Bonterms Data Protection Addendum (DPA)
(Version 1.0)

This Data Protection Addendum ("**DPA**") is an Attachment to the **Agreement**. Customer and Provider enter into this DPA by executing a DPA Setup Page. Capitalized terms not defined in this DPA are defined in the Agreement or DPA Setup Page.

1. Definitions.

1.1. "**Agreement**" means the Agreement between Customer and Provider incorporating the Bonterms Cloud Terms which is specified on the DPA Setup Page.

1.2. "**Audit**" and "**Audit Parameters**" are defined in Section 9.3 below.

1.3. "**Audit Report**" is defined in Section 9.2 below.

1.4. "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.

1.5. "**Customer Instructions**" is defined in Section 3.1 below.

1.6. "**Customer Personal Data**" means Personal Data in Customer Data (as defined in the Agreement).

1.7. "**Data Protection Laws**" means all laws and regulations applicable to the Processing of Customer Personal Data under the Agreement, including, as applicable: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder ("**CCPA**"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**" or "**GDPR**"), (iii) the Swiss Federal Act on Data Protection ("**FADP**"), (iv) 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**") and (v) the UK Data Protection Act 2018; in each case, as updated, amended or replaced from time to time.

1.8. "**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates.

1.9. "**DPA Effective Date**" is specified on the DPA Setup Page.

1.10. "**DPA Setup Page**" means a separate document executed by Customer and Provider which causes this DPA to become an Attachment to their Agreement.

1.11. "**EEA**" means European Economic Area.

1.12. "**Key Terms**" means Agreement, DPA Effective Date and Subprocessor List as specified by the parties on the DPA Setup Page.

1.13. "**Personal Data**" means information about an identified or identifiable natural person or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Data Protection Laws.

1.14. "**Processing**" and inflections thereof refer to any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.15. "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

1.16. "**Restricted Transfer**" means: (i) where EU GDPR applies, a transfer of Customer Personal Data from the EEA to a country outside the EEA that is not subject to an adequacy determination, (ii) where UK GDPR applies, a transfer of Customer Personal Data from the United Kingdom to any other country that is not subject to an adequacy determination or (iii) where FADP applies, a transfer of Customer Personal Data from Switzerland to any other country that is not subject to an adequacy determination.

1.17. "**Schedules**" means one or more schedules incorporated by the parties in their DPA Setup Page. The default Schedules for this DPA are:

Schedule 1	Subject Matter and Details of Processing
Schedule 2	Technical and Organizational Measures
Schedule 3	Cross-Border Transfer Mechanisms
Schedule 4	Region-Specific Terms

1.18. "**Security Incident**" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data being Processed by Provider.

1.19. "**Specified Notice Period**" is 48 hours.

1.20. "**Subprocessor**" means any third party authorized by Provider to Process any Customer Personal Data.

1.21. "**Subprocessor List**" means the list of Provider's Subprocessors as identified or linked to on the DPA Setup Page.

2. Scope and Duration.

2.1. Roles of the Parties. This DPA applies to Provider as a Processor of Customer Personal Data and to Customer as a Controller or Processor of Customer Personal Data.

2.2. Scope of DPA. This DPA applies to Provider's Processing of Customer Personal Data under the Agreement to the extent such Processing is subject to Data Protection Laws. This DPA is governed by the governing law of the Agreement unless otherwise required by Data Protection Laws.

2.3. Duration of DPA. This DPA commences on the **DPA Effective Date** and terminates upon expiration or termination of the Agreement (or, if later, the date on which Provider has ceased all Processing of Customer Personal Data).

2.4. Order of Precedence. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) any Standard Contractual Clauses or other measures to which the parties have agreed in Schedule 3 (Cross-Border Transfer Mechanisms) or Schedule 4 (Region-Specific Terms), (2) this DPA and (3) the Agreement. To the fullest extent permitted by Data Protection Laws, any claims brought in connection with this DPA (including its Schedules) will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations, set forth in the Agreement.

3. Processing of Personal Data.

3.1. Customer Instructions.

(a) Provider will Process Customer Personal Data as a Processor only: (i) in accordance with Customer Instructions or (ii) to comply with Provider's obligations under applicable laws, subject to any notice requirements under Data Protection Laws.

(b) "**Customer Instructions**" means: (i) Processing to provide the Cloud Service and perform Provider's obligations in the Agreement (including this DPA) and (ii) other reasonable documented instructions of Customer consistent with the terms of the Agreement.

(c) Details regarding the Processing of Customer Personal Data by Provider are set forth in Schedule 1 (Subject Matter and Details of Processing).

(d) Provider will notify Customer if it receives an instruction that Provider reasonably determines infringes Data Protection Laws (but Provider has no obligation to actively monitor Customer's compliance with Data Protection Laws).

3.2. Confidentiality.

(a) Provider will protect Customer Personal Data in accordance with its confidentiality obligations as set forth in the Agreement.

(b) Provider will ensure personnel who Process Customer Personal Data either enter into written confidentiality agreements or are subject to statutory obligations of confidentiality.

3.3. Compliance with Laws.

(a) Provider and Customer will each comply with Data Protection Laws in their respective Processing of Customer Personal Data.

(b) Customer will comply with Data Protection Laws in its issuing of Customer Instructions to Provider. Customer will ensure that it has established all necessary lawful bases under Data Protection Laws to enable Provider to lawfully Process Customer Personal Data for the purposes contemplated by the Agreement (including this DPA), including, as applicable, by obtaining all necessary consents from, and giving all necessary notices to, Data Subjects.

3.4. Changes to Laws. The parties will work together in good faith to negotiate an amendment to this DPA as either party reasonably considers necessary to address the requirements of Data Protection Laws from time to time.

4. Subprocessors.

4.1. Use of Subprocessors.

(a) Customer generally authorizes Provider to engage Subprocessors to Process Customer Personal Data. Customer further agrees that Provider may engage its Affiliates as Subprocessors.

(b) Provider will: (i) enter into a written agreement with each Subprocessor imposing data Processing and protection obligations substantially the same as those set out in this DPA and (ii) remain liable for compliance with the obligations of this DPA and for any acts or omissions of a Subprocessor that cause Provider to breach any of its obligations under this DPA.

4.2. Subprocessor List. Provider will maintain an up-to-date list of its Subprocessors, including their functions and locations, as specified in the **Subprocessor List**.

4.3. Notice of New Subprocessors. Provider may update the **Subprocessor List** from time to time. At least 30 days before any new Subprocessor Processes any Customer Personal Data, Provider will add such Subprocessor to the **Subprocessor List** and notify Customer through email or other means specified on the DPA Setup Page.

4.4. Objection to New Subprocessors.

(a) If, within 30 days after notice of a new Subprocessor, Customer notifies Provider in writing that Customer objects to Provider's appointment of such new Subprocessor based on reasonable data protection concerns, the parties will discuss such concerns in good faith.

(b) If the parties are unable to reach a mutually agreeable resolution to Customer's objection to a new Subprocessor, Customer, as its sole and exclusive remedy, may terminate the Order for the affected Cloud Service for convenience and Provider will refund any prepaid, unused fees for the terminated portion of the Subscription Term.

5. Security.

5.1. Security Measures. Provider will implement and maintain reasonable and appropriate technical and organizational measures, procedures and practices, as appropriate to the nature of the Customer Personal Data, that are designed to protect the security, confidentiality, integrity and availability of Customer Personal Data and protect against Security Incidents, in accordance with Provider's Security Measures referenced in the Agreement and as further described in Schedule 2 (Technical and Organizational Measures). Provider will regularly monitor its compliance with its Security Measures and Schedule 2 (Technical and Organizational Measures).

5.2. Incident Notice and Response.

(a) Provider will implement and follow procedures to detect and respond to Security Incidents.

(b) Provider will: (i) notify Customer without undue delay and, in any event, not later than the Specified Notice Period, after becoming aware of a Security Incident affecting Customer and (ii) make reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within Provider's reasonable control.

(c) Upon Customer's request and taking into account the nature of the applicable Processing, Provider will assist Customer by providing, when available, information reasonably necessary for Customer to meet its Security Incident notification obligations under Data Protection Laws.

(d) Customer acknowledges that Provider's notification of a Security Incident is not an acknowledgement by Provider of its fault or liability.

(e) Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

5.3. Customer Responsibilities.

(a) Customer is responsible for reviewing the information made available by Provider relating to data security and making an independent determination as to whether the Cloud Service meets Customer's requirements and legal obligations under Data Protection Laws.

(b) Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any Security Incidents.

6. Data Protection Impact Assessment. Upon Customer's request and taking into account the nature of the applicable Processing, to the extent such information is available to Provider, Provider will assist Customer in fulfilling Customer's obligations under Data Protection Laws to carry out a data protection impact or similar risk assessment related to Customer's use of the Cloud Service, including, if required by Data Protection Laws, by assisting Customer in consultations with relevant government authorities.

7. Data Subject Requests.

7.1. Assisting Customer. Upon Customer's request and taking into account the nature of the applicable Processing, Provider will assist Customer by appropriate technical and organizational measures, insofar as possible, in complying with Customer's obligations under Data Protection Laws to respond to requests from individuals to exercise their rights under Data Protection Laws, provided that Customer cannot reasonably fulfill such requests independently (including through use of the Cloud Service).

7.2. Data Subject Requests. If Provider receives a request from a Data Subject in relation to the Data Subject's Customer Personal Data, Provider will notify Customer and advise the Data Subject to submit the request to Customer (but not otherwise communicate with the Data Subject regarding the request except as may be required by Data Protection Laws), and Customer will be responsible for responding to any such request.

8. Data Return or Deletion.

8.1. During Subscription Term. During the Subscription Term, Customer may, through the features of the Cloud Service or such other means specified on the DPA Setup Page, access, return to itself or delete Customer Personal Data.

8.2. Post Termination.

(a) Following termination or expiration of the Agreement, Provider will, in accordance with its obligations under the Agreement, delete all Customer Personal Data from Provider's systems.

(b) Deletion will be in accordance with industry-standard secure deletion practices. Provider will issue a certificate of deletion upon Customer's request.

(c) Notwithstanding the foregoing, Provider may retain Customer Personal Data: (i) as required by Data Protection Laws or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, Provider will (x) maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to, retained Customer Personal Data and (y) not further Process retained Customer Personal Data except for such purpose(s) and duration specified in such applicable Data Protection Laws.

9. Audits.

9.1. Provider Records Generally. Provider will keep records of its Processing in compliance with Data Protection Laws and, upon Customer's request, make available to Customer any records reasonably necessary to demonstrate compliance with Provider's obligations under this DPA and Data Protection Laws.

9.2. Third-Party Compliance Program.

(a) Provider will describe its third-party audit and certification programs (if any) and make summary copies of its audit reports (each, an "**Audit Report**") available to Customer upon Customer's written request at reasonable intervals (subject to confidentiality obligations).

(b) Customer may share a copy of Audit Reports with relevant government authorities as required upon their request.

(c) Customer agrees that any audit rights granted by Data Protection Laws will be satisfied by Audit Reports and the procedures of Section 9.3 (Customer Audit) below.

9.3. Customer Audit.

(a) Subject to the terms of this Section 9.3, Customer has the right, at Customer's expense, to conduct an audit of reasonable scope and duration pursuant to a mutually agreed-upon audit plan with Provider that is consistent with the Audit Parameters (an "**Audit**").

(b) Customer may exercise its Audit right: (i) to the extent Provider's provision of an Audit Report does not provide sufficient information for Customer to verify Provider's compliance with this DPA or the parties' compliance with Data Protection Laws, (ii) as necessary for Customer to respond to a government authority audit or (iii) in connection with a Security Incident.

(c) Each Audit must conform to the following parameters ("**Audit Parameters**"): (i) be conducted by an independent third party that will enter into a confidentiality agreement with Provider, (ii) be limited in scope to matters reasonably required for Customer to assess Provider's compliance with this DPA and the parties' compliance with Data Protection Laws, (iii) occur at a mutually agreed date and time and only during Provider's regular business hours, (iv) occur no more than once annually (unless required under Data Protection Laws or in connection with a Security Incident), (v) cover only facilities controlled by Provider, (vi) restrict findings to Customer Personal Data only and (vii) treat any results as confidential information to the fullest extent permitted by Data Protection Laws.

10. Cross-Border Transfers/Region-Specific Terms.

10.1. Cross-Border Data Transfers.

(a) Provider (and its Affiliates) may Process and transfer Customer Personal Data globally as necessary to provide the Cloud Service.

(b) If Provider engages in a Restricted Transfer, it will comply with Schedule 3 (Cross-Border Transfer Mechanisms).

10.2. Region-Specific Terms. To the extent that Provider Processes Customer Personal Data protected by Data Protection Laws in one of the regions listed in Schedule 4 (Region-Specific Terms), then the terms specified therein with respect to the applicable jurisdiction(s) will apply in addition to the terms of this DPA.