



Clew
G-Cloud 15
Terms and Conditions Document

OVERVIEW

Clew's standard Terms of Use document contains reference to our Service Level Agreement (SLA) and Data Protection Agreement (DPA). Typically, these are embedded web links – however, noting the G-Cloud contractual obligations for these to remain unchanged we have provided fixed forms of all three elements in this document. These are provided in 3 Annexes:

Annex 1. Clew Terms of Use.

Annex 2. Service Level Agreement (SLA).

Annex 3. Data Protection Addendum (DPA).

ANNEX 1: TERMS OF USE

These Platform Terms of Use ("*Terms*") apply to any order form ("*Order Form*") incorporating these Terms for which Customer may use the Technology Platform. Corporate Governance Risk operates under the trading name "Clew Software" and all references to "Clew" in these Terms refer to Corporate Governance Risk entity as specified in the applicable Order Form. References to this Agreement mean the Order Form, the Appendices and any executed statements of work between the parties, together with these Terms. Capitalised terms shall have the meanings given to them in the Order Form unless otherwise defined in these Terms.

1. TECHNOLOGY PLATFORM

- 1.1. Clew will make its platform ("*Technology Platform*") available to Customer pursuant to this Agreement and grants to the Customer a limited, revocable, non-sublicensable, non-exclusive, non-transferable right during the Term to allow the Customer's authorized employees and contractors ("*Users*") to access and use the Technology Platform, subject to any Usage Limitations set forth in the applicable Order Form. The Customer is responsible for all activities conducted under the Users logins on the Technology Platform.
- 1.2. Clew will maintain a security program materially in accordance with industry standards designed to: (a) ensure the security of data uploaded or made available to the Technology Platform by Customer and output produced for Customer via use of the Technology Platform by Customer (collectively, "*Customer Data*"); and (b) prevent unauthorised access to Customer Data. Clew's security safeguards include measures for preventing access, modification or disclosure of Customer Data by Clew personnel except: (i) to provide the Technology Platform and prevent or address problems; (ii) as required by applicable law; or (iii) as permitted herein or by Customer. Clew will not materially diminish the protections provided herein.
- 1.3. The rights granted herein are subject to the following "*Licence Restrictions*". Customer will not directly or indirectly: (a) reverse engineer, decompile (except to the extent that such actions cannot be restricted under applicable law), modify, create derivative works of or otherwise create or derive the Technology Platform's source code; (b) breach the security of the Technology Platform or render it unusable for any user; (c) use the Technology Platform or Clew Confidential Information to develop a product or service that competes with Clew; (d) transfer, resell, license, or assign the Technology Platform; or (e) use the Technology Platform in violation of applicable law, to infringe third party rights or

outside the scope permitted hereunder. If Clew processes personal data on behalf of Customer when providing any services in connection with this Agreement, the data processing terms found at Annex 3 shall apply. Unless authorised in the Order Form or otherwise by Clew in writing, Customer agrees not to upload to the Technology Platform any special category of personal data that, pursuant to applicable data protection laws, require higher levels of protection due to its sensitive nature.

- 1.4. Customer: (a) will comply with applicable laws; (b) will provide (in a diligent and timely manner) all cooperation, personnel and materials specified by Clew; (c) is responsible for all use of the Technology Platform under its account (including all permission settings managed through its account) and for ensuring it is authorised to use and make available all Customer Data to the Technology Platform; (d) will use reasonable endeavours to prevent unauthorised access to the Technology Platform and notify Clew promptly of any unauthorised access; and (e) is solely responsible for obtaining and maintaining any equipment, software and ancillary services needed to use the Technology Platform. Open source libraries are provided in connection with the Technology Platform, are made available on request and are licensed pursuant to the terms of the applicable open source licence.

2. PROFESSIONAL SERVICES

- 2.1. Clew and Customer may enter into statements of work relating to specific professional services to be performed by Clew ("*Professional Services*"). Each statement of work executed by the parties ("*Statement of Work*") will form a part of and will be subject to the terms of this Agreement. Customer may submit to Clew written requests to change the scope of Professional Services described in a Statement of Work (each such request, a "*Change Order Request*"). If Clew elects to consider such a Change Order Request, then Clew will promptly notify Customer if it believes that the Change Order Request requires an adjustment to the fees or to the schedule for the performance of the Professional Services. In such event, the parties will negotiate in good faith a reasonable and equitable adjustment to the fees and/or Statement of Work, as applicable. Clew will continue to perform Professional Services pursuant to the existing Statement of Work and will have no obligation to perform any Change Order Request unless and until the parties have agreed in writing to such an equitable adjustment.

3. UPDATES AND SUPPORT

- 3.1. Updates for the Technology Platform ("*Updates*") will be provided from time to time by Clew and the Customer shall accept and assist with the implementation of the Updates when they are made generally available.
- 3.2. During the Term, Clew shall provide the Customer its standard support services in accordance with the Service Level Agreement appended to these Terms, conditional upon Customer's compliance with clause 3.1. The Technology Platform may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by Clew or by third-party providers, or because of other causes beyond Clew's reasonable control, but Clew shall use reasonable efforts to provide advance notice in writing or by e-mail of any scheduled service disruption.

4. FEES

- 4.1. Customer will pay Clew the fees set forth in the Order Form and any applicable Statements of Work within 30 days of receipt of Clew's invoice. Except as otherwise specified, fees are: (a) payable in the currency set forth in the Order Form or Statements of Work (as applicable); and (b) non-cancellable, non-proratable for partial months, and non-refundable, except as set forth herein.
- 4.2. Fees for each year of the Term shall be set out in the Order Form. Unless otherwise specified in a renewal Order Form, fees for each year of the Renewal Term shall be set at Clew's then-current list price.
- 4.3. Clew may suspend access to the Technology Platform upon notice if Customer fails to pay any amounts hereunder 5 days or more after their due date. If Customer disputes an invoice received from Clew, Customer must notify Clew in writing within 15 days of receiving the relevant invoice.
- 4.4. All amounts payable hereunder are exclusive of any sales, use and other taxes or duties ("*Taxes*"). Customer will not withhold Taxes from amounts due to Clew unless required by applicable law, in such circumstances the amount due from Customer shall be increased to an amount which (after making such withholding) leaves an amount equal to the payment which would have originally been due.

5. PROPRIETARY RIGHTS AND CONFIDENTIALITY

- 5.1. As between the parties, Clew owns the Technology Platform, Derived Data, and Clew's Confidential Information, and Customer owns Customer Data and

Customer's Confidential Information. Customer grants to Clew, its affiliates and applicable contractors a licence during the Term to host, copy, transmit and display Customer Data, as reasonably necessary for Clew to perform this Agreement. "*Derived Data*" means any data which is derived from the Customer's use of the Technology Platform or the processing by Clew of Customer Data, which will include: (i) aggregated and anonymised Customer Data, provided that such aggregated and anonymised data does not identify the Customer or any individual and cannot reasonably be re-identified; (ii) statistical data; (iii) any data which is processed and stored as mathematical constructs ; and (iv) data regarding web applications utilized in connection with the Technology Platform, configurations, log data, and the performance results for the Technology Platform. Customer may provide Clew with suggestions for new or enhanced features ("*Feedback*"). Clew has the full, unencumbered right, without any obligation to compensate Customer, to exploit such Feedback.

- 5.2. The Technology Platform integrates with certain third party content and/or technology controlled by or licensed to the Customer. Clew does not endorse or approve any third party content or technology, and makes no representation, warranty or commitment and shall have no liability or obligation whatsoever in relation to such content and technology or its integration with the Technology Platform.
- 5.3. Each party will use any information disclosed (whether before or after the Effective Date of this Agreement) directly or indirectly by the other that should reasonably be understood to be confidential ("*Confidential Information*") solely in accordance with this Agreement and, except as permitted hereunder, not disclose the same to any third party without the other's prior written consent, provided that information which: (a) is in the public domain through no fault of receiving party; (b) was properly known to receiving party, without restriction, prior to disclosing party's disclosure; (c) was properly disclosed to receiving party, without restriction, by another person with authority to do so; or (d) is independently developed by receiving party without use of or reference to disclosing party's Confidential Information is not Confidential Information. Furthermore, either party may disclose Confidential Information: (a) to its personnel and representatives who need to know it and are legally bound to keep it confidential by obligations consistent with those herein; and (b) as required by law (in which case the receiving party will provide the disclosing party with prior written notification and the opportunity to contest disclosure, and use its reasonable endeavours to minimise disclosure to the extent permitted by applicable law). Neither party will disclose the terms of this Agreement to any third party, except that it may confidentially disclose them to actual or potential lenders, investors or acquirers and Clew may refer to Customer's name and

trademarks in its marketing materials and website. Each party agrees to exercise due care in protecting Confidential Information from unauthorised use and disclosure. In the event of a breach of this Section or the Licence Restrictions, the non-breaching party will, notwithstanding anything herein, be entitled to seek injunctive and other equitable relief in any jurisdiction. Each party will promptly notify the other in writing if it becomes aware of any violations of this Section.

6. WARRANTIES AND DISCLAIMERS

- 6.1. Clew warrants that (a) the Technology Platform will materially conform with the technical specifications provided by Clew to Customer; and (b) any support services will be provided in a professional and workmanlike manner. As sole and exclusive remedy and Clew's entire liability for any breach of the foregoing warranty, Clew will, at its sole option and expense, as applicable, promptly correct the non-conforming Technology Platform, or re-perform any services that fail to meet this limited warranty.
- 6.2. Customer warrants that: (i) it has all rights necessary to provide any data (including Customer Data), information or other materials it provides to the Technology Platform or Clew, and to permit Clew to use the same as contemplated herein; (b) it has obtained all consents, permissions and authorizations required under applicable data protection laws for the processing of personal data by Clew in accordance with this Agreement; and (c) its provision to Clew and use by Clew of the Customer Data as permitted by this Agreement will not infringe any third party intellectual property rights.
- 6.3. Except as set forth herein, the Technology Platform and all related services provided by Clew are provided "as is", and Clew hereby disclaims any and all warranties, express or implied, including warranties of merchantability, title, non-infringement, and fitness for a particular purpose. Without limiting the foregoing, Clew does not warrant that the Technology Platform or any related services provided by Clew will be uninterrupted or error free, nor does it make any warranty as to the results that may be obtained from the use of the Technology Platform.

7. INDEMNIFICATION

- 7.1. Clew will defend Customer against any claim brought against it by a third party alleging that use of the Technology Platform infringes its intellectual property rights and will, subject to Section 8, indemnify Customer for damages finally awarded by a court of competent jurisdiction against Customer (or any Clew

approved settlement) in connection with such claim. If the use of the Technology Platform has become, or in Clew's opinion is likely to become, subject to any infringement claim, Clew may: (a) procure the right for Customer to continue using the Technology Platform as set forth herein; (b) replace the Technology Platform to make it non-infringing (with comparable functionality); or (c) terminate this Agreement and provide a pro rata refund of prepaid fees. Clew will have no Liability with respect to any claim to the extent caused by: (i) use of the Technology Platform other than as permitted hereunder; (ii) compliance with designs, guidelines or specifications provided by Customer; (iii) Customer's use of any downloadable component of the Technology Platform other than the latest version made available; (iv) modification of the Technology Platform by any party other than Clew without Clew's written consent; (v) Customer Data or Customer Confidential Information; or (vi) the combination, operation or use of the Technology Platform with other applications, products or services, in each case provided such combination, operation or use causes the infringement. This Section represents Customer's exclusive remedy for any claim related to infringement or misappropriation of intellectual property.

- 7.2. When a party ("*Indemnifier*") is to indemnify the other ("*Indemnified Party*") then: (a) the Indemnified Party shall promptly notify Indemnifier of the Claim in writing; (b) Indemnifier shall be given exclusive authority to defend and settle such Claim (provided that it may not settle without the Indemnified Party's prior written consent, not to be unreasonably withheld, conditioned or delayed); and (c) the Indemnified Party shall reasonably cooperate with Indemnifier in connection with such Claim.

8. LIMITATION OF LIABILITY

- 8.1. Nothing in this Agreement excludes or restricts any liability arising under, out of or in connection with this Agreement, whether or not foreseeable or in the contemplation of the parties at any time, in or under contract, tort (including negligence), indemnity, breach of statutory duty, misrepresentation, restitution or otherwise for: (a) anything that cannot be excluded or restricted under applicable law; (b) wilful default; (c) Customer's payment obligations; or (d) any breach of the Licence Restrictions by Customer.
- 8.2. Subject to clause 8.1, neither party has any liability for any: (a) indirect, special or consequential loss; (b) loss of goodwill; (c) loss of actual or anticipated profits (d) lost sales or business; (e) work stoppage; (f) computer failure or malfunction; (g) damage to equipment; or (h) lost content or data.

- 8.3. Subject to clause 8.1, the total aggregate liability of a party for all claims shall not exceed the amounts paid by Customer under the applicable Order Form in the 12 months preceding the incident or claim, less any amounts already paid or payable by that party to the other party (including by way of damages, settlement or otherwise) in connection with any previous incidents or claims.

9. TERM AND TERMINATION

- 9.1. This Agreement begins on the Effective Date of the Order Form and continues for the Initial Subscription Term, as specified in the Order Form ("Initial Subscription Term"). Thereafter, this Agreement shall automatically renew for successive terms equal to the length of its Initial Subscription Term or such other period as is mutually agreed in writing ("Renewal Term"), unless terminated in accordance with this Agreement. The Initial Subscription Term and any Renewal Term shall together be the "Term" of this Agreement.
- 9.2. Either party may terminate this Agreement on written notice to the other party on at least 30 days' notice, to take effect no earlier than the end of the Initial Subscription Term or then-current Renewal Term (as applicable). Each party may further terminate this Agreement upon written notice to the other party if: (a) the other party commits any material breach of this Agreement and fails to remedy such breach within 30 days after written notice of such breach; or (b) subject to applicable law, upon the other party's liquidation, commencement of dissolution proceedings or assignment of substantially all its assets for the benefit of creditors, or if the other party becomes the subject of insolvency or similar proceedings that are not dismissed within 60 days.
- 9.3. Upon expiry or termination of this Agreement: (a) the Customer will immediately discontinue use of the Technology Platform and; (b) Clew will return or destroy all copies of the Customer Data in its possession and control, and certify destruction (if applicable) to Customer within 40 days of termination. All rights and obligations will immediately terminate, except that accrued payment obligations and any terms that by their nature should survive such termination will survive, including the Licence Restrictions and terms and conditions relating to proprietary rights and confidentiality, disclaimers, indemnification, limitations of liability, termination and the general provisions below.

10. GENERAL

- 10.1. Customer agrees that Customer's use of the Technology Platform will comply with applicable export control and trade sanctions laws, rules and regulations

(collectively, "*Export Control Laws*"). Customer represents and warrants that no content created or submitted by Customer is or will be subject to any restriction on disclosure, transfer, download, export or re-export under the Export Control Laws. Customer agrees that it will not use the Technology Platform to disclose, transfer, download, export or re-export, directly or indirectly, any content to any country, entity or other party which is ineligible to receive such items under the Export Control Laws or under other laws or regulations to which Licensee may be subject. Customer acknowledges that the Technology Platform may not be available in all jurisdictions and that Customer is solely responsible for (i) complying with the Export Control Laws and (ii) monitoring them for any modifications.

- 10.2. Neither party shall have Liability to the extent caused by events beyond its reasonable control, including war or terrorist activity, riot, civil commotion, malicious damage, pandemics or epidemics, strike, lock-outs, or other industrial disputes, natural disaster, act of god, pandemic, cyber-attacks, power outage, failure of third party or customer software, hardware or network, any change in law, fire, flood, adverse weather conditions, or default of suppliers or sub-contractors, and other than set out herein has no obligation to take any action to prevent or mitigate such events.
- 10.3. Neither party may assign or transfer this Agreement without the other's prior written consent unless such assignment is to a successor to substantially all of its assets or business related to this Agreement or an affiliate.
- 10.4. No amendment to this Agreement, nor waiver of any rights hereunder, is effective unless mutually agreed. Failure or delay by either party to enforce this Agreement will not be deemed a waiver of future enforcement.
- 10.5. Nothing herein establishes any partnership, agency, employment or joint venture between the parties. Neither party has authority to bind the other, and nothing herein gives rise or is intended to give rise to any rights of any kind to any third parties (whether under the Contracts (Rights of Third Parties) Act 1999 or otherwise).
- 10.6. If a court of competent jurisdiction determines that any provision of this Agreement is invalid or unenforceable, such provision will be enforced as nearly as possible in accordance with the intention of the parties, while the remainder of this Agreement remains in full force. "Including" means "including without limitation".
- 10.7. This Agreement comprises the entire agreement between the parties with respect to its subject matter, supersedes all other proposals, statements,

materials and agreements (oral and written) and all statements, representations and warranties on which each party relies are incorporated into this Agreement. Neither party has a remedy for any statement, representation (including misrepresentation) or warranty (whether negligent or innocent) of any person not expressly set out herein and each party waives all rights and remedies which, but for this clause, might otherwise be available to it in respect of any such statement, representation or warranty. No terms contained in any purchase order or other document issued by Customer form part of any contract between the parties.

- 10.8. This Agreement, together with any dispute arising out of or in connection with it or its subject matter, is governed by the laws of England. Each party irrevocably agrees that the courts of London, England, have exclusive jurisdiction to settle any dispute under this Agreement.
- 10.9. Any notice hereunder will be given using the details in the latest effective Order Form and in writing by personal delivery, certified mail, return receipt requested or email provided no automated bounceback is received.
- 10.10. In the event of a conflict or inconsistency among the following documents, the order of precedence will be, in descending order (a) any Statement of Work; (b) any Order Form; and (c) these Terms.

ANNEX 2: SERVICE LEVEL AGREEMENT (SLA)

Definitions

"Availability" or "Available" means that the Technology Platform is available to be used by Customer materially as is described in the Agreement and is calculated as follows: in relation to a calendar month means the proportion of the calendar month when Users can or could substantially operate the Software, calculated by subtracting from 100% the percentage of minutes during that calendar month in which the Software was not accessible to Users, excluding periods resulting directly or indirectly from any exceptions set out in clause 2 of this Service Level Agreement.

"Availability Commitment" means the Technology Platform will be Available ninety-nine point nine percent (99.9%) of the time. The Availability Commitment does not include downtime resulting from the Exclusions.

"Business Day" means a day on which banks are open for general banking business in Australia or the UK - excluding Saturdays, Sundays or public holidays.

"Configuration Error" means any configuration settings that are not aligned with customer requirements.

"Customer Support Request" means a request raised from Level 2 for support from Clew, whether in relation to a suspected Error, system knowledge or wider support (such as configuration changes or training).

"Error" means either a Configuration Error or a Product Error.

"Exclusions" means:

suspension of Customer's access to the Technology Platform pursuant to the Agreement;

- breach of the Agreement (Excluding where the customer can evidence (to the reasonable satisfaction of Clew) that it has made best efforts to comply with the Agreement), negligence, or unlawful act or omission of the Customer, its representatives or service providers (other than Clew);
- disengagement of functionality of the Technology Platform, or service or resource reduction, due to a request from Customer;
- Customer's or its service provider's equipment, computer systems or networks, software, hardware, data (including Customer Data) or other technology;
- events beyond Clew's reasonable control as further described in clause 10.2 of the Agreement; or A Scheduled Upgrade Period.

"Knowledge Base" means Clew's repository of knowledge content related to the Technology Platform, access of which is made available to Customers during onboarding.

"Product Error" means any technical error (such as system outage or application bug) of the Technology Platform to perform in accordance with the technical specifications provided by Clew, or which causes the Technology Platform to display an error message due to the Technology Platform performing otherwise in accordance with its published functionality. Errors do not include queries about configuration changes, new features, and generic queries unrelated to any failure of or error in the Technology Platform.

"Professional Services" means any services required in relation to system configuration, including support required to fix a configuration as identified above (whether or not caused by the customer or Clew).

"Support Levels" define Licensor and Licensee responsibilities for resolving user support requests as follows:

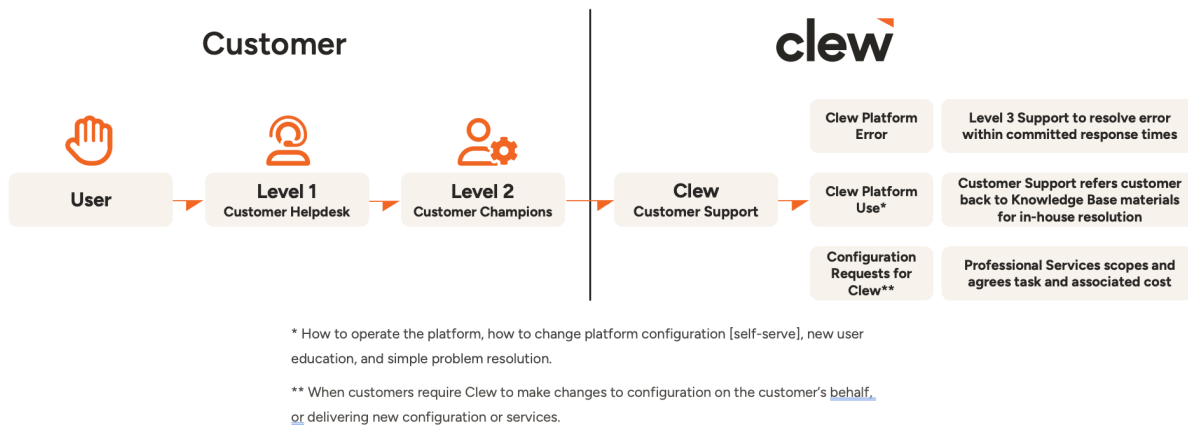
- Level 1 support is provided by **Customer Helpdesk** (usually IT support) and deals with all user management including login issues, as well as browser queries, and other IT basics. Suspected Errors and configuration/training issues are escalated to Level 2.
- Level 2 support is provided by **Customer Champions** (also known as subject matter experts), and deals with authorisation, alignment with policies & procedures, and training and configuration queries relating to software data fields, process flows, notifications and dashboards. Suspected Errors, and requests for Professional Services are escalated to Level 3.
- Level 3 support is requested, coordinated and delivered via Clew Customer Support which is accessible to (and only to be used by) identified Customer Champions by raising the request via: support@clew.io

"Technical Services Support" means any support required to fix a Product Error as defined above.

"Warranty Issue" means any Configuration Error that is the result of Clew failure to deliver configuration in accordance with specification during implementation.

Support Response Process

Clew's support and escalation model is visualised with the following diagram:



When reporting a Customer Support Request, the Customer Champion must provide any information relating to the Error reasonably requested by Clew. When an Error is reported, Clew will:

1. Determine whether the request relates to a Product Error requiring Technical Services Support, an escalated Warranty Issue requiring Professional Services support, or a knowledge issue that could be resolved in-house at Level 1-2.
2. If the request is not related to a Product Error or Warranty Issue, Clew will on a best endeavours basis ensure that the Customer Champion is aware of any Knowledge Base articles that would help them resolve the issue in-house or otherwise confirm that Professional Services is required and scope the delivery effort required in accordance with "Professional Services" below.
3. If the request is related to a Product Error, log and issue a support services reference number to Customer and:
 - a. Determine and agree with Customer a severity level for the Product Error in accordance with the response times in the table below and having regard to the degree to which the Product Error deprives Customer of functionality;
 - b. Respond to and action the Product Error in accordance with the time frames set out in the response times in the table below;
 - c. Provide Customer with an update in relation to the status of the Product Error upon request; and
 - d. Advise Customer, in writing, when the Product Error is resolved.

Product Error Correction Response

Customers contracted to Clew Australia will be serviced based on Australian business hours (9am-5pm) on Business Days; customers contracted to Clew UK or Clew Canada will be serviced based on UK business hours (9am-5pm) on Business Days.

Severity Level	Definition	Communication	Resolution Target
1	- No user can log in, disrupting critical business processes (e.g., complete outage). - Multiple clients unable to submit essential data. - Data corruption affecting accuracy of reporting or essential client records. - Severe performance issues causing the application to be unusable (e.g., pages fail to load entirely). - Security Breach including PII Data	Response within 1 business hour	6 business hours
2	- Single or multiple users unable to access key features, significantly affecting productivity (e.g., report generation functionality intermittently failing). - Multiple users experiencing frequent disconnects or errors that require workarounds. - Critical performance degradation impacting multiple users' productivity, but application remains functional.	Response within 2 business hours	1 business day (subject to QA checks prior to resolution confirmation)
3	- Minor bugs affecting individual client workflows but with simple and effective workarounds (e.g., UI glitch requiring page refresh). - Non-critical technical performance degradation causing slight delays without significant productivity loss.	1 business day	3 business days

Service Credits

If Clew fails to meet the Availability Commitment, the Customer will be eligible to receive a service credit, calculated as a percentage of the monthly subscription fee for the affected module of the Technology Platform, in the affected month, as set out in the table below:

Monthly Availability	Service Credit (% of monthly fee)
99.0% – 99.89%	5%
98.0% - 98.99%	10%
Less than 98.0%	20% (cap)

Service credits may only be applied against future invoices and have no cash value. The total amount of service credits that may be claimed by the Customer in any calendar month is capped at 20% of the applicable monthly subscription fee.

The Customer must submit a written claim for a service credit within thirty (30) days after the end of the calendar month in which the Availability Commitment was not met. Failure to submit a claim within this timeframe will result in forfeiture of the right to receive a service credit for that period.

Service credits will constitute the Customer's sole and exclusive remedy for any failure by Clew to meet the Availability Commitment.

Platform Upgrades

Clew upgrades the Technology Platform every 4 months. As part of this process, Clew follows these steps:

- A notification is sent about the upgrade 30 days before the upgrade date.
- The notification contains a changelog with all changes that will be applied to the platform, including changes to functionality and API.
- Clew then proceeds to upgrade the test environment [if available] for each Customer.
- The Customer then schedules the production upgrade in one of the time windows available via an online form. The period within which the production upgrade is installed is the "Scheduled Upgrade Period".

Professional Services

For Level 3 support escalations that are not Product Errors or Warranty Issues and that require support from Professional Services, Clew will assess the level of effort and secure

written approval from with the customer before proceeding with the work; funding for the work will be drawn down against a customer's contracted Support and Services Package. If a customer has not opted for a Support and Services Package, it will be charged at the day-rate identified in the contract pending confirmation of applicable Purchase Order and written approval from the customer.

Service Exclusions

Clew has no obligation to resolve Configuration Errors resulting from an Exclusion. If Clew elects to correct such Errors, such remediation services will be charged on a time and materials basis in accordance with Clew's then current rate card.

Service Obligations

Application Maintenance and Support Service Responsibilities

- **Break Fixes and Patches:** Clew will carry out break fixes and apply patches to maintain access to and use of the Technology Platform.
- **Software Updates:** Clew will provide software updates from time to time and the Customer shall accept and assist with the implementation of the Updates when they are made generally available.

ANNEX 3: DATA PROTECTION ADDENDUM (DPA)

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.
- 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.
- 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.
- 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.

DPA 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.

DPA SCHEDULE 2

Technical and organisational measures to ensure the security of 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.

DPA SCHEDULE 3

Sub-Processor List

Amazon Web Services

Clew Software

ABN: 16 148 000 980

Level 2, 267 St Georges Terrace, Perth

Western Australia 6000

Telephone: +61 8 9384 7000

www.clew.io

Clew

Company No: 09098835

The Blade, Abbey Square,

Reading, Berkshire, RG1 3BE

Telephone: +44 118 205 9378

www.clew.io

Clew

Corporation Number: 1236934-6

102-99 Holland Avenue

Ottawa, Ontario, Canada K1Y 0Y1

Telephone: +1 613 297 8717

www.clew.io