Data Processing Addendum

Last updated: October 1, 2025

This Data Processing Addendum ("DPA") supplements the Terms of Use (the "Agreement") entered into by and between Customer, as identified in the Agreement, ("Customer") and TakeUp, LLC ("TakeUp"), and any party which accedes to this DPA from time to time pursuant to Clause 7 of the EU SCCs (as defined below) (collectively with TakeUp and Customer, the "Parties"). This DPA incorporates the terms of the Agreement. TakeUp may update this DPA from time to time, and we will provide reasonable notice of any such updates. Any terms not defined in this DPA shall have the meaning set forth in the Agreement.

1. Definitions

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

1.2 "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.

1.3 "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.

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

1.5 "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.

1.6 "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.

1.7 "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.

1.8 "Personal Data" means any information provided to TakeUp 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.

1.9 "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," "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.

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

1.11 "TakeUp Account Data" means personal data that relates to TakeUp's relationship with Customer, including the names or contact information of individuals authorized by Customer to access Customer's account.

1.12 "TakeUp Usage Data" means Service usage data collected and processed by TakeUp 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.

1.13 "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 TakeUp is a Processor, or to the extent Customer is a Processor to a third-party Controller, TakeUp is a subprocessor.

2.2 TakeUp 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, TakeUp 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. Compliance with Privacy Laws. 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 TakeUp 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 TakeUp by or on behalf of Customer, (ii) the means by which Customer acquired any such Personal Data, and (iii) the instructions it provides to TakeUp regarding the processing of such Personal Data. Customer shall not provide or make available to TakeUp any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify TakeUp from all claims and losses in connection therewith. TakeUp shall immediately notify Customer if an instruction, in TakeUp's opinion, infringes Privacy Laws or instruction of a supervisory authority.

4. Use of Personal Data. TakeUp shall not: (i) sell or share Personal Data; (ii) retain, use, or disclose Personal Data outside of TakeUp's direct business relationship with Customer or for any purpose other than for a business purpose under the CCPA on behalf of Customer or as necessary to perform the Services for Customer pursuant to the Agreement, except as otherwise permitted in 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 TakeUp 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, TakeUp shall, either (i) make available for Customer's review copies of certifications or reports demonstrating TakeUp'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 TakeUp's data security infrastructure and procedures that is sufficient to demonstrate TakeUp'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 TakeUp'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 TakeUp for any time expended for on-site audits. If Customer and TakeUp 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 5.2.

6. Authorized Subprocessors.

6.1 Customer acknowledges and agrees that TakeUp 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 TakeUp to engage subprocessors as necessary to perform the Services.

6.2 A list of TakeUp's current Authorized Subprocessors (the "List") will be made available to Customer, either attached hereto, at a link provided to Customer, via email or through another means made available to Customer. Such List may be updated by TakeUp from time to time. TakeUp 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, TakeUp will add such third party to the List and notify Customer via email. Customer may object to such an engagement by informing TakeUp 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 TakeUp from offering the Services to Customer.

6.3 If Customer reasonably objects to an engagement in accordance with Section 6.2, and TakeUp 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 TakeUp. Discontinuation shall not relieve Customer of any fees owed to TakeUp under the Agreement.

6.4 TakeUp will enter into a written agreement with the Authorized Subprocessor imposing on the Authorized Subprocessor data protection obligations comparable to those imposed on TakeUp 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 TakeUp, TakeUp will remain liable to Customer for the performance of the Authorized Subprocessor's- obligations under such agreement.

6.5 If Customer and TakeUp 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 TakeUp 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 TakeUp 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 TakeUp beforehand, and that such copies will be provided by TakeUp only upon request by Customer.

7. Confidentiality; Security of Personal Data.

7.1 TakeUp shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance with TakeUp's confidentiality obligations in the Agreement. Customer agrees that TakeUp 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.

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, TakeUp 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, TakeUp shall, without undue delay, inform Customer of the Personal Data Breach and take such steps as TakeUp in its sole discretion deems necessary and reasonable to remediate such Personal Data Breach, to the extent that remediation is within TakeUp's reasonable control.

8.2 In the event of a Personal Data Breach, TakeUp shall, taking into account the nature of the processing and the information available to TakeUp, 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. TakeUp'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 TakeUp of any fault or liability with respect to the Personal Data Breach.

9. Transfers of Personal Data.

9.1 The parties agree that TakeUp may transfer Personal Data processed under this DPA outside the EEA, the UK, or Switzerland as necessary to provide the Services. Customer acknowledges that TakeUp'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 TakeUp transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission has not issued an adequacy decision, TakeUp 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 into this herein by reference) and completed as follows:

9.2.1 Module One (Controller to Controller) of the EU SCCs applies when TakeUp is processing Personal Data as a controller pursuant to Section 9 of this DPA.

9.2.2 Module Two (Controller to Processor) of the EU SCCs applies when Customer is a controller and TakeUp 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 TakeUp 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 1 (general written authorization) applies, and the minimum time period for prior notice of subprocessor changes shall be as set forth in Section 6.1 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 England and Wales.

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

9.5.1 As of the date of this DPA, TakeUp 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").

9.5.2 If TakeUp receives a Government Agency Request, TakeUp shall attempt to redirect the government agency to Customer. As part of this effort, TakeUp may provide Customer's basic contact information to the government agency. If TakeUp is compelled to disclose Personal Data, to the extent legally permitted, TakeUp shall notify Customer of the demand and reasonably cooperate to allow Customer to seek a protective order or other appropriate remedy. TakeUp 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 light of such a Government Agency Request.

9.5.3 The Parties will confer as appropriate to consider whether: (i) the protection afforded by the laws of the country of TakeUp 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 TakeUp, taking into account all relevant information available, including guidance by supervisory authorities, to the Parties.

9.5.4 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 TakeUp's processing and the information available to TakeUp, TakeUp 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 TakeUp's assistance. Notwithstanding the foregoing, Customer and TakeUp 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 TakeUp shall, to the extent permitted by Privacy Laws, notify Customer upon receipt of Data Subject Request. If TakeUp receives a Data Subject Request in relation to Personal Data, TakeUp 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 communicated to TakeUp, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.

11.2TakeUp 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 TakeUp's assistance and (ii) TakeUp 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 TakeUp.

12. **Return or Destruction of Personal Data.** Upon the termination or expiration of the Agreement, at Customer's choice, TakeUp 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, TakeUp 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 TakeUp 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 TakeUp to Customer only upon Customer's request.

13. TakeUp's Role as a Controller. The parties acknowledge and agree that with respect to TakeUp Account Data and TakeUp Usage Data, TakeUp is an independent controller, not a joint controller with Customer. TakeUp will process TakeUp Account Data and TakeUp Usage Data as a controller (i) to manage the relationship with Customer; (ii) to carry out TakeUp'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 TakeUp is subject; and (vi) as otherwise permitted under Privacy Laws and in accordance with this DPA and the Agreement. TakeUp may also process TakeUp Usage Data as a controller to provide, optimize, and maintain the Services, to the extent permitted by Privacy Laws. Any processing by TakeUp as a controller shall be in accordance with TakeUp'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) TakeUp'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.

Exhibit A

Details of Processing

Nature and Purpose of Processing: TakeUp 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 and testing
Updating data, including correcting, adaptation, alteration, alignment and combination
Protecting data, including restricting, encrypting, and security testing
Sharing data, including disclosure, dissemination, allowing access or otherwise making available
Returning data to the data exporter or data subject
Erasing data, including destruction and deletion

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

Categories of Data Subjects: Customer end-users/customers AND/OR Customer employees

Categories of Personal Data: TakeUp processes Personal Data contained in TakeUp Account Data, TakeUp 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 TakeUp 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, phone number, address, and title.

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: Customer

Address: As designated in the Order Form to the Agreement or within the Customer's account

Signature and Date: By entering into the Agreement, Customer is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Order Form or the date that Customer begins to use TakeUp's services.

Role (controller/processor): As provided in Section 2 of this DPA.

Data importer(s):

Name: TakeUp, LLC

Address: One Park Circle, Westfield Center, Ohio 44251, USA

Signature and date: By entering into the Agreement, Data Importer is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Order Form or the date that Customer begins to use TakeUp's services.

Role (controller/processor): As provided 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 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	TakeUp 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 Officer.

4. **List of Authorized Subprocessors**

Name of Authorized Subprocessor	Description of processing	Country in which subprocessing will take place
HubSpot	Customer relationship management	United States
Amazon Web Services	Cloud hosting	United States

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	Data encrypted in transit using TLS protocols; Data encrypted at rest via AWS and HubSpot; No pseudonymisation as only limited customer data (name, email, phone, address) is collected.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Use of AWS infrastructure providing redundancy, availability, and physical security; Internal access restricted to authorized personnel using MFA and role-based access controls.
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 daily backups of production data with robust recovery capabilities through AWS; Recovery testing performed periodically.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Centralized error monitoring via BugSnag; No formal SOC2/ISO 27001 certifications or external penetration tests performed to date; Internal security reviews conducted.
Measures for user identification and authorization	Multi-factor authentication (MFA) enforced for all systems; Role-based access controls applied based on job function.
Measures for the protection of data during transmission	Data encrypted in transit using TLS protocols across all systems.
Measures for the protection of data during storage	Data encrypted at rest using AWS and HubSpot default security measures.
Measures for ensuring physical security of locations at which personal data are processed	AWS data centers provide physical safeguards including restricted access, surveillance, and security personnel; No local storage of customer data.
Measures for ensuring events logging	All systems produce logs for access and event tracking; BugSnag provides centralized monitoring and alerting.
Measures for ensuring system configuration, including default configuration	Secure configuration defaults used across AWS/HubSpot environments; Configurations reviewed periodically.
Measures for internal IT and IT security governance and management	Engineering leadership oversees security management, employee access, and incident response processes.
Measures for certification/assurance of processes and products	No external certifications currently (SOC2/ISO 27001 not yet performed).
Measures for ensuring data minimisation	Only limited personal data collected: name, email, phone, address.
Measures for ensuring data quality	Data reviewed during onboarding and support processes to ensure accuracy.
Measures for ensuring limited data retention	Active customers: data retained for system functionality; Churned customers: data deleted upon request.
Measures for ensuring accountability	Employee access requires agreement to confidentiality and security policies; Security training included in onboarding for relevant roles.
Measures for allowing data portability and ensuring erasure	Customers can request data export or deletion; HubSpot and internal systems support deletion/export within standard response times.
Technical and organizational measures of subprocessors	TakeUp enters into data processing agreements with all subprocessors with data protection obligations equivalent to those 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	TakeUp
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

Annex 1A: List of Parties	As per Table 1 above
Annex 2B: 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.