law or court order]/[any

request from a government entity or regulator that pertains directly to its Processing of Customer Personal Data, provided such notice is not prohibited by law or court order.

7 Sub-processors

7.1 **Approved Sub-Processors.** Customer authorizes access or transfer to Service Provider's Sub-processors**.** At present, the Sub-processors Service Provider uses are listed at https://chatlio.com/legal/chatlio-subprocessors/. Service Provider will provide ten (10) calendar days' notice before utilizing a new Sub-processor by posting an update to the list at https://chatlio.com/legal/chatlio-subprocessors/. Customer authorizes Service Provider to use any such Sub-processor to process Customer Personal Data unless Customer objects within ten (10) calendar days of such notification. Any such objection must be based on reasonable grounds that any such Sub-processor is unable to adequately protect the Customer Personal Data in accordance with the Agreement. If such objection is justified, Customer and Service Provider will work together to find a mutually acceptable resolution to such objection, and if unsuccessful, Customer's sole remedy is termination of the relevant Services under the terms of the Agreement.

7.2 **Responsibility.** Service Provider will have a written agreement in place with each Sub-processor that obligates the Sub-processor to Process Customer Personal Data in a manner that is no less protective than the obligations on Service Provider under this DPA. Where Sub-processor fails to fulfil its obligations under any sub-processing agreement or Data Protection Laws, Service Provider will remain liable to Customer for the fulfilment of its obligations under this DPA and the Agreement.

8 **Location of Processing.** Service Provider will only process Customer Personal Data in the locations detailed at https://chatlio.com/legal/chatlio-subprocessors/

9 **Cross-Border Data Transfers.** With regard to countries, regions, or territories with Data Protection Laws requiring a mechanism for valid export of Customer Personal Data (such countries, regions, or territories, are "Limited Transfer Region(s)" and such data is "Limited Transfer Data"), Service Provider may not transfer, export, receive, or Process such Limited Transfer Data outside of such Limited Transfer Regions unless it or its Sub-processors take measures to adequately protect such data consistent with applicable Data Protection Laws. Such measures may include (to the extent consistent with Data Protection Laws):

9.1 Processing Customer Personal Data in a country, a territory, or one or more specified jurisdictions that are considered under Data Protection Laws as providing an adequate level of data protection);

9.2 The parties' agreement to enter into and comply with the Standard Contractual Clauses in Exhibit 4 and any successors or amendments to such clauses or such other applicable contractual terms adopted and approved under Data Protection Laws;

9.3 Processing in compliance with Binding Corporate Rules in accordance with Data Protection Laws;

9.4 Implementing any other data transfer mechanisms or certifications approved under Data Protection Laws, including, as applicable, any approved successor or replacement to the EU–US Privacy Shield framework and/or the Swiss–US Privacy Shield framework; or

9.5 To the extent that any substitute or additional appropriate safeguards or mechanisms under any Data Protection Laws of Limited Transfer Regions are required to transfer Customer Personal Data from a Limited Transfer Region, as applicable, to any third country, the parties agree to implement the same as soon as practicable and document such requirements for implementation in an attachment to this DPA governing the parties' Processing of Limited Transfer Data.

10 **Retention and Deletion of Customer Personal Data.** Upon Customer's written request, or upon termination or expiration of the Agreement, Service Provider will return or delete all Customer Personal Data under Service Provider's possession or control or provide Customer ability to delete such Customer Personal Data directly through tools or functionality made available by Service Provider. Service Provider will not delete to the extent that: (a) deletion is not permitted under Applicable Laws or the order of a governmental or regulatory body; (b) where Service Provider retains such data for internal record keeping, compliance with any legal obligations, and other lawfully permitted purposes; or (c) while Service Provider's then-current data retention or similar back-up system stores Customer Personal Data provided such data will remain protected in accordance with the measures described in the Agreement and this DPA.

11 **General Terms**

11.1 **Notices**. All notices under this DPA will be effective when delivered as stated in the Agreement.

11.2 **Termination and Survival. This DPA can be terminated as set forth in the Agreement**. The provisions of this DPA that, by their terms, require performance after the termination or expiration of this DPA, or have application to events that may occur after the termination or expiration of this DPA, will survive the termination or expiration of this DPA, including the order of precedence, and Sections 1 and 10

11.3 **Governing Law; Conflicts of Law; Severance.** The parties to this DPA agree to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims relating to or arising under this DPA; and this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement (without reference to its conflict of laws requirements), unless otherwise required by Data Protection Laws. To the extent any court or governmental entity with competent jurisdiction determines that a provision of this DPA is invalid or unenforceable, the parties agree and intend that such provision should be (a) amended solely as necessary to bring it back into force in a manner consistent with the parties' manifest intent, or if that is not possible (b) severed from the DPA in a manner to give maximum legal force and effect to the remaining provisions.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Agreement with effect from the date specified at the beginning of this DPA.

[Customer]

Signature _____

Name _____

Title _____

Date Signed _____

Chatlio LLC

Signature _____

Name _____

Title _____

Date Signed _____

EXHIBIT 1

DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This Exhibit 1 supplements the Agreement and DPA, and together, provide details about Company Personal Data processing by Service Provider.

Describe the Customer Business Purpose, including the nature and purpose of the Processing of Customer Personal Data. "Customer Business Purpose" is the purpose for which Customer is authorizing Service Provider to Process Company Personal Data in connection with providing the Services to Company, as further described in the Agreement and Exhibit 1 to this DPA.

Providing website chat functionality built on Slack.

The types of Customer Personal Data to be Processed

Contact information such as email address, documents and other data in electronic form provided in the context of the Services.

The types of Sensitive Customer Personal Data to be Processed

No Sensitive Customer Personal Data will be processed.

The categories of Data Subjects to whom the Customer Personal Data relates

Customer's representatives and end users including visitors to Customer's websites, contractors, employees, and other customers of Customer.

The frequency of the transfer of Customer Personal Data from Customer to Service Provider

Continuous basis.

Duration of the Processing of Customer Personal Data

The term of the Services Agreement, unless the parties agree otherwise in writing.

The obligations and rights of Customer

The obligations and rights of Customer are set out in the Agreement and this DPA.

EXHIBIT 2

INFORMATION SECURITY MEASURES

Service Provider's personnel will not process Customer Personal Data without authorization. Personnel are obligated to maintain the confidentiality of any Customer Personal Data and this obligation continues even after their engagement ends.

The technical and organizational measures implemented by Service Provider to provide an appropriate level of security include:

Measures of pseudonymization and encryption of personal data

Data is encrypted in-transit using TLS. Where applicable, data is encrypted at rest within the product(s) by AWS.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Chatlio uses vulnerability assessment, patch management, threat protection technologies, and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses, and other malicious code.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Business resiliency/continuity and disaster recovery procedures are in place, as appropriate, and are designed to maintain service and/or recovery from foreseeable emergency situations or disasters. Our production database has automatic backups enabled and backups are encrypted.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Chatlio uses multiple types of automated vulnerability scans and assessments which are run at various frequencies (e.g. when code changes occur, daily, weekly, and monthly). Additionally, we have third-party penetration tests ran and allow for vulnerabity reports to be submitted securely to us for evaluation.

Measures for user identification and authorization

Chatlio uses logical access controls designed to allocate appropriate privileges according to role, applying the principle of least privilege access. Chatlio applies a zero-trust model of identification and authorization. In addition, all Employees are required to use password manager and unique passwords and strong multi-factor authentication, including requiring the use of two-factor authentication (2FA) for all Chatlio accounts. We perform periodic review of Employees access and promptly revoke access when employment terminates.

Measures for the protection of data during transmission

Chatlio implements effective measures to protect Personal Data from being read, copied, altered or deleted by unauthorized parties during transmission, including by implementing protective measures against active and passive attacks on the sending and receiving systems providing transport encryption, such as adequate firewalls, mutual TLS encryption, API authentication, and encryption to protect the gateways and pipelines through which data travels, as well as testing for software vulnerabilities.

Measures for the protection of data during storage

Where applicable, data is encrypted within the product(s) by AWS.

Measures for ensuring physical security of locations at which personal data are processed

Physical and environmental controls are inherited from Amazon Web Services, Inc. (AWS)

Measures for ensuring events logging

Chatlio has system audit and event logging and related monitoring procedures in place to record user access and system activity. Automated analytics are used to generate alerts for suspicious or potentially malicious activity.

Measures for ensuring system configuration, including default configuration

Chatlio configuration is stored in the environment for maximum portability between environments using the twelve-factor app methodology. Baseline configuration is enforced with a default configuration set.

Measures for internal IT and IT security governance and management

Chatlio uses network security controls that provide for the use of enterprise firewalls (AWS and Cloudflare) and layered DMZ architectures, as well as intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of an attack.

Change management controls and procedures are established to ensure human review of production changes is performed to identify potential security issues before changes are made.

Measures for certification/assurance of processes and products

Chatlio regularly reviews its processes on an annual or as-needed basis.

Measures for ensuring data minimisation

Chatlio ensures data minimisation by processing only that data which is relevant and necessary for the provision of the service.

Measures for ensuring data quality

Chatlio will monitor data processed and any inaccuracies will be erased or modified without delay. Chatlio also monitors IP addresses for abuse and spam and will block any traffic originating from abusive IP blocks.

Measures for ensuring limited data retention

Chatlio only collects personal data that is absolutely necessary to fulfill a purpose. The data collected and the time it is stored is reviewed internally on an as-needed basis. Chatlio deletes personal data on request from customer.

Measures for ensuring accountability

Chatlio has defined roles and responsibilities within the company designed towards ensuring the confidentiality, integrity and availability of Personal Data. These roles and responsibilities are reviewed annually to ensure continued efficacy and compliance with Applicable Privacy Laws. Chatlio employs least privilege access mechanisms to control access to Personal Data. Role-based access controls are employed to ensure that access to Personal Data required for the provision, maintenance and securing of the Services is for an appropriate purpose and approved with management oversight.

Measures for allowing data portability and ensuring erasure

Data subject request processes are in place to handle erasure and data portability requests. Customers may reach out to privacy@chatlio.com in order to exercise their rights.

EXHIBIT 3
SUB-PROCESSORS

The Sub-processors authorized to Process Customer Personal Data are listed at https://chatlio.com/legal/chatlio-subprocessors/.

EXHIBIT 4

STANDARD CONTRACTUAL CLAUSES

1 **EEA Personal Data Transfers.** Limited Transfer Data subject to the GDPR that Customer transfers to Service Provider will be governed by Module Two ("Controller to Processor") and Module Three ("Processor to Processor") of the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as issued by the European Commission on June 4, 2021, and as also adopted by the Swiss Federal Data Protection and Information Commissioner ("FDPIC") (collectively "EU SCCs"), as applicable and as described herein. The elections and information required for the purposes of the EU SCCs is provided in Section 5 below and in Exhibit 1 to the DPA. The Parties agree that the EU SCCs are incorporated into this DPA without further need for reference, incorporation, or attachment and that by executing the DPA, each party is deemed to have executed the EU SCCs.

2 **Swiss Personal Data Transfers.** Limited Transfer Data subject to the Swiss Federal Data Protection Act ("Swiss DPA") that Customer transfers to Service Provider will be governed by the EU SCCs with the following modifications:

2.1 References to "Regulation (EU) 2016/679" and any articles therefrom shall be interpreted to include references to the Swiss DPA.

2.2 References to "EU," "Union" and "Member State" shall be interpreted to include references to "Switzerland."

3 **UK Personal Data Transfers.** Limited Transfer Data subject to the UK GDPR and UK Data Protection Act 2018 that Customer transfers to Service Provider will be governed by the EU SCCs and UK Transfer Addendum Version B1.0 (in force 21 March 2022) adopted by the UK Information Commissioner's Office (the "UK Transfer Addendum"). The Parties agree as follows:

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

3.2 The EU SCCs will be interpreted in accordance with Part 2 of the UK Transfer Addendum.

3.3 Sections **Error! Reference source not found.** to **Error! Reference source not found.** of the UK Transfer Addendum override Clause 5 (Hierarchy) of the EU SCCs.

3.4 For the purposes of Section 12 of the UK Transfer Addendum, the EU SCCs will be amended in accordance with Section 15 of the UK Transfer Addendum.

3.5 Information required by Part 1 of the UK Transfer Addendum is provided as Exhibit 1 to the DPA.

3.6 To the extent that any revised transfer addendums or mechanisms are issued by the UK ICO, the Parties agree to incorporate such revisions in accordance with Section 18-20 of the UK Transfer Addendum.

3.7 The Parties agree that the UK Transfer Addendum is incorporated into this DPA without further need for reference, incorporation, or attachment and that by executing the DPA, each

party is deemed to have executed the UK Transfer Addendum.

4 **Other Limited Transfer Region Transfers.** Limited Transfer Data that is not subject to the GDPR, Swiss DPA, or UK Data Protection Law, and that Customer transfers to Service Provider, will be governed by the EU SCCs with the following modifications: references to the General Data Protection Regulation will be replaced by applicable Data Protection Laws of the respective Limited Transfer Regions and for Clause 13 references to EU Member State shall be replaced with the applicable Limited Transfer Region.

5 **EU SCC and UK Transfer Addendum Information.**

SCC Clause	**GDPR**	**Swiss DPA**	**UK Data Protection Law**
Module in Operation **Module Two (Controller to Processor) and Module Three (Processor to Processor)**			
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.		
Clause 9(a)- Use of Sub-processors	GENERAL WRITTEN AUTHORISATION: The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.		
Clause 11 (Redress)	Optional language in Clause 11 shall not apply.		
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 Republic of Ireland.	These Clauses shall be governed by the law of Switzerland, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Switzerland.	These Clauses shall be governed by the law of the United Kingdom, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of England and Wales.

Clause 18 – Choice of Forum and Jurisdiction	The parties agree that those shall be the courts of Republic of Ireland.	The parties agree that those shall be the competent courts of Switzerland.	The parties agree that those shall be the competent courts of England and Wales.
Appendix, Annex I.A- List of Parties	The name, address, and contact person's name, position, and contact details, and each party's role in Processing Personal Data are as set forth in the DPA and Exhibit 1 to the DPA to which this Exhibit 4 is attached.		
Annex I>B – Description of Transfer	This information can be found in Exhibit 1 to the DPA to which this Exhibit 4 is attached. To the extent applicable, the descriptions of safeguards applied to the special categories of Personal Data can be found Exhibit 2 to the DPA to which this Exhibit 4 is attached.		
Clause 13 and Annex I>C – Competent Supervisory Authority	Identify the competent supervisory authority/ies in accordance with Clause 13: _____	Identify the competent supervisory authority/ies in accordance with Clause 13: FDPIC	Identify the competent supervisory authority/ies in accordance with Clause 13: UK Information Commissioner
Annex II – Technical and Organizational Measures	The description of technical and organization measures designed to ensure the security of Personal Data is in Exhibit 2 to the DPA to which this Exhibit 4 is attached.		
Annex II – Technical and Organizational Measures – Subprocessors	The description of technical and organization measures designed to ensure the security of Personal Data are described more fully Exhibits 2-3 to the DPA to which this Exhibit 4 is attached.		
Annex III – List of Subprocessors	As described in Exhibit 3 to the DPA to which this Exhibit 4 is attached.		
Ending the UK Transfer Addendum when the Approved Addendum changes	N/A		Which Parties may end this Addendum as set out in Section **Error! Reference source not found.**: ☒ Importer ☒ Exporter ☐ neither Party