Bonterms Standard Agreement
Data Protection Addendum v2.0
(Attachment Version)

This Bonterms Data Protection Addendum Version 2.0 (Attachment Version) ("**DPA**") is a set of standard terms entered into between Customer and Provider by completing the DPA Details and executing a written agreement that expressly incorporates this DPA (including the completed DPA Details) into the Main Agreement. The incorporation may be made in the Main Agreement itself or in an amendment, addendum or other written agreement.

1. Definitions.

1.1. **"Additional Terms"** means any additions to, or modifications of, this DPA (including any Exhibits) agreed by the parties.

1.2. "**Affiliate**" means an entity controlled, controlling or under common control with a party, where control means at least 50% ownership or power to direct an entity's management.

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

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

1.5. "**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.

1.6. **"Customer"** is identified in the DPA Details.

1.7. **"Customer Data"** means Customer Data as defined in the Main Agreement.

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

1.9. "**Customer Personal Data**" means Personal Data in Customer Data.

1.10. "**Data Protection Laws**" means all laws and regulations applicable to the Processing of Customer Personal Data under the Main Agreement, including, as applicable: (i) U.S. state privacy laws, including 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 the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended by the Data (Use and Access) Act 2025 (collectively, the "**UK GDPR**") and (v) the UK Data Protection Act 2018; in each case, as updated, amended or replaced from time to time.

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

1.12. **"DPA Details"** means the Key Terms, Processing Details and any Additional Terms as set forth below.

1.13. "**DPA Effective Date**" is specified in the DPA Details.

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

1.15. "**EU Standard Contractual Clauses**" or "**EU SCCs**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

1.16. "**Exhibit**" means each of Exhibit A (Cross-Border Transfer Mechanisms) and Exhibit B (Region-Specific Terms), as may be modified or replaced by the parties through Additional Terms.

1.17. "**Key Terms**" means Main Agreement, DPA Effective Date, Subprocessor List, Designated EU Governing Law and Designated EU Member State as specified by the parties in the DPA Details.

1.18. "**Main Agreement**" means the agreement between Customer and Provider under which Provider provides the Service to Customer.

1.19. "**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.

1.20. "**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.

1.21. "**Processing Details**" means the Subject Matter and Details of Processing and Security Measures specified by the parties in the DPA Details.

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

1.23. **"Provider"** is identified in the DPA Details.

1.24. "**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.

1.25. "**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.

1.26. "**Security Measures**" means the technical and organizational security measures for the Service as set forth in the Main Agreement or, if not set forth in the Main Agreement, as specified in the DPA Details.

1.27. "**Service**" means the services provided by Provider to Customer under the Main Agreement.

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

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

1.30. "**Subprocessor List**" means the list of Provider's Subprocessors as identified or linked to in the DPA Details.

1.31. **"Subprocessor Notice Method"** means email or in-product notification to an administrator.

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 Main Agreement to the extent such Processing is subject to Data Protection Laws. This DPA is governed by the governing law of the Main 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 Main Agreement (or, if later, the date on which Provider has ceased all Processing of Customer Personal Data).

2.4. Exhibits. Exhibit A (Cross-Border Transfer Mechanisms) and Exhibit B (Region-Specific Terms) are incorporated into this DPA.

2.5. Relationship to Main Agreement. This DPA (including the DPA Details) is incorporated into the Main Agreement.

2.6. 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 set forth in Exhibit A (Cross-Border Transfer Mechanisms), (2) Exhibit B (Region-Specific Terms), (3) any Additional Terms, (4) this DPA and (5) the Main Agreement. To the fullest extent permitted by Data Protection Laws, any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations, set forth in the Main 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 Service and perform Provider's obligations in the Main Agreement (including this DPA) and (ii) other reasonable documented instructions of Customer consistent with the terms of the Main Agreement.

(c) Details regarding the Processing of Customer Personal Data by Provider are set forth in the Processing Details.

(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 Main 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 applicable to 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 Main Agreement (including this DPA), including, as applicable, by obtaining all consents from, and giving all necessary notices to, Data Subjects, as required by Data Protection Laws.

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 Provider's compliance with its obligations under 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 in accordance with the Subprocessor Notice Method.

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 affected portion of the Service by providing written notice to Provider, and Provider will refund any prepaid, unused fees attributable to the terminated portion of the Service as of the date of such termination.

5. Security.

5.1. Technical and Organizational 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. Provider will regularly monitor its compliance with such Security 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 acknowledgment 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 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 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 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 the Term of the Main Agreement. During the term of the Main Agreement, Customer may, through the features of the Service or such other means specified in the Additional Terms, access, return to itself or delete Customer Personal Data.

8.2. Post Termination.

(a) Following termination or expiration of the Main Agreement, Provider will, in accordance with its obligations under the Main Agreement, delete all Customer Personal Data from Provider's systems. If the Main Agreement contains no such obligations, Provider will delete or return to Customer all Customer Personal Data in Provider's possession, custody or control as soon as reasonably practicable after such termination or expiration.

(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) Upon Customer's written request at reasonable intervals, 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 (subject to confidentiality protections for Provider).

(b) Customer may share copies 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 Service.

(b) If Provider engages in a Restricted Transfer, it will comply with Exhibit A (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 Exhibit B (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.

Exhibit A: Cross-Border Transfer Mechanisms

1. **EU Transfers**. Where Customer Personal Data is protected by EU GDPR and is subject to a Restricted Transfer, the following applies:

   1.1. The EU SCCs are hereby incorporated by reference as follows:

   (a) Module 2 (Controller to Processor) applies where Customer is a Controller of Customer Personal Data and Provider is a Processor of Customer Personal Data;

   (b) Module 3 (Processor to Processor) applies where Customer is a Processor of Customer Personal Data (on behalf of a third-party Controller) and Provider is a Processor of Customer Personal Data;

   (c) Customer is the "data exporter" and Provider is the "data importer"; and

   (d) by entering into this DPA, each party is deemed to have signed the EU SCCs (including their Annexes) as of the DPA Effective Date.

   1.2. For each Module, where applicable the following applies:

   (a) the optional docking clause in Clause 7 does not apply;

   (b) in Clause 9, Option 2 will apply, the minimum time period for prior notice of Subprocessor changes shall be as set out in Section 4.3 of this DPA, and Provider shall fulfill its notification obligations by notifying Customer of any Subprocessor changes in accordance with Section 4.3 of this DPA;

   (c) in Clause 11, the optional language does not apply;

   (d) in Clause 13, all square brackets are removed with the text remaining;

   (e) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Designated EU Governing Law;

   (f) in Clause 18(b), disputes will be resolved before the courts of the Designated EU Member State;

   (g) the Processing Details contain the information required in Annex I of the EU SCCs; and

   (h) the Processing Details contain the information required in Annex II of the EU SCCs.

   1.3. Where context permits and requires, any reference in this DPA to the EU SCCs shall be read as a reference to the EU SCCs as modified in the manner set forth in this Section 1.

2. **Swiss Transfers**. Where Customer Personal Data is protected by the FADP and is subject to a Restricted Transfer, the following applies:

2.1. The EU SCCs apply as set forth in Section 1 (EU Transfers) of this Exhibit A with the following modifications:

(a) in Clause 13, the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner;

(b) in Clause 17 (Option 1), the EU SCCs will be governed by the laws of Switzerland;

(c) in Clause 18(b), disputes will be resolved before the courts of Switzerland;

(d) the term Member State must not be interpreted in such a way as to exclude Data Subjects in Switzerland from enforcing their rights in their place of habitual residence in accordance with Clause 18(c); and

(e) all references to the EU GDPR in this DPA are also deemed to refer to the FADP.

3. **UK Transfers**. Where Customer Personal Data is protected by the UK GDPR and is subject to a Restricted Transfer, the following applies:

3.1. The EU SCCs apply as set forth in Section 1 (EU Transfers) of this Exhibit A with the following modifications:

(a) each party shall be deemed to have signed the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under section 119A of the Data Protection Act 2018;

(b) the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of Customer Personal Data;

(c) in Table 1 of the UK Addendum, the parties' key contact information is located in the Processing Details;

(d) in Table 2 of the UK Addendum, information about the version of the EU SCCs, modules and selected clauses which this UK Addendum is appended to are located above in this Exhibit A;

(e) in Table 3 of the UK Addendum:

(i) the list of parties is located in the Processing Details;

(ii) the description of transfer is located in the Processing Details;

(iii) Annex II is located in the Processing Details; and

(iv) the list of Subprocessors is located in the Processing Details.

(f) in Table 4 of the UK Addendum, both the Importer and the Exporter may end the UK Addendum in accordance with its terms (and the respective box for each is deemed checked); and

(g) Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

4. **Data Privacy Framework.** For clarity, a transfer of Customer Personal Data from the EEA, UK or Switzerland to Provider in the United States subject to the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and/or the Swiss-U.S. Data Privacy Framework, as applicable (collectively, the "**DPF**"), shall not constitute a Restricted Transfer so long as Provider maintains an active certification to the DPF and certification to the DPF remains a legal basis for transfer of Personal Data to the United States under the GDPR, UK GDPR or FADP, as applicable.

Exhibit B: Region-Specific Terms

A. **CALIFORNIA**

1. **Definitions**. CCPA and other capitalized terms not defined in this Exhibit are defined in the DPA.
   1.1. "business purpose", "commercial purpose", "personal information", "sell", "service provider" and "share" have the meanings given in the CCPA.
   1.2. The definition of "Data Subject" includes "consumer" as defined under the CCPA.
   1.3. The definition of "Controller" includes "business" as defined under the CCPA.
   1.4. The definition of "Processor" includes "service provider" as defined under the CCPA.

2. **Obligations**.

   2.1. Customer is providing the Customer Personal Data to Provider under the Main Agreement for the limited and specific business purposes of providing the Service as described in the Processing Details and otherwise performing under the Main Agreement.

   2.2. Provider will comply with its applicable obligations under the CCPA and provide the same level of privacy protection to Customer Personal Data as is required by the CCPA.

   2.3. Provider acknowledges that Customer has the right to: (i) take reasonable and appropriate steps under Section 9 (Audits) of this DPA to help to ensure that Provider's use of Customer Personal Data is consistent with Customer's obligations under the CCPA, (ii) receive from Provider notice and assistance under Section 7 (Data Subject Requests) of this DPA regarding consumers' requests to exercise rights under the CCPA and (iii) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data.

   2.4. Provider will notify Customer promptly after it makes a determination that it can no longer meet its obligations under the CCPA.

   2.5. Provider will not retain, use or disclose Customer Personal Data: (i) for any purpose, including a commercial purpose, other than the business purposes described in Section A.2.1 of this Exhibit or (ii) outside of the direct business relationship between Provider and Customer, except, in either case, where and to the extent permitted by the CCPA.

   2.6. Provider will not sell or share Customer Personal Data received under the Main Agreement.

   2.7. Provider will not combine Customer Personal Data with other personal information except to the extent a service provider is permitted to do so by the CCPA.

DPA DETAILS

The following information is to be completed by the Customer and Provider entering into this DPA.

Key Terms	
Main Agreement	This DPA is incorporated into the Main Agreement between Customer and Provider identified below: [Include name and date of Main Agreement between Customer and Provider]
DPA Effective Date	[Fill in date]
Subprocessor List	[Attach or link to location of Provider's Subprocessor List (or state "None")]
Designated EU Governing Law	[EU member state law governing the EU SCCs, or "N/A" if Exhibit A does not apply]
Designated EU Member State	[EU member state whose courts will resolve disputes under the EU SCCs, or "N/A" if Exhibit A does not apply]

Processing Details	
Subject Matter and Details of Processing	
Customer/ 'Data Exporter' Details	
Name:	
Contact details for data protection:	
Main address:	
Customer activities:	
Role:	Controller
Provider/ 'Data Importer' Details	
Name:	
Contact details for data protection:	
Main address:	
Provider activities:	
Role:	Processor
Details of Processing	
Categories of Data Subjects:	***[Uncheck any boxes that do not apply. List additional categories of data subjects or add any additional detail as necessary. This list is not necessarily exhaustive.]*** The following, as applicable under the circumstances: ☒ Customer's customers ☒ Customer's prospective customers ☒ Customer's business contacts ☒ Users ☒ Employees, other personnel and job candidates ☐ Other: [specify]

Categories of Customer Personal Data:	***[Uncheck any boxes that do not apply. List additional categories of personal data or add any additional detail as necessary. This list is not necessarily exhaustive.]*** The following, as applicable under the circumstances: ☒ Contact information ☒ Account information ☒ Demographic information ☒ Professional information ☒ Transaction information ☒ Communications information ☒ User generated content ☒ Unique identifiers ☐ Other: [specify other categories] *For Sensitive or Special Categories of Personal Data, see immediately below.*
Sensitive or Special Categories of Personal Data:	***[Check applicable box]*** ☐ Yes, sensitive or special categories of Personal Data: [specify categories] If Yes, additional restrictions on Processing: [specify restrictions] ☐ None/Not Applicable
Frequency of transfer:	***[Check applicable box]*** ☐ Continuous ☐ Other: [specify]
Nature of the Processing:	Processing operations required to provide the Service in accordance with the Main Agreement.
Purpose of the Processing:	To provide the Service and carry out Customer Instructions.
Duration of Processing / retention period:	Concurrent with the term of the Main Agreement and thereafter pursuant to Section 8 (Data Return or Deletion) of the DPA.
Transfers to Subprocessors:	As described in the Subprocessor List for the purposes described therein.
Competent EU Supervisory Authority:	If the EU SCCs apply, the competent supervisory authority is determined in accordance with Clause 13 of the EU SCCs. If the applicable authority has been identified, specify it here: [specify].
Security Measures	
Technical and Organizational Measures	[If Security Measures are not described in the Main Agreement, describe or link to Provider's technical and organizational measures here. If addressed in the Main Agreement, state "See Main Agreement."]

Additional Terms
The following additions to or modifications of the Bonterms Data Protection Addendum (including any Exhibits) are agreed by the parties and control in the event of any conflicts: