Supplier Data Protection Addendum

Last Updated: December 7, 2022

This Supplier Data Protection Addendum ("***Addendum***") supplements the agreement between Twilio and Supplier into which it is incorporated by reference ("***Agreement***").

I. Introduction

1. Definitions.

Any capitalized term used but not defined in this Addendum has the meaning provided to it in the Agreement.

- *"**Applicable Data Protection Law**"* refers to all laws and regulations applicable to either party's processing of personal data under the Agreement.
- *"**controller**"* means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- *"**personal data**"* means any information relating to an identified or identifiable natural person ("***data subject***"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- *"**processor**"* means the entity which processes personal data on behalf of the controller.
- *"**processing**"* (and "***process***") means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- *"**Privacy Policy**"* means the applicable then current Twilio privacy policy available https://www.twilio.com/legal/privacy; or https://www.twilio.com/legal/employee-privacy.
- *"**Supplier Data**"* means any personal data Twilio receives from Supplier under the Services.
- *"**Security Incident**"* means a confirmed or reasonably suspected accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Twilio Data.
- *"**Services**"* means Supplier's services as outlined in the Agreement.
- *"**Standard Contractual Clauses**"* has the meaning set forth in Schedule 3 (Cross Border Transfer Mechanisms) of this Addendum.
- *"**sub-processor**"* means any third-party engaged by Supplier to process Twilio Processor Data.
- *"**Third Party Request**"* means any request, correspondence, inquiry, or complaint from a data subject, regulatory authority, or third party.
- *"**Twilio Controller Data**"* means any personal data that Supplier processes as a controller subject to Section 2.2 and 4.
- *"**Twilio Data**"* means any data Supplier received from Twilio during the provision of the Services, including Personal Data. Twilio Data includes Twilio Controller Data and Twilio Processor Data.
- *"**Twilio Processor Data**"* means any Twilio Data that is not Twilio Controller Data.

II. Controller and Processor

2. Relationship of the Parties.

2.1 Supplier as a processor of Twilio Data. The parties acknowledge and agree that with regard to the processing of Twilio Processor Data, Twilio is a controller and Supplier is a processor. Supplier will process Twilio Processor Data in accordance with Twilio's instructions as set forth in Section 5 (Twilio Instructions).

2.2 Supplier as a Controller of Twilio Data. The parties acknowledge that Supplier may act as an independent controller of Twilio Data where necessary to provide the Services under an applicable Statement of Work or Purchase Order (and for clarity, not as a joint controller with Twilio). Where Supplier processes Twilio Controller Data, it shall only do so only (a) as set forth in an applicable Statement of Work or Purchase Order and as necessary

to provide the Services to Twilio; (b) as necessary to comply with applicable law or regulation, including Applicable Data Protection Law; and (c) as otherwise agreed in writing between the parties.

2.3 Twilio as a Controller of Supplier Data. The parties acknowledge and agree that with regard to the processing of Supplier Data, Supplier is a controller and Twilio is an independent controller, not a joint controller with Supplier. Twilio will process Supplier Data as permitted under Applicable Data Protection Law and in accordance with this Addendum, the Agreement, and the Privacy Policy.

3. Purpose Limitation. Supplier will process personal data in order to provide the Services in accordance with the Agreement. Schedule 1 (Details of Processing) of this Addendum further specifies the nature and purpose of the processing, the processing activities, the duration of the processing, the types of personal data and categories of data subjects.

4. Compliance.

4.1 General Compliance. Each party shall comply with its obligations under Applicable Data Protection Law, and this Addendum, when processing personal data. Supplier additionally warrants that Supplier obtained all necessary rights, consents, and permissions to collect, process, share, use and transfer Supplier Data as contemplated in this Agreement, including but not limited to, Twilio's marketing, sales and recruiting purposes. Upon request, Supplier shall make available any and all records, disclosures or documentation relating to such consents or other authorisations obtained by Supplier.

4.2 CCPA compliance. To the extent that the processing of personal data under the Agreement is subject to the California Consumer Privacy Act ("**CCPA**") Supplier shall (i) comply with the obligations applicable to it under the CCPA; (ii) provide personal data with the same level of privacy protection as is required by the CCPA; and (iii) notify Twilio if it makes a determination that it can no longer meet its obligations under the CCPA.

III. Supplier as a Processor of Twilio Data

5. Twilio Instructions.

5.1 Instructions. Twilio appoints Supplier as a processor to process Twilio Processor Data on behalf of, and in accordance with, Twilio's instructions (a) as set forth in the Agreement, this Addendum and as necessary to provide the Services to Twilio, and (b) as otherwise agreed in writing between the parties. Supplier is prohibited from selling or sharing Twilio Processor Data, or retaining, using, or disclosing Twilio Processor Data (i) for any purpose other than those outlined in this section, including retaining, using, or disclosing Twilio Processor Data for any other commercial purpose; or (ii) outside of the direct business relationship between the parties. Supplier shall not combine personal data that it receives from, or on behalf of, Twilio with personal data that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, except on the instruction of Twilio. Supplier certifies that it understands these prohibitions and will comply with them.

6. Confidentiality.

6.1 Responding to third party requests. In the event any third party request is made directly to Supplier in connection with Supplier's processing of Twilio Processor Data, Supplier will promptly inform Twilio and provide details of the same, to the extent legally permitted. Supplier will not respond to any Third Party Request without Twilio's prior consent, except as legally required to do so or to confirm that such Third Party Request relates to Twilio.

6.2 Confidentiality obligations of Supplier Personnel. Supplier will ensure that any person it authorizes to process Twilio Data has agreed to protect personal data in accordance with Twilio's confidentiality obligations in the Agreement.

7. Subcontracting. Should Twilio provide a written authorization for Supplier to engage sub-processors to process Twilio Processor Data, any such authorization is conditioned on the following requirements:

(a) Supplier provides Twilio an up-to-date list of all Supplier sub-processors prior to allowing any sub-processor to process personal data. Supplier shall give notice of any change in sub-processors at least thirty (30) days prior to any such change to privacy@twilio.com;

(b) Supplier certifies that it has entered into a written contract that includes terms substantially similar to this Addendum in which Supplier imposes data protection terms that require sub-processors to protect the personal data to the standard required by this Addendum and Applicable Data Protection Law;

(c) Supplier remains liable for any breach of this Addendum that is caused by an act, error or omission of its sub-processor;

(d) Twilio may object to Supplier's appointment or replacement of a sub-processor prior to its appointment or replacement, provided such objection is based on reasonable grounds. In such an event, the parties shall discuss commercially reasonable alternative solutions in good faith. If the parties cannot reach resolution, Supplier will either not appoint or replace the sub-processor or, if this is not possible, Twilio may suspend or terminate the Agreement; and

(e) Supplier conducts appropriate due diligence on its sub-processors.

8. Data Subject Rights. To the extent Twilio, in its ordinary use of the Services, does not have the ability to address a data subject's request to exercise their rights under Applicable Data Protection Law, Supplier shall, upon Twilio's request, provide commercially reasonable assistance to Twilio in resolving any such data subject request.

9. Impact Assessments and Consultations. Supplier shall provide reasonable cooperation to Twilio in connection with any data protection impact assessment or consultations with supervisory authorities that may be required under Applicable Data Protection Law

10. Return or Deletion of Twilio Data. Upon Twilio's request or upon termination of the Agreement, Supplier agrees, at Twilio's option, to either deliver to Twilio or destroy in a manner that prevents Twilio Data from being reconstructed, any Twilio Data and any copies in Supplier's control or possession. Such delivery or destruction shall occur as soon as practicable and in any event within fifteen (15) business days after the effective date of such termination or the date of Twilio's request. Upon reasonable notice and if requested by Twilio, Supplier shall provide Twilio a certificate by an officer of compliance with this Section. This Section shall survive termination of the Agreement.

IV. Security and Audits

11. Security.

11.1 Security Measures. Each party has implemented appropriate technical and organizational measures for ensuring the security of the personal data being processed and will maintain the technical and organizational security measures as set forth in the Agreement. Additional information about the technical and organizational security measures to protect personal data is set forth in Schedule 2 (Technical and Organizational Security Measures).

11.2 Security Incident Notification. Supplier shall, to the extent permitted by law, immediately notify Twilio of any reasonably suspected or actual Security Incident. Notices of a Security Incident should be given within 72 hours to Twilio at security-sirt@twilio.com. The notice shall summarize in reasonable detail the nature and scope of the Security Incident (including the nature of the data and data subjects impacted) and the corrective action already taken or to be taken by Supplier. The notice shall be timely supplemented in the detail reasonably requested by Twilio, inclusive of relevant forensic reports. Unless prohibited by an applicable statute or court order, Supplier shall also notify Twilio of any third-party legal process relating to any Security Incident, including, but not limited to, any legal process initiated by any governmental entity.

11.3 Security Incident Remediation. Supplier shall promptly take all necessary and advisable corrective actions, and shall, at its sole cost and expense, assist Twilio in investigating, remedying, providing notices required by law and taking any other action Twilio deems necessary regarding any Security Incident and any dispute, inquiry or

claim concerning any Security Incident. Supplier shall use best efforts to remedy any Security Incident immediately but no later than within thirty (30) days of discovery of a Security Incident. Supplier's failure to remedy any Security Incident in a timely manner will be a material breach of the Agreement.

11.4 Required Breach Notices. Supplier acknowledges that it is solely responsible for the confidentiality and security of the personal data in its possession, custody or control, or for which Supplier is otherwise responsible. Twilio will decide on whether any notice of breach is legally required to be given to any person, and if so, the content of that notice. Supplier will bear all costs of the notice. If Twilio reasonably determines that the Security Incident is likely to have substantial adverse impact on Twilio's relationship with its customers or associates or otherwise substantially harm its reputation, Twilio may terminate the Agreement.

12. Audits. Subject to reasonable notice, Supplier shall provide Twilio an opportunity to conduct a privacy and security audit of Supplier's security program and systems and procedures that are applicable to the Services. Audits will occur at most annually or following notice of a security incident. If the audit reveals any vulnerability, Supplier shall correct such vulnerability at its sole cost and expense. Supplier shall use best efforts to correct all vulnerabilities immediately. Supplier's failure to complete corrections in a timely manner will be a material breach of the Agreement.

V. International Provisions

13. Processing Locations. Supplier will only process personal data in the locations outlined in Section 7 (Processing Locations) of Schedule 1.

14. Cross Border Data Transfer Mechanisms for Data Transfers. To the extent Twilio's use of the Services requires an onward transfer mechanism to lawfully transfer personal data from a jurisdiction (i.e. the European Economic Area, the United Kingdom or Switzerland) to a recipient in locations outside of that jurisdiction ("***Transfer Mechanism***"), the terms set forth in Schedule 3 (Cross Border Transfer Mechanisms) will apply.

VI. Miscellaneous

15. Cooperation and Data Subject Rights. In the event that either party receives (a) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure, and data portability, as applicable) or (b) any Third Party Request relating to the processing of personal data conducted by the other party as a controller, such party will promptly inform such other party in writing. The parties agree to cooperate, in good faith, as necessary to respond to any Third Party Request and fulfill their respective obligations under Applicable Data Protection Law

16. Conflict. In the event of any conflict or inconsistency among the Agreement, this Addendum, or any applicable Statement of Work regarding Supplier's privacy and security obligations, the provision more protective of personal data shall control.

17. Entire Agreement. This Addendum supersedes and replaces all prior proposals, statements, sales materials or presentations and agreements, oral and written, with regard to the subject matter of this Addendum, including any prior data processing addenda entered into between Twilio and Supplier.

SCHEDULE 1

DETAILS OF PROCESSING

1. Nature and Purpose of the processing.

Supplier or Twilio, as applicable, will process personal data as necessary to, respectively, provide or obtain the benefit of the Services. Supplier does not sell Twilio personal data and does not share such end users' information with third parties for compensation or for those third parties' own business interests.

2. Processing Activities. Personal data will be subject to the processing activities necessary for the provision or to obtain the benefit of the Services, as applicable.

3. Duration of the processing. The period for which personal data will be retained will be for the duration of the Agreement, or earlier, if so requested by Twilio. Where Supplier, as controller, provides personal data to Twilio as an independent controller in connection with the Agreement, the personal data shall be retained for as long as necessary for Twilio to obtain the benefit of the Services.

4. Categories of Data Subjects. Twilio's employees, customers, end users, sales leads or job candidates.

5. Categories of Personal Data. Supplier or Twilio, as applicable, process such categories of personal data as necessary to provide or receive the benefit of the Services, including, without limitation, the categories of personal data specified in the Agreement, Statement of Work or Purchase Order and may include the names, email addresses and other contact details of data subjects.

6. Sensitive Data or Special Categories of Data. Sensitive data is not being processed under the Agreement.

7. Processing locations. The parties shall only process personal data in the countries listed in the table below, or as agreed upon in a separate signed writing between the parties.

Twilio Data

Supplier must only process Twilio Data in any of the following countries:

a) Australia, Bhutan, Brazil, Colombia, Hong Kong, India, Japan, Philippines, Singapore, or the United States; or

b) Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain or Sweden; or

c) Any country the European Union has recognized as providing adequate protection to personal data: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, and Uruguay.

Supplier Data

Twilio may process Supplier Data in any country in which Twilio maintains office locations. Twilio's office locations can be found at https://www.twilio.com/company.

Temporary Workers

Temporary workers provided by Supplier must be located in any of the following countries: Australia, Belgium, Brazil, Canada, Estonia, France, Germany, India, Ireland, Israel, Italy, Japan, Mexico, Netherlands, Poland, Singapore, Spain, Sweden, The United Kingdom, or The United States.

---

8. For transfers to Supplier's sub-processors, the subject matter, nature, and duration of the processing for each approved sub-processor is as necessary for the provision of the Services.

SCHEDULE 2

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

This Schedule 2 details the technical and organizational security measures taken by Twilio and Supplier respectively and as applicable with respect to personal data processed in connection with the Agreement.

TWILIO:

The full text of Twilio's technical and organizational security measures to protect personal data is available at https://www.twilio.com/legal/security-overview ("**Security Overview**").

SUPPLIER:

Supplier has implemented and will maintain the technical and organizational security measures set forth in the table below to protect Twilio Data and personal data it receives from Twilio from Security Incidents. The security measures shall be appropriate to the nature and risk to personal data, and in any event shall not be less stringent than those prescribed under applicable laws. Supplier shall comply with the security requirements laid out in this Schedule 2, which shall be in addition to security obligations in the Agreement. Supplier will not materially decrease the overall security of the Services during the term during which it processes personal data.

Technical and Organizational Security Measure

Evidence of Technical and Organizational Security Measure

Measures of pseudonymisation and encryption of personal data

Supplier maintains Twilio data in an encrypted format at rest using a minimum of AES 256 and in transit using a minimum of TLS 1.2. Supplier pseudonymizes personal data only in accordance with Twilio's instructions.

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

Supplier maintains a risk-based security program. The framework for Supplier's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Twilio data. Supplier's security program is intended to be appropriate to the nature of the Services and the size and complexity of Supplier's business operations. The provision of the Services in particular involves the use of a variety of tools and mechanisms to achieve high availability and resiliency. Supplier leverages specialized tools that monitor server performance, data, and traffic load capacity within each availability zone as applicable. Supplier maintains a security team with sufficient expertise to address the IT security risks arising from the Services.

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

Supplier's availability and backup strategy is designed to ensure replication and fail-over protections in the event of a physical or technical incident. Personal data is backed up and maintained using at least industry standard

methods, and personal data is replicated in at least one secondary database in a separate location to the primary hosting database. Personal data is encrypted in transit and at rest in the backup process as specified above.

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

Supplier maintains industry standard security certifications, subject to regular audits. Examples of such certifications include, but are not limited to, ISO 27001 and SOC 2 Type II. Supplier performs regular penetration tests and engages industry recognised penetration service providers to conduct penetration tests at appropriate levels. Security threats and vulnerabilities that are detected are prioritized, triaged, and remediated promptly.

Measures for user identification and authorisation

Supplier implements industry standard access controls and detection capabilities. Supplier personnel are required to use unique user access credentials and passwords for authorization. Supplier personnel are authorized to access personal data based on their job function, role and responsibilities, and such access requires approval prior to being provided. Access is promptly changed or removed as applicable upon role change or termination.

Measures for the protection of data during transmission

Personal data is encrypted when in transit between Supplier and the Services using secure encryption.

Measures for the protection of data during storage

Stored personal data is encrypted using the encryption standard specified above.

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

Supplier’s servers and office spaces have a physical security program that manages visitors, building entrances, CCTVs (closed circuit televisions), and overall office security. All employees and contractors are required to have approved access cards and visitors are required to be escorted throughout those parts of the premises containing personal data.

Measures for ensuring events logging

Supplier’s security infrastructure logs information with respect to applications, tools and resources that process personal data about system behavior, traffic received, system authentication, and other application requests. Systems aggregate log data and security personnel are alerted and investigate anomalous activities.

Measures for ensuring system configuration, including default configuration

Supplier applies industry standard processes to perform numerous security-related activities for its systems including, without limitation, internal security reviews prior to the deployment of new Services and creating threat models to detect any potential security threats and vulnerabilities. Supplier has a change management process to administer changes to the production environment for the Services, including changes to its underlying software, applications, and systems. Relevant security personnel are notified of changes made to critical infrastructure and services that do not adhere to the change management processes.

Measures for internal IT and IT security governance and management

Supplier maintains a risk-based security program. The framework for Supplier's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of personal data. Supplier's security program is intended to be appropriate to the nature of the Services and the size and complexity of Supplier's business operations. Supplier maintains a security team with sufficient expertise to address the IT security risks arising from the Services. Information security policies and standards are reviewed and approved by management regularly and are made available to all Supplier personnel for reference.

Measures for certification/assurance of processes and products

Supplier conducts regular third-party audits to attest to its security certifications including those certifications specified above. Supplier applies industry standard processes to perform numerous security-related activities for its systems including, without limitation, internal security reviews prior to the deployment of new Services and creating threat models to detect any potential security threats and vulnerabilities. Supplier has a change management process to administer changes to the production environment for the Services, including changes to its underlying software, applications, and systems. Relevant security personnel are notified of changes made to critical infrastructure and services that do not adhere to the change management processes. Security is managed at the highest level of the company with regular meetings by senior management to discuss and coordinate security initiatives company-wide and for new processes and products.

Measures for ensuring data minimisation

Supplier ensures data minimisation in accordance with its instructions from Twilio, data privacy policies and industry standards.

Measures for ensuring data quality

Supplier ensures data quality in accordance with the requirements of the Services and the Agreement.

Measures for ensuring limited data retention

Supplier maintains internal policies to ensure that personal data is not kept for longer than necessary. In accordance with the addendum, Supplier deletes personal data on request from Twilio. This is done using industry standard methods for comprehensive deletion of personal data.

Measures for ensuring accountability

Supplier has adopted measures for ensuring accountability, such as implementing data privacy policies across its business, notifying (where appropriate) Security Incidents involving personal data, and appointing an employee or contractor with primary responsibility for the business' compliance with relevant data privacy obligations. Supplier also conducts regular audits to ensure compliance with its privacy and security standards.

Measures for allowing data portability and ensuring erasure

Supplier specifies in the Addendum that it will provide commercially reasonable assistance to Twilio as may be required to comply with Twilio's obligations under Applicable Data Protection Laws to respond to requests from individuals to exercise their rights under Applicable Data Protection Laws. If Supplier receives a request from a data subject in relation to their personal data, Supplier will provide that request immediately to Twilio, advise the data subject to submit their request to Twilio and provide such structured access or comply with such reasonable instructions from Twilio, as Twilio may reasonably require in order for it to comply with the request for the portability or erasure of personal data.

Technical and organizational measures to be taken by the [sub]-processor to provide assistance to the controller and, for transfers from a processor to a [sub]-processor, to the Customer.

When Supplier engages a sub-processor under this Addendum, Supplier and the sub-processor enter into an agreement with data protection terms substantially similar to those contained herein. Each sub-processor agreement must ensure that Supplier is able to meet its obligations to Twilio. In addition to implementing technical and organizational measures to protect personal data, sub-processors must a) notify Supplier in the event of a Security Incident so Supplier may notify Twilio; b) delete data when instructed by Supplier in accordance with Twilio's instructions to Supplier; c) not engage additional sub-processors without authorization in accordance with this Addendum; d) assist with responses to data subject requests; and e) not process data in a manner which conflicts with Twilio's instructions to Supplier.

SCHEDULE 3

CROSS BORDER DATA TRANSFER MECHANISMS

1. Definitions

- "***2021 Standard Contractual Clauses***" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.
- "***UK IDTA***" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022.

2. Cross Border Data Transfer Mechanisms.

2.1 2021 Standard Contractual Clauses. The parties agree that the 2021 Standard Contractual Clauses will apply to personal data that is transferred via the Services from the European Economic Area or Switzerland, either directly or via onward transfer, to any country or recipient outside the European Economic Area or Switzerland that is not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for personal data. For data transfers from the European Economic Area that are subject to the 2021 Standard Contractual Clauses, the 2021 Standard Contractual Clauses will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

(a) Module One (Controller to Controller) of the 2021 Standard Contractual Clauses will apply where Twilio or Supplier, as controller, are processing personal data originating in the European Economic Area.

(b) Module Two (Controller to Processor) of the 2021 Standard Contractual Clauses will apply where Twilio is a controller and Supplier is processing Twilio Data.

(c) Module Four (Processor to Controller) of the 2021 Standard Contractual Clauses will apply where Twilio is a processor of personal data and Supplier, in its provision of the Services, acts as a controller in respect of that personal data.

(d) For each Module, where applicable:

(i) in Clause 7 of the 2021 Standard Contractual Clauses, the optional docking clause will not apply;

(ii) in Clause 9 of the 2021 Standard Contractual Clauses, Option 2 will apply and the time period for prior notice of sub-processor changes will be as set forth in Section 7(a) (Subcontracting) of this Addendum;

(iii) in Clause 11 of the 2021 Standard Contractual Clauses, the optional language will not apply;

(iv) in Clause 17 (Option 1), the 2021 Standard Contractual Clauses will be governed by Irish law;

(v) in Clause 18(b) of the 2021 Standard Contractual Clauses, disputes will be resolved before the courts of Ireland;

(vi) in Annex I, Part A of the 2021 Standard Contractual Clauses:

Data Exporter and Data Importer: Twilio or Supplier, as applicable.

Contact details: Twilio: privacy@twilio.com; Supplier: Supplier's publicly-available email address for receiving privacy-related notices.

Data Exporter Role: The Data Exporter's role is set forth in Section 2 (Relationship of the Parties) of this Addendum.

Data Importer Role: The Data Importer's role is set forth in Section 2 (Relationship of the Parties) of this Addendum.

Signature and Date: By entering into the Agreement, Data Exporter and Data Importer are deemed to have signed these 2021 Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

(vii) in Annex I, Part B of the 2021 Standard Contractual Clauses:

The categories of data subjects are described in Section 4 of Schedule 1 (Details of Processing) of this Addendum.

The Sensitive Data transferred is described in Section 6 of Schedule 1 (Details of Processing) of this Addendum.

The frequency of the transfer is a continuous basis for the duration of the Agreement or as may otherwise be specified in the Agreement, a Statement of Work or a Purchase Order.

The nature of the processing is described in Section 1 of Schedule 1 (Details of Processing) of this Addendum.

The purpose of the processing is described in Section 1 of Schedule 1 (Details of Processing) of this Addendum.

The period for which the personal data will be retained is described in Section 3 of Schedule 1 (Details of Processing) of this Addendum.

For transfers to sub-processors, the subject matter, nature, and duration of the processing is set forth in Section 7(f) of the Addendum.

(viii) in Annex I, Part C of the 2021 Standard Contractual Clauses: The Irish Data Protection Commission will be the competent supervisory authority.

(ix) Schedule 2 (Technical and Organizational Security Measures) of this Addendum serves as Annex II of the 2021 Standard Contractual Clauses.

(e) For data transfers from Switzerland that are subject to the 2021 Standard Contractual Clauses, the 2021 Standard Contractual Clauses will be deemed entered into (and incorporated into this Addendum by this reference) and completed as set out in Section 2.1(a) - (d) of this Schedule 3 above, subject to the following modifications:

(i) references to "EU Member State" and "Member State" will be interpreted to include Switzerland, and

(ii) insofar as the transfer or onward transfers are subject to the Swiss Federal Act on Data Protection, as revised (FADP):

(1) references to "Regulation (EU) 2016/679" are to be interpreted as references to the FADP;

(2) the "competent supervisory authority" in Annex I, Part C will be the Swiss Federal Data Protection and Information Commissioner;

(3) in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by the laws of Switzerland; and

(4) in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Switzerland.

2.2 UK International Data Transfer Agreement. The parties agree that the UK IDTA will apply to personal data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body as providing an adequate level of protection for personal data. For data transfers from the United Kingdom that are subject to the UK IDTA, the UK IDTA will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

(a) In Table 1 of the UK IDTA, the parties' details and key contact information is located in Section 2.1(d)(vi) of Schedule 3 of this Addendum.

(b) In Table 2 of the UK IDTA, information about the version of the Approved EU SCCs, modules and selected clauses which this UK International Data Transfer Agreement is appended to is located in Section 2.1 of this Addendum.

(c) In Table 3 of the UK IDTA:

1. The list of Parties is located in Section 2.1(d)(vi) of Schedule 3 of this Addendum.

2. The description of the transfer is set forth in Section 1 (Nature and Purpose of the Processing) of Schedule 1 (Details of the Processing) of this Addendum.

3. Annex II is located in Schedule 2 (Technical and Organizational Security Measures) of this Addendum.

(d) In Table 4 of the UK IDTA, both the Importer and the Exporter may end the UK IDTA in accordance with the terms of the UK IDTA.