Data Processing Addendum

11-August-2026

This Data Processing Addendum ("DPA") forms part of, and applies only in connection with, a written master services agreement, subscription agreement, order form, or other written commercial agreement between Valency Systems Inc. ("Company") and the customer identified therein ("Customer" and, together with Company, the "Parties"), under which Company Processes Personal Data on behalf of Customer (the "Agreement"). This DPA does not apply to any individual or entity that accesses or uses the Services solely under Company's publicly available terms of service, including free, trial, evaluation, and self-service accounts. Company's processing of personal data in connection with such use is governed by those terms of service and by Company's privacy policy. Upon this DPA becoming effective in accordance with Section 14 herein, each Party enters into this DPA on behalf of itself and, to the extent required under Privacy Laws (defined below), its affiliates. This DPA incorporates the terms of the Agreement, and any capitalized terms that are used but not defined in this DPA shall have the meanings set forth in the Agreement.

1. Definitions

1.1 "Authorized Subprocessor" means a third-party entity engaged by Company to process Personal Data in order to provide the Services and that has been approved by Customer in accordance with Section 6.

1.2 "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.

1.3 "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 similar data.

1.4 "Data Privacy Framework" means, as applicable, EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and/or the Swiss-U.S. Data Privacy Framework.

1.5 "Data Subject" means a natural person whose Personal Data is protected by Privacy Laws. For the avoidance of doubt, "Data Subject" includes the term "Consumer" under Privacy Laws.

1.6 "Data Subject Request" means a request from a Data Subject to exercise their rights over Personal Data afforded pursuant to Privacy Laws.

1.7 "EU SCCs" means 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 9 of this DPA.

1.8 "ex-EEA Transfer" means the transfer of Personal Data subject to the GDPR from the European Economic Area (the "EEA"), to a country where the transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

1.9 "ex-UK Transfer" means the transfer of Personal Data subject to Chapter V of the UK GDPR from outside the United Kingdom (the "UK") where 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.

1.10 "Personal Data" means any information provided to Company by or on behalf of Customer in connection with the Services that relates to an identified or identifiable Data Subject and constitutes "personal data," "personal information," or equivalent term under Privacy Laws.

1.11 "Privacy Laws" means any applicable laws and regulations in any relevant jurisdiction relating to the processing of Personal Data including, each to the extent applicable: (i) 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"), (ii) the Swiss Federal Act on Data Protection, (iii) the UK Data Protection Act 2018, (iv) the Privacy and Electronic Communications (EC Directive) Regulations 2003, and (v) U.S. state comprehensive privacy laws, such as the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 (the "CCPA"); in each case, as updated, amended or replaced from time to time. The terms "affiliates," "business purpose," "Controller," "Personal Data Breach," "Processor," "process" or "processing," "sell," "share," or "supervisory authority," shall have the meanings set forth for those or equivalent terms under Privacy Laws. For the avoidance of doubt, the terms "Controller" and "Processor" include "Business" and "Service Provider," respectively, as defined in the CCPA.

1.12 "Standard Contractual Clauses" means, as applicable, the EU SCCs and the UK SCCs.

1.13 "UK Addendum" means the template International Data Transfer Addendum issued by the Information Commissioner and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022 (as may be amended from time to time), as completed by Exhibit D.

1.14 "UK SCCs" means the EU SCCs, as amended by the UK Addendum.

2. Role of the Parties; Description of Processing.

2.1 Except as expressly set forth in this DPA or the Agreement, with respect to Personal Data, Customer is the Controller and Company is a Processor, or to the extent Customer is a Processor to a third-party Controller, Company is a subprocessor.

2.2 Company shall process Personal Data only (i) for purposes set forth in the Agreement, (ii) in a manner consistent with the documented instructions provided by Customer, which shall include the Agreement and this DPA, and (iii) as required by Privacy Laws or a supervisory authority; in such case, Company shall inform Customer of that legal requirement before processing to the extent legally permitted. The subject matter, nature, purpose, and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects involved, are described in Exhibit A to this DPA.

3. Customer's Obligations. Customer shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Privacy 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 Privacy 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 Agreement or otherwise inappropriate for the nature of the Services**, and shall indemnify Company from all claims and losses in connection therewith. Company shall **immediately** notify Customer if an instruction, in Company's opinion, infringes Privacy Laws or an instruction of a supervisory authority.

4. Use of Personal Data. Company shall not: (i) sell or share Personal Data; (ii) retain, use, or disclose Personal Data outside of Company's direct business relationship with Customer or for any purpose other than for a business purpose under the CCPA on behalf of Customer or than as necessary to perform the Services for Customer pursuant to the Agreement, except as otherwise permitted in the Agreement or by Privacy Laws; and (iii) combine Personal Data received from, or on behalf of, Customer with Personal Data that it receives from, or on behalf of, another party or person, except as necessary to provide the Services or as otherwise instructed by Customer.

5. Audit.

5.1 Company shall maintain records sufficient to demonstrate its compliance with its obligations under this DPA. Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Company shall, either (i) make available for Customer's review copies of certifications or reports demonstrating Company's compliance with prevailing data security standards applicable to the processing of Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Privacy Laws, allow Customer's independent third party representative to conduct an audit or inspection of Company's data security infrastructure and procedures that is sufficient to demonstrate Company's compliance with its obligations under Privacy Laws, *provided that* (a) Customer provides reasonable prior written notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Company's business; (b) such audit shall only be performed during business hours and occur no more than once per calendar year; and (c) such audit shall be restricted to data relevant to Customer. Customer shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Company for any time expended for on-site audits. If Customer and Company have entered into Standard Contractual Clauses as described in Section 9 (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 5.1.

5.2 To the extent permitted under Privacy Laws, if Customer determines that Company is processing Personal Data in an unauthorized manner, Customer may, taking into account nature of Company's processing and the nature of the Personal Data processed by Company on behalf of Customer, and upon providing prior written notice, take commercially reasonable and appropriate steps to stop and remediate such unauthorized processing as set forth in this DPA.

6. Authorized Subprocessors.

6.1 Customer acknowledges and agrees that Company may (1) engage its affiliates as well as the Authorized Subprocessors listed in Exhibit B to this DPA to access and process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the processing of Personal Data pursuant to Section 6.2. By way of this DPA, Customer provides general written authorization to Company to engage subprocessors as necessary to perform the Services.

6.2 A list of Company's current Authorized Subprocessors (the "List") will be made available to Customer, either attached hereto, at a link provided to Customer, via email to support@valency.io or through another means made available to Customer. Such List may be updated by Company from time to time. Company may provide a mechanism to subscribe to notifications of new Authorized Subprocessors and Customer agrees to subscribe to such notifications where available. At least ten (10) days before enabling any third party other than existing Authorized Subprocessors to access or participate in the processing of Personal Data, Company will add such third party to the List and notify Customer via email. Customer may object to such an engagement by informing Company within ten (10) days of receipt of the aforementioned notice to Customer, provided such objection is in writing and based on reasonable grounds relating to data protection. If Customer does not object during this period, that third party will be deemed an Authorized Subprocessor. Customer acknowledges that certain subprocessors are essential to providing the Services and that objecting to the use of a subprocessor may prevent Company from offering the Services to Customer.

6.3 If Customer reasonably objects to an engagement in accordance with Section 6.2, and Company cannot provide a commercially reasonable alternative within a reasonable period of time, 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.

6.4 Company will enter into a written agreement with the Authorized Subprocessor imposing on the Authorized Subprocessor data protection obligations comparable to those imposed on Company under this DPA with respect to the protection of Personal Data. In case an Authorized Subprocessor 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 Subprocessor's obligations under such agreement.

6.5 If Customer and Company have entered into Standard Contractual Clauses as described in Section 9 (Transfers of Personal Data), (i) 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, and (ii) the parties agree that the copies of the agreements with Authorized Subprocessors that must be provided by Company to Customer pursuant to Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by Company beforehand, and that such copies will be provided by Company only upon request by Customer.

7. Confidentiality; Security of Personal Data.

7.1 Company shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance 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 Privacy Laws and this DPA, the Agreement, or the provision of Services to Customer.

7.2 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, Company shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Personal Data, as described in Exhibit C.

8. Personal Data Breach.

8.1 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 remediate such Personal Data Breach, to the extent that remediation is within Company's reasonable control.

8.2 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 Privacy Laws with respect to notifying (i) the relevant supervisory authority or regulatory agency and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

8.3 The obligations described in Sections 8.1 and 8.2 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer. Company's obligation to report or respond to a Personal Data Breach under Sections 8.1 and 8.2 will not be construed as an acknowledgement by Company of any fault or liability with respect to the Personal Data Breach.

9. Transfers of Personal Data.

9.1 The parties agree that Company may transfer Personal Data processed under this DPA outside the EEA, the UK, or Switzerland as necessary to provide the Services. Customer acknowledges that Company's primary processing operations take place in the United States, and that the transfer of 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, Company will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Privacy Laws.

9.2 Ex-EEA Transfers. The Parties agree that ex-EEA Transfers shall either be made pursuant to (i) the Data Privacy Framework to the extent the recipient of the ex-EEA Transfer is certified accordingly, or (ii) the EU SCCs, which are deemed entered into (and incorporated herein by reference) and completed as follows:

9.2.1 Module One (Controller to Controller) of the EU SCCs applies when Company is processing Personal Data as a controller pursuant to Section 13 of this DPA.

9.2.2 Module Two (Controller to Processor) of the EU SCCs applies when Customer is a controller and Company is a processor of Personal Data in accordance with Section 2 of this DPA.

9.2.3 Module Three (Processor to Subprocessor) of the EU SCCs applies when Customer is a processor and Company is a subprocessor of Personal Data in accordance with Section 2 of this DPA.

9.3 For each module, where applicable the following applies:

9.3.1 The optional docking clause in Clause 7 does not apply.

9.3.2 In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of subprocessor changes shall be as set forth in Section 6.2 of this DPA.

9.3.3 In Clause 11, the optional language does not apply.

9.3.4 All square brackets in Clause 13 are hereby removed.

9.3.5 In Clause 17 (Option 1), the EU SCCs will be governed by **Irish** law.

9.3.6 In Clause 18(b), disputes will be resolved before the courts of **Ireland**.

9.3.7 Exhibit B to this DPA contains the information required in Annex I of the EU SCCs.

9.3.8 Exhibit C to this DPA contains the information required in Annex II of the EU SCCs.

9.3.9 By entering into this DPA, the Parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

9.4 Ex-UK Transfers. The Parties agree that ex-UK Transfers shall either be made pursuant to (i) the Data Privacy Framework to the extent that the recipient of the ex-UK Transfer is certified accordingly, or (ii) the UK SCCs, which are deemed entered into and incorporated herein by reference. 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.

9.5 Transfers from Switzerland. The Parties agree that transfers from Switzerland shall either be made pursuant to (i) the Data Privacy Framework to the extent that the recipient of the transfer from Switzerland is certified accordingly, or (ii) the EU SCCs with the following modifications:

9.5.1 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.

9.5.2 Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner ("FDPIC") 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 Clause 13 shall be observed.

9.5.3 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.

9.6 Supplementary Measures. In respect of any transfer of Personal data made pursuant to the Standard Contractual Clauses, the following supplementary measures shall apply:

9.6.1 As of the date of this DPA, Company 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) such Personal Data ("Government Agency Requests").

9.6.2 If Company receives a Government Agency Request, Company shall attempt to redirect the government agency to Customer. As part of this effort, Company may provide Customer's basic contact information to the government agency. If Company is compelled to disclose Personal Data, to the extent legally permitted, Company shall notify Customer of the demand and reasonably cooperate to allow Customer to seek a protective order or other appropriate remedy. Company shall not voluntarily disclose Personal Data to any law enforcement or government agency. The Parties shall determine whether all or any transfers of Personal Data pursuant to this DPA should be suspended in the light of such a Government Agency Request.

9.6.3 The Parties will confer as appropriate to consider whether: (i) the protection afforded by the laws of the country of Company to data subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA or the UK, as applicable; (ii) additional measures are reasonably necessary for the transfer to comply with Privacy Laws; and (iii) it is still appropriate for Personal Data to be transferred to the relevant Company, taking into account all relevant information available, including guidance by supervisory authorities, to the Parties.

9.6.4 If either (i) any of the means of legitimizing a transfer cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, the Parties agree to amend the means of legitimizing transfers in accordance with Privacy Laws. To the extent necessary to ensure the enforceability of the Standard Contractual Clauses, the Parties shall execute the Standard Contractual Clauses as a separate agreement.

10. Data Protection Assessments. Taking into account the nature of Company's processing and the information available to Company, Company shall reasonably cooperate with Customer to conduct any data protection or privacy impact assessments as required by Privacy Laws, including by providing Customer with information and documents necessary for such assessments that Customer cannot otherwise obtain without Company's assistance. Notwithstanding the foregoing, Customer and Company each remain responsible only for the measures respectively allocated to them under Privacy Laws pertaining to any such assessment.

11. Data Subject Request.

11.1 Company shall, to the extent permitted by Privacy Laws, notify Customer upon receipt of a Data Subject Request. If Company receives a Data Subject Request in relation to Personal Data, Company will advise the Data Subject to submit their request to Customer and 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.

11.2 Company shall, at the request of Customer, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, *provided that* (i) Customer is itself unable to respond without Company's assistance and (ii) Company is able to do so in accordance with all applicable laws, rules, and regulations. Customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

12. Return or Destruction of Personal Data. Upon the termination or expiration of the Agreement, at Customer's choice, Company shall return or delete Personal Data, unless further storage of such Personal Data is required or authorized by applicable law. 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 required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If Customer and Company have entered into Standard Contractual Clauses as described in Section 9 (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.

13. 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 Privacy 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 Privacy Laws. Any processing by Company as a controller shall be in accordance with Company's privacy policy.

14. Miscellaneous. 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; (2) the terms of this DPA; (3) the Agreement, and (4) Company's privacy policy. Any claims brought in connection with this DPA will be subject to the Agreement, including, but not limited to, the exclusions and limitations set forth in the Agreement.

15. Execution of this DPA. This DPA is incorporated by reference into, and forms part of, the Agreement. This DPA becomes effective as of the effective date of the Agreement and applies only to the extent that Company Processes Personal Data on behalf of Customer in Company's capacity as a Processor or Service Provider under the Agreement. Where the Agreement expressly incorporates this DPA by reference, no separate signature is required for this DPA to become effective; otherwise, this DPA becomes effective upon execution by both Parties. Where the individual executing or accepting the Agreement does so on behalf of an entity, that individual represents and warrants that they have full legal authority to bind that entity to this DPA, and "Customer" means that entity. For the avoidance of doubt, this DPA does not become effective, and neither Party may rely on it, in respect of access to or use of the Services solely under Company's publicly available terms of service, including free, trial, evaluation, and self-service accounts.

Exhibit A

Details of Processing

Nature and Purpose of Processing: Company will process 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
Holding data, including storage, organization and structuring
Using data, including analysis, consultation, testing, automated decision making and profiling
Updating data, including correcting, adaptation, alteration, alignment and combination
Protecting data, including restricting, encrypting, and security testing
Returning data to the data exporter or data subject
Erasing data, including destruction and deletion

Duration of Processing: Company will process Personal Data as long as required (i) to provide the Services to Customer under the Agreement; or (ii) 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 end-users/customers and/or Customer employees.

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, location, email address and ORCID.

Sensitive Data or Special Categories of Data: None

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: The Customer, as identified in the Agreement

Address: The Customer's address

Contact person's name, position and contact details: The Customer's contact details, as set out in the Agreement.

Role (controller/processor): Controller (either as the Controller; or acting in the capacity of a Controller, as a Processor, on behalf of another Controller)

Activities relevant to the data transferred under these Clauses: Processing of Data in connection with Customer's use of the Services under the Agreement

Data importer(s): Valency Systems Inc.

Name: FAO "Privacy Officer" at support@valency.io

Address: 2168 Shattuck Avenue, Ste 300, Berkeley California, 94704

Role (controller/processor): Processor

Activities: Processing of Data in connection with Customer's use of the Services under the Agreement.

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 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	Company will maintain and provide a list of its Subprocessors upon request.

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 Office.

4. List of Authorized Subprocessors

A list of Company's current Authorized Subprocessors (the "List") will be made available to Customer via email to support@valency.io using subject line "Authorized Subprocessors List Request".

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 Appendix II of the UK Addendum.

Technical and Organizational Security Measure	Details
Measures of pseudonymisation and encryption of personal data	Personal data that is external facing is encrypted in transit and at rest using industry-standard algorithms (TLS 1.2+, AES-256); identifiers are pseudonymised or tokenised where processing does not require direct identification.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Services run on AWS infrastructure across redundant infrastructure with automated health monitoring, alerting, and documented incident response procedures.
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	Automated encrypted backups are taken regularly with defined RPO/RTO targets and periodic restoration testing.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	SOC 2 Type 1 certification efforts underway with continuous control monitoring via Vanta.
Measures for user identification and authorization	Role-based access control on least-privilege principles, SSO with mandatory multi-factor authentication, and periodic access reviews with prompt deprovisioning on role change or termination.
Measures for the protection of data during transmission	All external data in transit is encrypted over TLS 1.2 or higher; unencrypted protocols are disabled.
Measures for the protection of data during storage	Data at rest is encrypted in line with best practices.
Measures for ensuring physical security of locations at which personal data are processed	Production data is hosted in AWS data centres with 24/7 monitoring, biometric/keycard access control and access logging; corporate offices use keycard entry and a managed, segmented network.
Measures for ensuring events logging	Application, infrastructure and administrative access events are centrally logged, and monitored for anomalous activity.
Measures for ensuring system configuration, including default configuration	Infrastructure is provisioned from version-controlled, hardened baseline configurations with change management review; managed endpoints are monitored for configuration compliance via Vanta Device Monitor.
Measures for internal IT and IT security governance and management	A documented information security program with assigned ownership, written policies reviewed at least annually, and formal risk assessment and vendor review processes.
Measures for certification/assurance of processes and products	SOC 2 Type 1 certification efforts underway with continuous control monitoring via Vanta.
Measures for ensuring data minimisation	Only personal data necessary to deliver the contracted service is collected and processed; collection is reviewed at design stage and unnecessary fields are not captured.
Measures for ensuring data quality	Input validation, schema constraints, and customer-facing controls allowing correction or update of personal data.
Measures for ensuring limited data retention	Customer data is retained only for the term of the agreement plus a defined post-termination window, after which it is deleted or anonymised per the documented retention schedule.

Measures for ensuring accountability	Mandatory security and privacy training at onboarding and annually.
Measures for allowing data portability and ensuring erasure	Customer data can be exported in structured, machine-readable format on request, and deleted within 30 days of a verified deletion request or contract termination.
Technical and organizational measures of subprocessors	Company enters into data processing agreements with its Authorized Subprocessors 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

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 Sections 9.2 and 9.3 of the DPA.

Table 3: Appendix Information

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

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

Ending this UK Addendum when the Approved UK Addendum changes	☒ Importer ☒ Exporter ☐ Neither Party

Part 2: Mandatory Clauses

The Mandatory Clauses of the UK Addendum are incorporated herein by reference.