

DATA PROTECTION ADDENDUM

This Data Protection Addendum (“**DPA**”) is entered into by and between _____, a _____ (“**Customer**”), having its principal place of business at _____, and Copper CRM, Inc., a Delaware corporation (“**Copper**”), as of the last dated signature of this DPA (“**Effective Date**”). This DPA supplements any existing and currently valid Copper Subscription Agreement, Copper Terms of Service, or other agreement by and between Copper and Customer pursuant to which Customer obtains access to the Service, as applicable (the “**Agreement**”).

All capitalized terms that are not expressly defined (either directly or by reference) in this DPA have the meanings given to them in the Agreement. Except where the context otherwise requires, all section references in this DPA refer to sections of this DPA.

In addition to Part A (General Information Security Terms), Part B (EU-Specific Provisions) of this DPA applies only to the extent Copper Processes Personal Information that is subject to Applicable Data Protection Laws of the EU.

PART A: General Information Security Terms

1. Definitions.

- (a) “**Applicable Data Protection Laws**” means all privacy, data security and data protection laws, directives, regulations and rules in any jurisdiction applicable to Copper and the Service, including, where applicable, EU Data Protection Law.
- (b) “**Customer Personal Information**” means Customer Content that is Personal Information.
- (c) “**Data Controller**” means an individual or entity that determines the purposes and means of the Processing of Personal Information.
- (d) “**Data Processor**” means an entity that Processes Personal Information on behalf of a Data Controller.
- (e) “**Data Protection Authority Request**” has the meaning set forth in Part A, Section 7.
- (f) “**EU**” means European Economic Area and its member states, the United Kingdom, and/or Switzerland.
- (g) “**EU Customer Personal Information**” means Customer Personal Information that is subject to the EU Data Protection Law.
- (h) “**EU Data Protection Law**” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation or “**GDPR**”).
- (i) “**Personal Information**” means (i) any information about an identified or identifiable individual and (ii) information that is not specifically about an identified or identifiable individual but, when combined with other information, may identify an individual.
- (j) “**Privacy Shield**” means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of 12 July 2016 and by the Swiss Federal Council on January 11, 2017, respectively.

- (k) **“Privacy Shield Principles”** means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced).
- (l) **“Process”** or **“Processing”** means to create, collect, receive, acquire, record, consult, alter, use, process, store, retrieve, maintain, disclose, or dispose of data or sets of data, whether or not by automated means.
- (m) **“Reasonable”** means reasonable and appropriate to (i) the size, scope, and complexity of Copper’s business, (ii) the nature of the Personal Information being Processed, and (iii) the need for privacy, confidentiality and security of the Personal Information.
- (n) **“Report”** has the meaning set forth in Part A, Section 7.
- (o) **“Safeguards”** has the meaning set forth in Part A, Section 4.
- (p) **“Security Incident”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Information in Copper’s custody or control.
- (q) **“Third Party Provider”** means any contractor or other third party that Copper authorizes to Process Customer Personal Information on Copper’s behalf in connection with performing the Service.

2. **Compliance with Laws; Use Limitation.**

- (a) **Role of the Parties.** As between Copper and Customer, Customer is the Data Controller of Customer Personal Information, and Copper will process Customer Personal Information only as a Data Processor acting on behalf of Customer. To the extent any Service Data is considered Personal Information under Applicable Data Protection Laws, Copper is the Data Controller of such information and will process such information in accordance with the Agreement and Applicable Data Protection Laws applicable to Data Controllers.
- (b) **Customer Processing of Personal Data.** Customer agrees that: (i) it will comply with its obligations under Applicable Data Protection Laws in respect of its processing of Personal Information, including any obligations specific to its role as a Data Controller (where Applicable Data Protection Laws recognize such concept); (ii) it has provided all notice and obtained all consents, permissions and rights necessary under Applicable Data Protection Laws for Copper to lawfully process Personal Information for the purposes set forth in Part A, Section 2(c); and (iii) it will ensure its processing instructions are lawful and that the processing of Customer Personal Information in accordance with such instructions will not violate Applicable Data Protection Laws.
- (c) **Customer Instructions.** Copper will Process Customer Personal Information only for the limited and specified purposes stated in the Agreement and Customer’s documented lawful instructions. Taking into account the nature of Processing and the information available to Copper, Copper shall take steps to cause any natural person acting under Copper’s authority who has access to Customer Personal Information to not Process Customer Personal Information except on instructions from the Controller, unless such person is required to do so by Applicable Data Protection Laws. The parties agree that the Agreement (including this DPA) sets out the Customer’s complete and final instructions to Copper in relation to the Processing of Customer Personal Information. Any Processing of Customer Personal Information outside the scope of these instructions (if any) will require prior written agreement between Customer and Copper.

3. **Third Party Providers.**

- (a) **Appointment of Third Party Providers.** Customer acknowledges and agrees that Copper may engage Third Party Providers in connection with Copper's provision of the Service. Copper will contractually require each Third Party Provider that has access to Customer Personal Information to protect the privacy, confidentiality, and security of such Customer Personal Information using at least the same level of protection and confidentiality obligations that apply to Copper under this DPA to the extent applicable to the Service or portion thereof provided by such Third Party Provider.
- (b) **List of Third Party Providers.** Copper will make available to Customer a current list of Third Party Providers and a mechanism by which Customer may automatically receive updates of any intended changes concerning the addition or replacement of Third Party Providers.
- (c) **Liability.** Copper will be liable for the acts and omissions of its Third Party Providers to the same extent Copper would be liable if performing the services of such Third Party Providers under this DPA, unless otherwise set forth in the Agreement.

4. **Safeguards.**

- (a) **Copper's Safeguards.** At all times that Copper Processes Customer Personal Information, Copper will maintain the administrative, physical and technical controls, which are designed to protect the security, confidentiality and integrity of the Customer Personal Information ("**Safeguards**") set out on **Annex A** to this DPA.
- (b) **Updates to Safeguards.** Copper may update or modify the Safeguards from time to time provided that such updates and modifications do not result in any material degradation of the overall security of the Service.
- (c) **Customer Assessment of Safeguards.** Customer is solely responsible for reviewing and evaluating for itself whether the Service, the Safeguards and Copper's commitments under this Section 4 will meet Customer's needs, including with respect to any security obligations of Customer under Applicable Data Protection Law. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Personal Information, as well as the risks to individuals) the Safeguards provide a level of security appropriate to the risk in respect of the Customer Personal Information.

5. Security Incident Response.

- (a) **Security Incident Response Program.** Copper will maintain a Reasonable incident response program to respond to Security Incidents.
- (b) **Notice.** Upon Copper's confirmation that a Security Incident has occurred, Copper will without undue delay following such confirmation, send an email to Copper's administrative account contact and provide a summary description of the details known by Copper about the Security Incident. Copper's notification of a Security Incident shall not be construed as an admission of fault or liability with respect to such Security Incident.
- (c) **Investigation; Remediation.** If a Security Incident has occurred, Copper will promptly (i) investigate Security Incident, (ii) take Reasonable steps to remediate the root cause of the Security Incident and (iii) identify relevant contact people who will be reasonably available until the Security Incident has been resolved.
- (d) **Security Incidents Caused by Customer.** The obligations set forth in this Part A, Section 5 do not apply to any Security Incident that is caused by Customer or Customer's users of the Service. ☐

6. Legal Process. Without limitation to Section 5 of the Agreement, Copper may disclose Customer Personal Information to the extent that such disclosure is required by Applicable Data Protection Laws or by order of a court or other governmental authority. To the extent it is legally permitted to do so, Copper agrees to give Customer Reasonable notice of any disclosure made or to be made under this Part A, Section 6 so as to allow Customer to seek a protective order or other appropriate remedy.

7. Vulnerability Testing. Copper has obtained third-party vulnerability testing of its networks, systems, software and devices used to access Customer Personal Information. Upon Customer's written request, Copper will provide Customer with a report that summarizes the results of the vulnerability testing (a "**Report**"). Customer will treat these results as Copper's Confidential Information for purposes of the Agreement. Notwithstanding the foregoing, Customer may disclose a Report as allowed under the applicable confidentiality section of the Agreement, including where requested or required by data protection authorities having jurisdiction over Customer even if not legally required ("**Data Protection Authority Request**"); provided, however, that Customer will give Copper prior written notice of the Data Protection Authority Request such that Copper can attempt to secure confidential treatment for the Report. If Customer is not legally permitted to give Copper prior notice, Customer agrees to use reasonable efforts to secure confidential treatment for the Report and further agrees to not remove or obscure any "confidential", "proprietary", or similar markings from the Report.

8. Retention and Deletion of Customer Personal Information. For thirty (30) days following termination or expiration of the Agreement, Customer will have the option to retrieve any remaining Customer Personal Information in accordance with the Agreement. Copper will automatically delete all remaining (if any) Customer Personal Information (including copies) within a Reasonable time period in accordance with Copper's data retention policies; provided that Copper will not be required to delete Customer Personal Information that has been archived in Copper's archival or backup systems and such Customer Personal Information is not used for active Processing by the Service (other than to the extent Copper restores such Customer Personal Information due to a disaster recovery or similar event which requires restoration of such Customer Personal Information). Notwithstanding the foregoing, Copper will delete all Customer Personal Information (including archival and backup Customer Personal Information) within thirty (30) days of the date that it receives specific written instructions from Customer to delete such Customer Personal Information. Notwithstanding the foregoing, Copper will not be required to delete Customer Personal Information to the extent Copper is required by Applicable Law or order of a governmental or regulatory body to retain some or all of the Customer Personal Information.

9. **Survival.** Obligations under this DPA will survive expiration or termination of the Agreement and completion of the Service as long as Copper continues to Process Customer Personal Information.
10. **Prior Agreements.** The parties agree that this DPA will replace and supersede any existing data processing addendum, attachment or exhibit the parties may have previously entered into in connection with the Services.
11. **Limitation of Liability.** Copper's liability arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of Copper means the aggregate liability of Copper under the Agreement and all DPAs together.

Part B: EU-Specific Provisions

1. **Definitions.** Unless otherwise defined in the DPA, all terms in Part B will have the definitions given to them by the EU Data Protection Law.
2. **Data Processor Obligations:** To the extent Copper Processes EU Customer Personal Information as a Data Processor, Copper agrees to do the following:
 - (a) **Requests from Data Subjects and Government Authorities.** Through the Service, Copper provides Customer with a number of controls that Customer may use to retrieve, correct, delete or restrict EU Customer Personal Information, which Customer may use to assist it in connection with its obligations under the EU Data Protection Law, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Customer is unable to access EU Customer Personal Information within the Service using such controls or through other means reasonably available to Customer, taking into account the nature of the Processing, Copper will, at Customer's request and expense, provide reasonable cooperation to assist Customer to respond to any requests from individuals in the EU to exercise their rights under EU Data Protection Law or from applicable data protection authorities relating to the processing of EU Customer Personal Information under the Agreement. In the event that any request from individuals or applicable data protection authorities is made directly to Copper where such request identifies Customer as the Data Controller with respect to the requested EU Customer Personal Information, Copper will not respond to such communication directly without Customer's prior authorization, unless legally required to do so, and instead, after being notified by Copper, Customer will respond. If Copper is required to respond to such a request, Copper will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.
 - (b) **Cessation of Processing.** Copper will stop Processing EU Customer Personal Information if at any time it is determined by a EU supervisory authority of competent jurisdiction that Copper is not Processing such Customer Personal Information in compliance with the Agreement and, if applicable, the Privacy Shield Principles.

- (c) **Notice to Customer.** Copper will immediately inform Customer if Copper is of the opinion that any Customer instruction to Copper to make available to Customer information necessary to demonstrate compliance with Article 28 of the EU Data Protection Law or in relation to audits, including inspections, if any, by Customer or an auditor mandated by Customer infringes the EU Data Protection Law or other Applicable Data Protection Laws of the EU or its member states.
 - (d) **Assistance to Customer.** To the extent Copper is required under EU Data Protection Law, Copper will (at Customer's request and expense) provide reasonably requested information regarding the Service to enable Customer to carry Customer's data protection impact assessments or prior consultations with data protection authorities as required by EU Data Protection law to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Copper.
- 3. Data Controller Obligations:** To the extent Customer provides Copper with access to EU Customer Personal Information, Customer agrees to provide individuals with a clear and conspicuous privacy notice that (i) accurately describes how Copper Processes the Personal Information and (ii) complies with Applicable Data Protection Laws.
- 4. EU Data Transfers.** To the extent that Copper processes any EU Customer Personal Information, the parties agree that Copper makes available the transfer mechanisms listed below, for any transfers of EU Customer Personal Information from the EU to Copper located in a country which does not ensure an adequate level of protection (within the meaning of EU Data Protection Law) and to the extent such transfers are subject to EU Data Protection Law:
- (a) If and when Copper is self-certified to the Privacy Shield: (i) the parties acknowledge and agree that Copper will be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for EU Customer Personal Information by virtue of having self-certified its compliance with the Privacy Shield; (ii) Copper agrees to process EU Customer Personal Information in compliance with the Privacy Shield Principles; and (iii) if Copper is unable to comply its obligations under this subsection, Copper will inform the Customer.
 - (b) To the extent the transfer mechanism identified in Part B, Section 4(a) does not apply to the transfer, is invalidated and/or Copper is not self-certified to the Privacy Shield, Copper agrees to enter into an agreement with Customer based on the European Commission's or Swiss Federal Data Protection and Information Commissioner's standard contractual clauses.
- 5. Details of the Processing.** The subject-matter and duration of the Processing, the nature and purpose of the Processing, the types of Customer Personal Information and categories of Data Subjects Processed, and the obligations and rights of Customer as Data Controller under this DPA are further specified in **Annex B** to this DPA.

[Signature page follows]

This Data Protection Addendum is entered into by the parties set forth below as of the Effective Date.

COPPER CRM, INC.

_____ Customer Name

By:

By:

Name:

Name:

Title:

Title:

Date:

Date:

Annex A

Safeguards

1. **Physical Access.** Copper will maintain physical access controls designed to secure relevant facilities, infrastructure, data centers, hard copy files, servers, backup systems and Copper-owned equipment (including mobile devices) used to access Customer Personal Information.
2. **User Authentication.** Copper will maintain user authentication and access controls within operating systems, applications and equipment.
3. **Personnel Security.** Copper will maintain policies and practices restricting access to Customer Personal Information, including requiring written confidentiality agreements and background checks consistent with Applicable Law for all Copper personnel who are authorized to Process Customer Personal Information or who maintain, implement, or administer Copper's information security program and Safeguards.
4. **Logging and Monitoring.** Copper will log and monitor access to Customer Personal Information on networks, systems and devices operated by Copper.
5. **Malware Controls.** Copper will maintain Reasonable controls designed to protect all networks, systems and devices that access Customer Personal Information from malware and unauthorized software.
6. **Security Patches.** Copper will maintain controls and processes designed to update networks, systems and devices (including operating systems and applications) that access Customer Personal Information, including prompt implementation of identified high-severity security patches when issued and validated for Copper's environment.
7. **Access Controls.** Copper will maintain controls designed to restrict access to Customer Personal Information to only personnel who have a legitimate need to Process Customer Personal Information under the Agreement.
8. **Training and Supervision.** Copper will provide reasonable ongoing privacy and information protection training and supervision for all Copper's personnel who access Customer Personal Information.
9. **Vulnerability Testing.** Copper will periodically obtain third-party vulnerability testing of its systems and software used to access Customer Personal Information and will obtain penetration tests by an independent third-party expert at least annually. Copper's security personnel will review and take steps to address vulnerabilities revealed by such tests in accordance with Copper's security policies and practices.
10. **Encryption.** Customer Personal Information stored and/or transmitted by Copper will be encrypted by generally-accepted, non-proprietary encryption algorithms, such as AES-256, subject to applicable technological constraints and legal requirements.

Annex B

Details of Processing of Personal Information

1. The subject matter and duration of the Processing of Customer Personal Information:	The subject matter of the Processing of Customer Personal Information is the performance of the Service by Copper, as set out in the Agreement and this DPA. The duration of Processing of Personal Information is set out in Part A, Section 8 of this DPA.
2. The nature and purpose of the Processing of Customer Personal Information:	Copper will Process Customer Personal Information as necessary to perform Service pursuant to the terms and subject to the conditions of the Agreement, as further specified in the Agreement and any attachments, exhibits, or schedules thereto, and as further instructed by Customer in its use of the Service.
3. The types of Customer Personal Information to be Processed:	Any Customer Content that is Personal Information.
4. The categories of Data Subjects to whom the Customer Personal Information relates:	<ul style="list-style-type: none">● Customer's End Users, as defined in the Agreement● Customer's employees, contractors, consultants and agents● Third-parties with whom Customer does business● Others, whose data may be collected or processed by Copper, a subsidiary or a third party
5. The obligations and rights of Customer:	The obligations and rights of Customer are set out in the Agreement and this DPA.