

Data Processing Addendum

This Data Processing Addendum (“DPA”) supplements the PayStandards Software as a Service Agreement (the “Agreement”) entered into by and between the customer signing this DPA (“Customer”) and PayStandards, Inc. (“Company”). By executing the DPA, whether by signing the DPA or by the DPA’s incorporation into an executed Agreement, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws (defined below), in the name and on behalf of its Affiliates (defined below), if any. This DPA is incorporated into and subject to the terms of the Agreement. Any terms not defined in this DPA shall have the meaning set forth in the Agreement.

1. Definitions

- 1.1. “Affiliate” means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.
- 1.2. “Authorized Sub-Processor” means a third-party who has a need to know or otherwise access Customer’s Personal Data to enable Company to perform its obligations under this DPA or the Agreement, and who is either (1) listed in Exhibit B or (2) subsequently authorized under Section 4.2 of this DPA.
- 1.3. “Company Account Data” means personal data that relates to Company’s relationship with Customer, including the names or contact information of individuals authorized by Customer to access Customer’s account and billing information of individuals that Customer has associated with its account. Company Account Data also includes any data Company may need to collect for the purpose of managing its relationship with Customer, identity verification, or as otherwise required by applicable laws and regulations.
- 1.4. “Company Usage Data” means Service usage data collected and processed by Company in connection with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.
- 1.5. “Data Exporter” means Customer.
- 1.6. “Data Importer” means Company.
- 1.7. “Data Protection Laws” means any applicable laws and regulations in any relevant jurisdiction relating to the privacy and processing of Personal Data including: (i) the California Consumer Privacy Act (“CCPA”), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) (“EU GDPR”) and the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the “UK GDPR”) (together, collectively, the “GDPR”), (iii) the Swiss Federal Act on Data Protection, ; (iv) the UK Data Protection Act 2018; and (v) the Privacy and Electronic Communications (EC Directive) Regulations 2003; in each case, as updated, amended or replaced from time to time. The terms “Data Subject”, “Personal Data”, “Personal Data Breach”, “processing”, “processor,” “controller,” and “supervisory authority” shall have the meanings set forth in the GDPR. For the purposes of the DPA, “Personal Data” is as defined herein but further limited to that Personal Data contained in Your Content (as defined the Agreement) and for which Company acts as a processor. For the avoidance of doubt, if Company’s processing activities involving Personal Data are not within the scope of Data Protection Law, such law is not applicable for purposes of the DPA.
- 1.8. “EU SCCs” means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time), as modified by Section 6.2 of this DPA.

- 1.9. “ex-EEA Transfer” means the transfer of Personal Data, which is processed in accordance with the GDPR, from the Data Exporter to the Data Importer (or its premises) outside the European Economic Area (the “EEA”), and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.
- 1.10. “ex-UK Transfer” means the transfer of Personal Data covered by Chapter V of the UK GDPR, which is processed in accordance with the UK GDPR and the Data Protection Act 2018, from the Data Exporter to the Data Importer (or its premises) outside the United Kingdom (the “UK”), and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018.
- 1.11. “Services” shall have the meaning set forth in the Agreement.
- 1.12. “Standard Contractual Clauses” means the EU SCCs and the UK SCCs.
- 1.13. “UK SCCs” means the EU SCCs, as amended by the UK Addendum.

2. Relationship of the Parties; Processing of Data

- 2.1. The parties acknowledge and agree that with regard to the processing of Personal Data, Customer may act either as a controller or processor and, except as expressly set forth in this DPA or the Agreement, Company is a processor. Customer shall, in its use of the Services, at all times process Personal Data, provision or otherwise make available Personal Data to Company, and provide instructions for the processing of Personal Data, in compliance with Data Protection Laws. Customer shall ensure that the processing of Personal Data in accordance with Customer’s instructions will not cause Company to be in breach of the Data Protection Laws. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Company by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the instructions it provides to Company regarding the processing of such Personal Data. Customer shall not provide or make available to Company any Personal Data in violation of the DPA or the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Company from all claims and losses in connection therewith.
- 2.2. Company shall not process Personal Data (i) for purposes other than those in connection with its provision of the Services and/or as set forth in the Agreement and/or Exhibit A, (ii) in a manner violating this DPA. Customer hereby instructs Company to process Personal Data in accordance with the foregoing subsection (i) and as part of any processing initiated by Customer in its use of the Services.
- 2.3. The subject matter, nature, purpose, and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this DPA.
- 2.4. Following expiration or termination of the Agreement, upon Customer’s election and written notice, Company shall return or delete Customer’s Personal Data, unless further storage of such Personal Data is required or authorized by applicable law or otherwise contemplated under the Agreement. If return or destruction is impracticable or prohibited by law, rule or regulation, Company shall take measures to block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing necessary in connection with the foregoing) and shall continue to protect the Personal Data remaining in its possession, custody, or control in accordance with the DPA. If Customer and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 8.1(d) and Clause 8.5 of the EU SCCs (as applicable) shall be provided by Company to Customer only upon Customer’s request.
- 2.5. CCPA. Except with respect to Company Account Data and Company Usage Data, the parties acknowledge and agree that Company is a service provider for the purposes of the CCPA (to the extent it applies) and is receiving personal information from Customer in order to provide the Services pursuant to the Agreement, which constitutes a business purpose. Company shall not sell any such personal information, provided that the provision of the Services by Company does not constitute a sale. Company shall not retain, use or disclose any personal information provided by Customer pursuant to the Agreement and in Company’s capacity as a service provider except as necessary for the specific purpose of performing the Services for

Customer pursuant to the Agreement, or otherwise as set forth in the Agreement or as permitted by the CCPA. The terms “personal information,” “service provider,” “sale,” and “sell” are as defined in Section 1798.140 of the CCPA. Company certifies that it understands the restrictions of this Section 2.5.

3. Confidentiality

Company shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data consistent with Company’s confidentiality obligations in the Agreement. Customer agrees that Company may disclose Personal Data to its advisers, auditors or other third parties as reasonably required in connection with the performance of its obligations under this DPA, the Agreement, or the provision of Services to Customer.

4. Authorized Sub-Processors

- 4.1.** Customer acknowledges and agrees that Company may (1) engage its Affiliates as well as the Authorized Sub-Processors on the List (defined below) to access and otherwise process Personal Data in connection with the Services and (2) from time to time engage additional third parties in connection with providing the Services, including without limitation the processing of Personal Data. By way of this DPA, Customer provides general written authorization to Company to engage sub-processors as necessary to perform the Services.
- 4.2.** A list of Company’s current Authorized Sub-Processors (the “List”) is available to Customer upon request. Such List may be updated by Company from time to time. Company will provide a mechanism to subscribe to notifications (which may include but are not limited to email notifications) of new Authorized Sub-Processors and Customer, if it wishes, will subscribe to such notifications where available. If Customer does not subscribe to such notifications, Customer waives any right it may have to receive prior notice of changes to Authorized Sub-Processors. At least ten (10) days before making material changes to Authorized Sub-Processors, Company will add such third party to the List and notify subscribers, via the aforementioned notifications. Customer may object to such an engagement by informing Company in writing within ten (10) days of receipt of the aforementioned notice, provided such objection is based on reasonable grounds relating to data protection. Company may institute or replace an Authorized Sub-Processor if the need is urgent and reasonably necessary to perform under the Agreement. In such instance, Company shall notify Customer of the replacement as soon as reasonably practicable, and Customer shall retain the right to object to the replacement Sub-Processor. Customer acknowledges that certain sub-processors are essential to providing the Services and that objecting to the use of a sub-processor may prevent Company from offering the Services to Customer.
- 4.3.** If Customer reasonably objects to an engagement in accordance with Section 4.2, and Company cannot provide a commercially reasonable alternative, Customer may discontinue the use of the affected Service by providing written notice to Company. Discontinuation shall not relieve Customer of any fees owed to Company under the Agreement.
- 4.4.** If Customer does not object to the engagement of a third party in accordance with Section 4.2 within ten (10) days of notice by Company, that third party will be deemed an Authorized Sub-Processor for the purposes of this DPA.
- 4.5.** Company will enter into a written agreement with the Authorized Sub-Processor consistent with this DPA, as required under applicable Data Protection Law. In case an Authorized Sub-Processor fails to fulfill its data protection obligations under such written agreement with Company, Company will remain liable to Customer for the performance of the Authorized Sub-Processor’s obligations under such agreement.
- 4.6.** If Customer and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the above authorizations will constitute Customer’s prior written consent to the subcontracting by Company of the processing of Personal Data if such consent is required under the Standard Contractual Clauses.

5. Security of Personal Data.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, contemplating the use of the Services as intended by Company, Company shall maintain the technical and organizational measures set forth in Exhibit C designed to ensure a level of security appropriate to the risk of processing Personal Data.

6. Transfers of Personal Data

- 6.1.** The parties agree that Company may transfer Personal Data processed under this DPA outside the EEA, the UK, Switzerland, or any other jurisdiction in accordance with the provision of the Services. Customer acknowledges that Company's primary processing operations take place in the United States, and that the transfer of Customer's Personal Data to the United States is necessary for the provision of the Services to Customer. If Company transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission has not issued an adequacy decision, the EEA SCCs and/or UK SCCs will apply, as applicable.
- 6.2. Ex-EEA Transfers.** The parties agree that ex-EEA Transfers are made pursuant to the EU SCCs, which are deemed entered into (and incorporated into this DPA by this reference) and completed as follows:
 - 6.2.1.** Module One (Controller to Controller) of the EU SCCs apply when Company is processing Personal Data as a controller pursuant to Section 9 of this DPA.
 - 6.2.2.** Module Two (Controller to Processor) of the EU SCCs apply when Customer is a controller and Company is processing Personal Data for Customer as a processor pursuant to Section 2 of this DPA.
 - 6.2.3.** Module Three (Processor to Sub-Processor) of the EU SCCs apply when Customer is a processor and Company is processing Personal Data on behalf of Customer as a sub-processor.
- 6.3.** For each module, where applicable the following applies:
 - 6.3.1.** The optional docking clause in Clause 7 does not apply.
 - 6.3.2.** In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 4.2 of this DPA;
 - 6.3.3.** In Clause 11, the optional language does not apply;
 - 6.3.4.** All square brackets in Clause 13 are hereby removed;
 - 6.3.5.** In Clause 17 (Option 1), the EU SCCs will be governed by Ireland law.
 - 6.3.6.** In Clause 18(b), disputes will be resolved before the courts of Ireland;
 - 6.3.7.** Exhibit B to this DPA contains the information required in Annex I and Annex III of the EU SCCs;
 - 6.3.8.** Exhibit C to this DPA contains the information required in Annex II of the EU SCCs; and
 - 6.3.9.** By entering into this DPA, the parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.
- 6.4. Ex-UK Transfers.** The parties agree that ex-UK Transfers are made pursuant to the UK SCCs, which are deemed entered into and incorporated into this DPA by reference, and amended and completed in accordance with the UK Addendum, which is incorporated herein as Exhibit D of this DPA.
- 6.5. Transfers from Switzerland.** The parties agree that transfers from Switzerland are made pursuant to the EU SCCs with the following modifications:
 - 6.5.1.** The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the EU SCCs shall be interpreted to include the Federal Act on Data Protection of 19 June 1992 (the "FADP," and as revised as of 25 September 2020, the "Revised FADP") with respect to data transfers subject to the FADP.

6.5.2. The terms of the EU SCCs shall be interpreted to protect the data of legal entities until the effective date of the Revised FADP.

6.5.3. Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner (“FDPI”) of Switzerland shall have authority over data transfers governed by the FADP and the appropriate EU supervisory authority shall have authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Section 13 shall be observed.

6.5.4. The term “EU Member State” as utilized in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

6.6. Supplementary Measures. In respect of any ex-EEA Transfer or ex-UK Transfer, the following supplementary measures shall apply:

6.6.1. As of the date of this DPA, the Data Importer has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Personal Data is being exported, for access to (or for copies of) Customer’s Personal Data (“Government Agency Requests”);

6.7. If either (i) any of the means of legitimizing transfers of Personal Data outside of the EEA or UK set forth in this DPA cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, then Data Importer may by notice to the Data Exporter, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Data Protection Laws.

7. Rights of Data Subjects

Company shall, to the extent permitted by law, notify Customer following receipt of a request by a Data Subject to exercise the Data Subject’s right under applicable Data Protection Laws (such requests individually and collectively “Data Subject Request(s)”). If Company receives a Data Subject Request in relation to Customer’s Personal Data, Company may advise the Data Subject to submit their request to Customer. Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Customer is solely responsible for ensuring that Data Subject Requests are communicated to Company, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.

8. Actions and Access Requests; Audits

8.1. Taking into account the nature of the processing and the information available to Company, Company will, at Customer’s request and subject to Customer paying all of Company’s fees at prevailing rates, and all expenses, provide Customer with reasonable assistance to facilitate conducting data protection impact assessments and consultation with data protection authorities, if Customer is required to engage in such activities under Applicable Law, and solely to the extent that such assistance is necessary and relates to the Processing by Company of Customer Personal Data, and in each case to the extent that such information or access is within Company’s control and Company is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

8.2. To the extent required by the GDPR, Company will, at Customer’s request and subject to Customer paying all of Company’s fees at prevailing rates and expenses, (i) provide Customer with all information reasonably necessary to demonstrate its compliance with this DPA, and (ii) contribute to audits, including inspections, conducted by Customer or an auditor mandated by Customer, in each case to the extent that such information or access is within Company’s control and Company is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party. Any audit must be: (i) conducted during Company’s regular business hours; (ii) with reasonable advance notice to Company; (iii) carried out in a manner that prevents unnecessary disruption to Company’s operations; (iv) subject to reasonable confidentiality procedures; and (v) carried out not more often than once per year, unless an audit is carried out at the direction of a government authority having proper jurisdiction. If Customer and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal

Data), the parties agree that the audits described in Clause 8.9 of the EU SCCs shall be carried out in accordance with this Section 8.2.

- 8.3.** Company shall promptly notify Customer if an instruction, in the Company's opinion, infringes the Data Protection Laws or Supervisory Authority.
- 8.4.** In the event of a Personal Data Breach, Company shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as Company in its sole discretion deems necessary and reasonable to mitigate such violation (to the extent that mitigation is within Company's reasonable control).
- 8.5.** In the event of a Personal Data Breach, Company shall, taking into account the nature of the processing and the information available to Company, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under the GDPR with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

9. Company's Role as a Controller. The parties acknowledge and agree that with respect to Company Account Data and Company Usage Data, Company is an independent controller, not a joint controller with Customer. Company will process Company Account Data and Company Usage Data as a controller (i) to manage the relationship with Customer; (ii) to carry out Company's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Customer; (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Company is subject; and (vi) as otherwise permitted under Data Protection Laws and in accordance with this DPA and the Agreement. Company may also process Company Usage Data as a controller to provide, optimize, and maintain the Services, to the extent permitted by Data Protection Laws. Any processing by the Company as a controller shall be in accordance with the Company's privacy policy set forth at www.paystandards.com/privacypolicy.

10. Conflict. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in the Standard Contractual Clauses, solely to the extent necessary to validate ex-EEA Transfers or ex-UK Transfers, as applicable; (2) the terms of this DPA; (3) the Agreement; and (4) the Company's privacy policy. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

Exhibit A

Details of Processing

Nature and Purpose of Processing: Company will process Customer's Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this DPA, and in accordance with Customer's instructions as set forth in this DPA. The nature of processing includes, without limitation:

- Receiving data, including collection, accessing, retrieval, recording, and data entry
- Protecting data, including restricting, encrypting, and security testing
- Holding data, including storage, organization, and structuring
- Erasing data, including destruction and deletion
- Analyzing data, including product usage assessment
- Sharing data, including disclosure to subprocessors as permitted in this DPA

Duration of Processing: Company will process Customer's Personal Data as long as required (i) to provide the Services to Customer under the Agreement; (ii) for Company's legitimate business needs; or (iii) by applicable law or regulation. Company Account Data and Company Usage Data will be processed and stored as set forth in Company's privacy policy.

Categories of Data Subjects: Customer's employees, consultants, contractors, and/or agents.

Categories of Personal Data: Company processes Personal Data contained in Company Account Data, Company Usage Data, and any Personal Data provided by Customer (including any Personal Data Customer collects from its end users and processes through its use of the Services) or collected by Company in order to provide the Services or as otherwise set forth in the Agreement or this DPA. Categories of Personal Data include name, email, job title, username, Company device identifiers (e.g. serial number), IP address for company device, installed applications for company device, background check verification records (at discretion of Controller), security training records.

Sensitive Data or Special Categories of Data: Customer represents and warrants to Company that Personal Data does not and will not contain, and Customer has not and will not otherwise provide or make available to Company for processing any sensitive Personal Data, including but not limited to financial information (e.g. credentials to any financial accounts or tax return data); health information (e.g. protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding an individual's medical history, mental, or physical condition, or medical treatment or diagnosis by a health care professional, health insurance information, or genetic information); biometric information; government IDs or other government-issued identifiers (e.g. social security numbers); passwords for online accounts (other than passwords necessary to access the Services); credit reports or consumer reports; any payment card information subject to the Payment Card Industry Data Security Standard; information subject to the Gramm-Leach-Bliley Act, Fair Credit Reporting Act, or similar laws, or the regulations promulgated thereunder; information subject to restrictions under applicable law governing personal data of children, including, without limitation, all information about children under 16 years of age; or any information that falls within any special categories of data (as defined under the GDPR or otherwise interpreted under the implementing laws of the EEA member states).

Exhibit B

The following includes the information required by Annex I and Annex III of the EU SCCs, and Table 1, Annex 1A, and Annex 1B of the UK Addendum.

1. The Parties

Data exporter(s):

Name:

Trading Name (if different):

Address:

Official Registration Number (if any) (company number or similar identifier):

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: As described in Section 2 of the DPA.

Signature and date:

Role (controller/processor): Controller

Data importer(s):

Name: PayStandards Inc.

Trading Name (if different): N/A

Address and contact information: 40 Wall Street, #2706, New York, NY 10005;

privacy@paystandards.com

Official Registration Number (if any) (company number or similar identifier): N/A

Activities relevant to the data transferred under these Clauses: ... As described in Section 2 of the DPA.

Signature and date:

Role (controller/processor): As described in Section 2 of the DPA.

2. Description of the Transfer

Data Subjects	As described in Exhibit A of the DPA
Categories of Personal Data	As described in Exhibit A of the DPA
Special Category Personal Data (if applicable)	As described in Exhibit A of the DPA
Nature of the Processing	As described in Exhibit A of the DPA
Purposes of Processing	As described in Exhibit A of the DPA
Duration of Processing and Retention (or the criteria to determine such period)	As described in Exhibit A of the DPA
Frequency of the transfer	As necessary to provide perform all obligations and rights with respect to Personal Data as provided in the Agreement or DPA
Recipients of Personal Data Transferred to the Data Importer	Amazon Web Services is PayStandards Inc.'s only subprocessor as of November 2023.

3. Competent Supervisory Authority

The supervisory authority shall be the supervisory authority of the Data Exporter, as determined in accordance with Clause 13 of the EU SCCs. The supervisory authority for the purposes of the UK Addendum shall be the UK Information Commissioner's Officer.

Exhibit C

Description of the Technical and Organisational Security Measures implemented by the Data Importer

The following includes the information required by Annex II of the EU SCCs and Annex II of the UK Addendum. Each of the following are reasonably designed to ensure certain standards and protocols, in accordance with the Details column.

Technical and Organizational Security Measure	Details
Measures of pseudonymisation and encryption of personal data	Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Databases housing sensitive customer data are encrypted at rest. Company uses only recommended secure cipher suites and protocols to encrypt all traffic in transit and Customer Data is securely encrypted with strong ciphers and configurations when at rest.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Company has undergone a SOC 2 Type 2 audit that includes the Security and Processing Integrity Trust Service Criteria.
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	Daily, weekly and monthly backups of production datastores are taken. Backups are periodically tested in accordance with information security and data management policies.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Company has undergone a SOC 2 Type 2 audit that includes the Security and Processing Integrity Trust Service Criteria.
Measures for user identification and authorization	Company uses secure access protocols and processes and follows industry best-practices for authentication.
Measures for the protection of data during transmission	Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Company uses only recommended secure cipher suites and protocols to encrypt all traffic in transit (i.e. TLS 1.2)
Measures for the protection of data during storage	Encryption-at-rest is automated using AWS's transparent disk encryption, which uses industry standard AES-256 encryption to secure all volume (disk) data. All keys are fully managed by AWS.
Measures for ensuring physical security of locations at which personal data are processed	All Company processing occurs in physical data centers that are managed by AWS. https://aws.amazon.com/compliance/data-center/controls/
Measures for ensuring events logging	Company monitors access to applications, tools, and resources that process or store Customer Data, including cloud services. Monitoring of security logs is managed by the security and engineering teams. Log activities are investigated when necessary and escalated appropriately.
Measures for ensuring system configuration, including default configuration	Company adheres to a change management process to administer changes to the production environment for the Services, including changes to its underlying software, applications, and systems. All production changes are automated through CI/CD tools to ensure consistent configurations.

Measures for certification/assurance of processes and products	Company undergoes annual SOC 2 Type II audits.
Measures for ensuring data minimisation	Company's Customers unilaterally determine what data they route through the Services. As such, Company operates on a shared responsibility model. Company gives Customers control over exactly what data enters the platform. Additionally, Company has built in self-service functionality to the Services that allows Customers to delete and suppress data at their discretion.
Measures for ensuring data quality	Company has a multi-tiered approach for ensuring data quality. These measures include: (i) unit testing to ensure quality of logic used to process API calls, (ii) database schema validation rules which execute against data before it is saved to our database, (iii) a schema-first API design that enforces a strict contract between official clients and API resolvers. Company applies these measures across the board, both to ensure the quality of any Usage Data that Company collects and to ensure that the Company Platform is operating within expected parameters. Company ensures that data quality is maintained from the time a Customer sends Customer Data into the Services and until that Customer Data is presented or exported.
Measures for ensuring limited data retention	Customers unilaterally determine what data they route through the Services. As such, Company operates on a shared responsibility model. If a Customer is unable to delete Personal Data via the self-services functionality of the Services, then the Company deletes such Personal Data upon the Customer's written request, within the timeframe specified in this DPA and in accordance with Applicable Data Protection Law. All Personal Data is deleted from the Services following service termination.
Measures for ensuring accountability	Company has adopted measures for ensuring accountability, such as implementing data protection and information security policies across the business, recording and reporting Personal Data Breaches, and formally assigning roles and responsibilities for information security and data privacy functions. Additionally, the Company conducts regular third-party audits to ensure compliance with our privacy and security standards.
Measures for allowing data portability and ensuring erasure	<p>Personal Data submitted to the Services by Customer may be deleted by the Customer or at the Customer's request.</p> <p>Personal Data is incidental to the Company's Services. Based on Privacy by Design and Data Minimization principles, Company severely limits the instances of Personal Data collection and processing within the Services. Most use cases for porting Personal Data from Company are not applicable. However, Company will respond to all requests for data porting in order to address Customer needs.</p>
Technical and organizational measures of sub-processors	The Company enters into Data Processing Agreements with its Authorized Sub-Processors with data protection obligations substantially similar to those contained in this DPA.

Exhibit D

UK Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

i. Part 1: Tables

Table 1: Parties

Start Date	This UK Addendum shall have the same effective date as the DPA	
The Parties	Exporter	Importer
Parties' Details	Customer	Company
Key Contact	See Exhibit B of this DPA	See Exhibit B of this DPA

Table 2: Selected SCCs, Modules and Selected Clauses

EU SCCs	The Version of the Approved EU SCCs which this UK Addendum is appended to as defined in the DPA and completed by Section 6.2 and 6.3 of the DPA.
---------	--

Table 3: Appendix Information

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

ii. Annex 1A: List of Parties	iii. As per Table 1 above
iv. Annex 2B: Description of Transfer	v. See Exhibit B of this DPA
vi. Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	vii. See Exhibit C of this DPA
viii. Annex III: List of Sub processors (Modules 2 and 3 only):	ix. See Exhibit B of this DPA

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

- x.** [SELECT OPTION] *[Note: This provision permits the selected party (if any) to terminate the UK Addendum if the ICO changes the approved UK Addendum which directly results in a substantial, disproportionate, and demonstrable*

increase in (a) its direct costs of performing its obligations under the UK Addendum or (b) its risk under the UK Addendum.]

Ending this UK Addendum when the Approved UK Addendum changes	<input checked="" type="checkbox"/> Importer
	<input checked="" type="checkbox"/> Exporter
	<input type="checkbox"/> Neither Party

xi.

xi. Entering into this UK Addendum:

1. Each party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other party also agreeing to be bound by this UK Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making ex-UK Transfers, the Parties may enter into this UK 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 UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

xiii. Interpretation of this UK Addendum

3. Where this UK 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:

UK Addendum	means this International Data Transfer Addendum incorporating the EU SCCs, attached to the DPA as Exhibit D.
EU SCCs	means the version(s) of the Approved EU SCCs which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information
Appendix Information	shall be as set out in Table 3
Appropriate Safeguards	means the standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making an ex-UK Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved UK Addendum	means 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 may be revised under Section 18 of the UK Addendum.
Approved EU SCCs	means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).
ICO	means the Information Commissioner of the United Kingdom.
ex-UK Transfer	shall have the same definition as set forth in the DPA .

UK	means the United Kingdom of Great Britain and Northern Ireland
UK Data Protection Laws	means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	shall have the definition set forth in the DPA.

4. The UK 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 UK Addendum amend the Approved EU SCCs in any way which is not permitted under the Approved EU SCCs or the Approved UK Addendum, such amendment(s) will not be incorporated in the UK 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 the UK Addendum, UK Data Protection Laws applies.

7. If the meaning of the UK 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 the UK Addendum has been entered into.

xiv. 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 ex-UK Transfers, the hierarchy in Section 10 below will prevail.

10. Where there is any inconsistency or conflict between the Approved UK Addendum and the EU SCCs (as applicable), the Approved UK Addendum overrides the EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved UK Addendum.

11. Where this UK Addendum incorporates EU SCCs which have been entered into to protect ex-EU Transfers subject to the GDPR, then the parties acknowledge that nothing in the UK Addendum impacts those EU SCCs.

xv. Incorporation and Changes to the EU SCCs:

12. This UK Addendum incorporates the EU SCCs which are amended to the extent necessary so that:

- c. 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;
- c. Sections 9 to 11 above override Clause 5 (Hierarchy) of the EU SCCs; and

- c. the UK Addendum (including the 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.

13. Unless the parties have agreed alternative amendments which meet the requirements of Section 12 of this UK Addendum, the provisions of Section 15 of this UK Addendum will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 of this UK Addendum may be made.

15. The following amendments to the EU SCCs (for the purpose of Section 12 of this UK Addendum) are made:

- a. References to the “Clauses” means this UK Addendum, incorporating the EU SCCs;
- b. In Clause 2, delete the words: “and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679”,
- c. Clause 6 (Description of the transfer(s)) is replaced with: “The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;
- d. Clause 8.7(i) of Module 1 is replaced with: “it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;
- e. Clause 8.8(i) of Modules 2 and 3 is replaced with: “the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;
- f. References to “Regulation (EU) 2016/679”, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;
- g. References to Regulation (EU) 2018/1725 are removed;
- h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
- i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
- j. Clause 13(a) and Part C of Annex I are not used;
- k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
- l. In Clause 16(e), subsection (i) is replaced with: “the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply”;
- m. Clause 17 is replaced with: “These Clauses are governed by the laws of England and Wales”;

n. Clause 18 is replaced with: “Any dispute arising from these Clauses shall be resolved by the courts of England and Wales.” A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The parties agree to submit themselves to the jurisdiction of such courts.”; and

o. The footnotes to the Approved EU SCCs do not form part of the UK Addendum, except for footnotes 8, 9, 10 and 11.

i. Amendments to the UK Addendum

16. The parties may agree to change Clauses 17 and/or 18 of the 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 UK 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 UK Addendum which:

a. makes reasonable and proportionate changes to the Approved UK Addendum, including correcting errors in the Approved UK Addendum; and/or

b. reflects changes to UK Data Protection Laws;

The revised Approved UK Addendum will specify the start date from which the changes to the Approved UK Addendum are effective and whether the parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved UK Addendum from the start date specified.

19. If the ICO issues a revised Approved UK Addendum under Section 18 of this UK Addendum, if a party will as a direct result of the changes in the Approved UK Addendum have a substantial, disproportionate and demonstrable increase in:

c. its direct costs of performing its obligations under the UK Addendum; and/or

c. its risk under the UK Addendum,

1. and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other party before the start date of the revised Approved UK Addendum.

1. The parties do not need the consent of any third party to make changes to this UK Addendum, but any changes must be made in accordance with its terms.