DATA PROCESSING ADDENDUM

This Data Processing Addendum (including all Schedules attached hereto, the "DPA") is incorporated into, and is subject to the terms and conditions of, the Clew Technology Platform Terms of Use ("Agreement") between the entity identified as Clew on the order form ("Clew") and the entity identified as the customer on the order form ("Customer"). This DPA applies to the extent Clew's Processing of Customer Personal Data is subject to the Data Protection Laws. This DPA shall be effective for the term of the Agreement.

1. Definitions

1.1. "Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

1.2. "Customer Personal Data" means the Personal Data described under Schedule 1 to this DPA.

1.3. "Data Protection Laws" means all laws and regulations, including laws and regulations of: (i) the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom; (ii) the United States (including, but not limited to the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA")); and (iii) any other jurisdiction in which the parties operate, all (i)–(iii) applicable to the Processing of Personal Data under the Agreement.

1.4. "Data Subjects" means the individuals identified in Schedule 1.

1.5. "EU SCCs" means the Standard Contractual Clauses approved with Commission Implementing Decision (EU) 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended, supplemented, updated or replaced from time to time;

1.6. "GDPR" means the General Data Protection Regulation (EU) 2016/679 together with any national implementing laws in any member state of the EEA ("EU GDPR") and the EU GDPR as incorporated into the laws of the United Kingdom ("UK GDPR");

1.7. "Personal Data" and "Processing" will each have the meaning given to them in the Data Protection Laws. The term "Personal Data" includes "personal information," "personally identifiable information," and equivalent terms as such terms may be defined by the Data Protection Laws.

1.8. "Personal Data Breach" means a material breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data.

1.9. "Processor" means the entity which Processes Personal Data on behalf of the Controller.

1.10. "Sell" has the meaning given in the Data Protection Laws.

1.11. "Service" means the services provided by Clew to Customer pursuant to the Agreement.

1.12. "Share" has the meaning given in the CCPA.

© 2026 clew – Commercial in Confidence

1.13. "UK Addendum" means the International Data Transfer Addendum to the EU SCCs, issued by the UK Information Commissioner for parties making restricted transfers, which entered into force on 21 March 2022 (collectively, with the EU SCCs, "the SCCs")

Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

2. Processing of Customer Personal Data

2.1. Customer is a Controller of Customer Personal Data and Clew is a Processor of Customer Personal Data. The details of Clew's Processing of Customer Personal Data are described in Schedule 1.

2.2. Clew will only Process Customer Personal Data as a Processor on behalf of and in accordance with Customer's prior written instructions, including any instructions provided through Customer's use of the Service. Customer hereby instructs Clew to Process Customer Personal Data to the extent necessary to provide the Service as set forth in the Agreement and this DPA. Clew shall not (1) retain, use, or disclose Customer Personal Data other than as provided for in the Agreement, as needed to provide the Service, or as otherwise permitted by Data Protection Laws; (2) retain, use, or disclose Customer Personal Data outside of the direct business relationship between Customer and Clew, including by combining Customer Personal Data with Personal Data Clew receives from third parties, other than Customer, except as permitted by the Data Protection Laws; or (3) Sell or Share Customer Personal Data. Upon notice to Clew, Customer may take reasonable and appropriate steps to remediate Clew's use of Customer Personal Data in violation of this DPA.

2.3. Clew will inform Customer if, in its opinion, an instruction from Customer infringes the Data Protection Laws. If applicable laws preclude Clew from complying with Customer's instructions, Clew will inform Customer of its inability to comply with the instructions, to the extent permitted by law.

2.4. Each of Customer and Clew will comply with their respective obligations under the Data Protection Laws. Clew shall notify Customer if it determines that it cannot meet its obligations under the Data Protection Laws. Customer has the right to take reasonable steps to ensure that Clew uses Customer Personal Data in a manner consistent with Customer's obligations under Data Protection Laws by exercising Customer's audit rights in Section 10.

3. Cross-Border Transfers of Personal Data

3.1. With respect to Customer Personal Data originating from the European Economic Area ("EEA"), the United Kingdom (the "UK") or Switzerland that is transferred from Customer to Clew, to the extent required under Data Protection Laws, the parties agree to comply with the general clauses and with "Module Two" (Controller to Processor) of the EU SCCs, which are incorporated herein by reference, with Customer as the "data exporter" and Clew as the "data importer."

3.2. For purposes of the EU SCCs the parties agree that:

3.2.1. In Clause 7, the optional docking clause will not apply.

3.2.2. In Clause 9, Option 2 will apply and the time period for prior notice of Sub-Processor changes will be as set forth in Section 5.1 of this DPA.

3.2.3. In Clause 11, the optional language will not apply.

© 2026 clew – Commercial in Confidence

3.2.4. For the purposes of Clause 15(1)(a), Clew shall notify Customer and/or Customer (only) and not the Data Subject(s) in case of government access requests and Customer and/or Customer shall be solely responsible for promptly notifying the affected Data Subjects as necessary.

3.2.5. In Clause 17, Option 1 applies and the EU SCCs shall be governed by the laws of Ireland.

3.2.6. In Clause 18(b), the parties agree to submit to the jurisdiction of the courts of Ireland.

3.2.7. In Annex I, Section A (List of Parties), (i) the Customer is the data exporter and Clew is the data importer and their identity and contact details and, where applicable, information about their respective data protection officer and/or representative in the EEA are those set forth in the Agreement or as otherwise communicated by each party to the other party; (ii) Customer is a Controller, and Clew is a Processor; (iii) the activities relevant to the data transferred under the EU SCCs relate to the provision of the Service pursuant to the Agreement; and (iv) entering into this DPA shall be treated as each party's signature of Annex I, Section A, as of the effective date of this DPA.

3.2.8. In Annex I, Section B (Description of Transfer): (i) Schedule 1 to this DPA describes Clew's Processing of Customer Personal Data; (ii) the frequency of the transfer is continuous (for as long as Customer uses the Service); (iii) Customer Personal Data will be retained in accordance with Clause 8.5 of the EU SCCs and this DPA; (iv) Clew uses the Sub-Processors listed in Schedule 3 to support the provision of the Service.

3.2.9. In Annex I, Section C (Competent Supervisory Authority), the competent supervisory authority identified in accordance with Clause 13 of the EU SCCs is the competent supervisory authority communicated by Customer to Clew.

3.2.10. In Annex II, data importer has implemented and will maintain appropriate technical and organizational measures to protect the security, confidentiality and integrity of Customer Personal Data as described in Schedule 2.

3.3. If the transfer of Customer Personal Data is subject to the Swiss Federal Act on Data Protection ("FADP"), the parties agree to rely on the EU SCCs with the following modifications: (i) the Federal Data Protection and Information Commissioner (FDPIC) will be the competent supervisory authority under Clause 13 of the EU SCCs; (ii) the parties agree to abide by the GDPR standard in relation to all Processing of Customer Personal Data that is governed by the FADP; (iii) the term "Member State" in the EU SCCs will not prevent Data Subjects who habitually reside in Switzerland from initiating legal proceedings in Switzerland in accordance with Clause 18(c) of the EU SCCs; and (iv) references to the 'GDPR' in the EU SCCs will be understood as references to the FADP.

3.4. With respect to transfers from Customer to Clew of Customer Personal Data originating from the UK, to the extent required under Data Protection Laws, the parties agree that the UK Addendum will complement the EU SCCs to the extent required under Data Protection Law. The UK Addendum is incorporated herein by reference. The parties agree that the UK Addendum is completed as follows:

3.4.1. For the purpose of Part 1 of the UK Addendum:

3.4.1.1. Table 1: the start date is the effective date of the Agreement, the exporter is the Customer and the importer is Clew, the table is deemed to be completed with the information set out in Section 3.2 of this DPA, and by signing this DPA, parties are deemed to have signed the UK Addendum.

3.4.1.2. Table 2: the "Approved EU SCCs" which the UK Addendum is appended to are the EU SCCs incorporated into this DPA and completed as set out in Section 3.2 of this DPA.

3.4.1.3. Table 3: the information requested in Annex 1 is provided in Section 3.2.8 and 3.2.9 of this DPA; the security measures requested in Annex 2 is provided in Schedule 2; the list of Subprocessors is available in Schedule 3.

3.4.1.4. Table 4: the importer may end the UK Addendum as set out in section 19 of the UK Addendum.

4. Confidentiality and Security

4.1. Clew will require Clew's personnel who access Customer Personal Data to commit to protect the confidentiality of Customer Personal Data.

4.2. Clew will implement commercially reasonable technical and organisational measures, as further described in Schedule 2, that are designed to protect against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.

4.3. To the extent required by Data Protection Laws, Clew will provide Customer with reasonable assistance as necessary for the fulfilment of Customer's obligations under Data Protection Laws to maintain the security of Customer Personal Data.

5. Sub-Processing

5.1. Customer hereby grants a general authorisation to Clew to engage Sub-Processors to Process Customer Personal Data on Customer's behalf. Clew's current list of Sub-Processors is set out in Schedule 3. Clew shall inform Customer of any intended changes concerning the addition or replacement of Sub-Processors. Customer may object to the addition of a Sub-Processor based on reasonable grounds relating to a potential or actual violation of Data Protection Law by providing written notice detailing the grounds of such objection within thirty (30) days following Clew's notification of the intended change.

5.2. Clew will impose on its Sub-Processors substantially the same data protection obligations that apply to Clew under this DPA. Clew will be liable to Customer for its Sub-Processors' acts or omissions as it would be for its own.

5.3. The parties agree that the copies of the Sub-Processor agreements that must be provided by Clew to Customer pursuant to the SCCs, if applicable, may have commercial information or clauses unrelated to the SCCs removed by Clew beforehand; and, that such copies will be provided by Clew, in a manner to be determined in its discretion, only upon Customer's written request.

6. Data Subject Rights

Customer is responsible for responding to any Data Subject requests relating to Customer Personal Data ("Requests"). If Clew receives any Requests during the term, Clew will advise the Data Subject to submit the request directly to Customer. Clew will provide Customer with reasonable assistance to permit Customer to respond to Requests.

7. Personal Data Breaches

Upon becoming aware of a Personal Data Breach affecting Customer Personal Data, Clew will (i) promptly take measures designed to remediate the Personal Data Breach and (ii) notify

Customer without undue delay. Customer is solely responsible for complying with Personal Data Breach notification requirements applicable to Customer. Customer may request that Clew reasonably assist Customer's efforts to notify Personal Data Breaches to the competent data protection authorities and/or affected Data Subjects, if Customer is required to do so under the Data Protection Laws. Clew's notice of or response to a Personal Data Breach under this Section 7 will not be an acknowledgement or admission by Clew of any fault or liability with respect to the Personal Data Breach.

8. Data Protection Impact Assessment; Prior Consultation

Customer may request reasonable assistance from Clew in connection with conducting data protection impact assessments and consultation with data protection authorities if Customer is required to engage in such activities under applicable Data Protection Laws and the data protection impact assessment or consultation relate to the Processing by Clew of Customer Personal Data.

9. Deletion of Customer Personal Data

Customer instructs Clew to delete Customer Personal Data within 90 days of the termination of the Agreement and delete existing copies unless applicable law requires otherwise. Notwithstanding the foregoing, Clew may retain Customer Personal Data to the extent and for the period required by applicable laws provided that Clew maintains the confidentiality of all such Customer Personal Data and Processes such Customer Personal Data only as necessary for the purpose(s) specified in the applicable laws requiring its storage.

10. Audits

10.1. Customer may audit Clew's compliance with its obligations under this DPA up to once per year. In addition, Customer may perform more frequent audits (including inspections) in the event: (1) Clew suffers a Personal Data Breach affecting Customer Personal Data; or (2) where required by the Data Protection Laws, including where mandated by regulatory or governmental authorities with jurisdiction over Customer Personal Data. Clew will contribute to such audits by providing Customer or Customer's regulatory or governmental authority with the information and assistance reasonably necessary to conduct the audit, including any relevant records of Processing activities applicable to the Service, as described below.

10.2. To request an audit, Customer must submit a detailed proposed audit plan to contact@clew.io at least one month in advance of the proposed audit start date. The proposed audit plan must describe the proposed scope, duration, start date of the audit, and the identity of any third party Customer intends to appoint to perform the audit. Clew will review the proposed audit plan and provide Customer with any concerns or questions (for example, Clew may object to the third party auditor as described in Section 10.3, provide an Audit Report as described in Section 10.4, or identify any requests for information that could compromise Clew confidentiality obligations or security, privacy, employment or other relevant policies). The parties will negotiate in good faith to agree on a final audit plan at least two weeks in advance of the proposed audit start date. Nothing in this Section 10 shall require Clew to breach any duties of confidentiality.

10.3. Clew may object to third party auditors that are, in Clew's reasonable opinion, not suitably qualified or independent, a competitor of Clew, or otherwise manifestly unsuitable. Customer will appoint another auditor or conduct the audit itself if the parties cannot resolve Clew's auditor objection after negotiating in good faith.

© 2026 clew – Commercial in Confidence

10.4. If the requested audit scope is addressed in an SSAE 18/ISAE 3402 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor on Clew's systems that Process Customer Personal Data ("Audit Reports") within twelve (12) months of Customer's audit request and Clew confirms there are no known material changes in the controls audited, Customer agrees to accept the Audit Report in lieu of requesting an audit of the controls covered by the Audit Report.

10.5. The audit must be conducted at a mutually agreeable time during regular business hours at the applicable facility, subject to the agreed final audit plan and Clew's health and safety or other relevant policies. The audit may not unreasonably interfere with Clew business activities.

10.6. Any audits are at Customer's expense and Customer will promptly disclose to Clew any perceived non-compliance or security concerns discovered during the audit, together with all relevant details.

10.7. The parties agree that the audits described in the SCCs, if applicable, shall be performed in accordance with this Section 10.

11. Liability

11.1. Each party's liability towards the other party under or in connection with this DPA will be limited in accordance with the provisions of the Agreement.

11.2. Customer acknowledges that Clew is reliant on Customer for direction as to the extent to which Clew is entitled to Process Customer Personal Data on behalf of Customer in performance of the Service. Consequently, Clew will not be liable under the Agreement for any claim brought by a Data Subject arising from (a) any action or omission by Clew in compliance with Customer's instructions or (b) from Customer's failure to comply with its obligations under the Data Protection Laws.

12. General Provisions

12.1. With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA shall prevail. In the event of inconsistencies between the DPA and the SCCs, the SCCs will prevail.

12.2. This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

© 2026 clew – Commercial in Confidence

SCHEDULE 1

Details of Processing

1. Categories of Data Subjects. This DPA applies to Clew's Processing of Customer Personal Data relating to Customer's personnel ("Data Subjects").

2. Types of Personal Data. The extent of Customer Personal Data Processed by Clew is determined and controlled by Customer in its sole discretion and includes names, email addresses, and any other Personal Data that may be transmitted through the Service by Data Subjects. Customer Personal Data does not include any special category of personal data that, pursuant to Data Protection Laws, require higher levels of protection due to its sensitive nature, except to the extent expressly set out in this section.

3. Subject-Matter and Nature of the Processing. Customer Personal Data will be subject to the Processing activities that Clew needs to perform in order to provide the Service pursuant to the Agreement.

4. Purpose of the Processing. Clew will Process Customer Personal Data for purposes of providing the Service as set out in the Agreement.

5. Duration of the Processing. Customer Personal Data will be Processed for the duration of the Agreement, subject to Section 9 of the DPA.

© 2026 clew – Commercial in Confidence

SCHEDULE 2

Technical and organisational measures to ensure the security of the Customer Data

Clew has implemented the following technical and organizational measures:

1. Physical and Separation Control – AWS Data Centre

Clew uses Amazon Web Services (AWS) to host its infrastructure. Physical access to systems processing Personal Data is protected through AWS's industry-certified data centre security controls, including perimeter protection, surveillance, and access restrictions to authorised personnel. AWS maintains compliance with ISO 27001, SOC 1/2/3, and other recognised security standards.

Clew is certified to ISO 27001 and Cyber Essentials Plus, both of which are recognised standards for information security management.

Clew enforces logical separation of customer environments and data through its platform architecture. development, staging, and production environments are segregated to prevent unauthorised cross-environment access.

2. Virtual Access Control – Application Level

Clew implements measures at the application level to prevent unauthorised access to systems processing Personal Data. These include single sign-on (SSO), role-based access controls (RBAC), strong password policies, session timeout and account lockout features, and multi-factor authentication for privileged accounts. Clew also conducts regular penetration testing and security assessments to identify and address vulnerabilities within the application environment.

3. Data Access Control – Customer Configuration

While Clew provides the tools and access framework, clients are responsible for correctly configuring and managing user permissions within their own environments. Access is granted based on business need, with defined procedures for approval, modification, and removal. Clew provides the means for the customer to apply role-based and attribute-based access controls (alongside audit logging and encryption) to ensure that Personal Data is accessible only to authorised users.

4. Disclosure Control

Personal Data is protected during transmission through encryption and secure communication protocols such as TLS. Data is transmitted via secure channels including HTTPS, SFTP, and VPN, with all transfers logged and auditable. Clew maintains regular data backups and implements business continuity measures to support data availability and recoverability. In the event of a critical incident, Clew has defined procedures in place to restore services or migrate to an alternative hosting provider to maintain continuity of service.

5. Entry Control – Audit Logging

Clew maintains a complete audit history of activity related to the creation, modification, and deletion of Personal Data within its systems. All relevant user actions are logged with associated timestamps and user identifiers, enabling full traceability of changes. These audit trails are regularly reviewed to detect unauthorised or anomalous activity and are retained in accordance with Clew's data retention and security policies.

© 2026 clew – Commercial in Confidence

6. Availability Control – Data Backup & Resilience

Regular, encrypted backups are performed, and data is stored across multiple availability zones within certified cloud infrastructure to ensure high availability and fault tolerance. Clew's hosting providers maintain infrastructure-level redundancy, uninterruptible power supplies, and failover capabilities. A documented disaster recovery and business continuity plan is in place, with testing conducted periodically to ensure continued operational resilience.

© 2026 clew – Commercial in Confidence

SCHEDULE 3

Sub-Processor List

Amazon Web Services (AWS)

© 2026 clew – Commercial in Confidence