Last Updated: 9-03-20

DATA PROTECTION ADDENDUM

This Data Protection Addendum ("**DPA**") is incorporated into and forms part of the Terms of Service (the "**Agreement**") entered into by and between the Customer and Copper CRM, Inc. ("**Copper**") pursuant to which Customer obtains access to the Service.

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.

1. Definitions.

(a) **"Applicable Data Protection Laws"** means the General Data Protection Regulation 2016/679 ("**GDPR**") and UK Data Protection Act 2018 ("**DPA 2018**") and the California Consumer Privacy Act ("**CCPA**").

(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) "**Personal Information**" means any information relating to an identified natural person or a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person or is otherwise as defined in Applicable Data Protection Law.

(f) "**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.

(g) "**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Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced).

(h) "**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.

(i) "**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.

(j) "**Report**" has the meaning set forth in Section 5(e).

(k) "**Safeguards**" has the meaning set forth in Section 4.

(l) **"Security Incident"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Information in Copper's custody or control.

(m) **"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. 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 A** to this DPA.

(b) **Customer Processing of Personal Information**. 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 herein and the Agreement; 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) **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 Customer Personal Information, which Customer may use to assist it in connection with its obligations under Applicable Data Protection Laws, 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 Applicable Data Protection Laws 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.

(d) **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.

(e) **Cessation of Processing**. Copper will stop Processing Customer Personal Information if at any time it is determined by a 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.

(f) **Impact Assessments**. To the extent required under Applicable 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. The foregoing is applicable only to the extent Customer does not otherwise have access to the relevant information and such information is available to Copper.

3. Third-Party Providers.

(a) **Appointment of Third-Party Providers**. Customer consents to Copper engaging Copper's affiliates and Third-Party Providers to Process Customer Personal Information in connection with Copper's provision of the Service. Copper will maintain a list of its Third-Party Providers on its website located at https://support.copper.com/hc/en-us/articles/360001006747, or a publicly available successor website as determined by Copper in its sole discretion (the "**Third-Party Provider List**"). Copper will update the Third-Party Provider List with details of any new in Third-Party Providers prior to any such change and will provide Customer with a mechanism to receive automatic notification of any such change prior to it going into effect. If Customer reasonably objects to Copper's addition of Third-Party Providers on data protection grounds, Customer will notify Copper of its objections and the reasons therefore in writing within ten (10) business days of receipt of information or the effective date of such change, whichever is earlier, about the change and the parties will discuss possible alternatives to use of the new Third-Party Provider. If the parties do not agree to such an alternative in a reasonable period of time, which will not exceed thirty (30) days from the date that Copper receives Customer's objection notice, Customer may terminate the Agreement by providing written notice to Copper. Such termination shall be Customer's sole and exclusive remedy in relation to its objection.

(b) **Agreements with Third-Party Providers.** Copper will impose data protection terms on any Third-Party Provider it appoints as required to protect Customer Personal Information to the standard required by the Applicable Data Protection Laws.

(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 B** 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 Customer's administrative account contact for the Service 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. Copper will provide reasonable information and cooperation to Customer so that Customer can fulfill any data breach reporting obligations it may have under (and in accordance with the timescales required by) Applicable Data Protection Laws.

(d) **Security Incidents Caused by Customer**. The obligations set forth in Section 5(c) do not apply to any Security Incident that is caused by Customer or Customer's users of the Service.

(e) **Vulnerability Testing.** Copper has obtained third-party vulnerability testing of its application. 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 Reports as Copper's Confidential Information for purposes of the Agreement.

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 Section 6 so as to allow Customer to seek a protective order or other appropriate remedy.

7. **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 legally required or permitted to retain some or all of the Customer Personal Information.

8. **EU Data Transfers.** Copper will not transfer Personal Information outside the European Economic Area ("**EEA**") unless it takes such measures as are necessary to provide adequate protection for such Customer Personal Information consistent with the requirements of Data Protection Laws. To the extent Copper Processes (or causes to be Processed) any Personal Information originating from the EEA in a country that has not been designated by the European Commission as providing an adequate level of protection for Personal Information, the Personal Information shall be deemed to have adequate protection (within the meaning of Applicable Data Protection Laws) by virtue of the Standard Contractual Clauses attached as **Annex C** to this DPA. The parties agree that this DPA addresses business related issues pertinent to the subject matter of the Standard Contractual Clauses, and that the terms of this DPA are intended to supplement and govern the matters provided for in the Standard Contractual Clauses to the maximum extent permitted by Directive 95/46/EC; provided that, in the event of a contradiction between the terms of this DPA and the Standard Contractual Clauses, the terms of the Standard Contractual Clauses shall prevail.

9. **Audit**. Copper shall make available to Customer upon its written request all information necessary to demonstrate compliance with the obligations of data processors laid down in Article 28 of GDPR; provided that if Copper has obtained a SOC 2 audit report for a period ended not more than 18 months prior to the date of such request, Copper shall be deemed to have satisfied this obligation by providing Customer with a copy of such report. Not more than once per year, Copper will also respond to a Customer security questionnaire and meet by teleconference to address follow-up questions. Not more than once per year, Customer may contact Copper in accordance with the "Notice" provisions of the Agreement to request an inspection and audit of the procedures relevant to the protection of Personal Information. Before the commencement of any such audit, Customer and Copper shall mutually agree upon the scope, timing, and duration of the audit and the reimbursement rate for any travel or other expenses Copper incurs in the course of such audit. All reimbursement rates shall be reasonable, taking into account the resources expended by Copper. Customer shall promptly notify Copper with information related to any non-compliance identified by Customer in connection with such audit.

10. **Changes to Law**. If any changes or prospective changes to Applicable Data Protection Laws

result or will result in one or both parties not complying with the Applicable Data Protection Laws, then the parties shall enter into good faith discussions to agree such variations to this DPA as may be necessary to strictly remedy such non-compliance.

11. **Survival**. Obligations under this DPA and the Standard Contractual Clauses will survive expiration or termination of the Agreement and completion of the Service as long as Copper continues to Process Customer Personal Information.

12. **Other Agreements**. This DPA does not replace or supersede any agreement or addendum relating to processing of Personal Information entered into between Customer and Copper and referenced in the Agreement or, if applicable, any order form entered into by Copper and Customer thereunder, and any such individually negotiated agreement or addendum, shall apply instead of this DPA.

13. **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.

[*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

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 Section 7 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:	• 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.

Annex B

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 C

Standard Contractual Clauses (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:	
address:	
tel:	
fax:	
e-mail:	
Other information needed to identify the organisation	
(the data exporter)	
Name of the data importing organisation:	Copper CRM, Inc.
address:	301 Howard St., Suite 600
tel:	(415) 231-6360
fax:	N/A
e-mail:	legal@copper.com
Other information needed to identify the organisation	N/A
(the data importer)	

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in **nex C-1**.

1. Definitions

For the purposes of the Clauses:

(a) **personal data**, **special categories of data**, **process/processing**, **controller**, **processor**, **data subject** and **supervisory authority** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1);

(b) **the data exporter** means the controller who transfers the personal data;

(c) **the data importer** means the processor who agrees to receive from the data exporter personal data intended for processing on its behalf after the transfer in accordance with its instructions and the terms of the Clauses and who is not subject to a third

country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) **the sub-processor** means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with its instructions, the terms of the Clauses and the terms of the written subcontract;

(e) **the applicable data protection law** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) **technical and organisational security measures** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in **Annex C-1** which forms an integral part of the Clauses.

3. Third-party beneficiary clause

The data subject can enforce against the data exporter this clause 3, clause 4(b) to clause 4(i), clause 5(a) to clause 5(e) and clause 5(g) to clause 5(j), clause 6.1 and clause 6.2, clause 7, clause 8.2 and clause 9 to clause 12 as third-party beneficiary.

The data subject can enforce against the data importer this clause, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2 and clause 9 to clause 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.1. The data subject can enforce against the sub-processor this clause 3.1, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2, and clause 9 to clause 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in **Annex C-2** to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to clause 5(b) and clause 8.3 to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of **Annex C-2** and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subjects as the data importer under the Clauses; and

(j) that it will ensure compliance with clause 4(a) to clause 4(i).

5. Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in **Annex C-2** before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

  (ii) any accidental or unauthorised access; and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of **Annex C-2** which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with clause 11; and

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6. Liability

6.1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in clause 3 or in clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

6.2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or its sub-processor of any of their obligations referred to in clause 3 or in clause 11 because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

6.3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in clause 3 or in clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

7.1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Cooperation with supervisory authorities

8.1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in clause 5(b).

9. Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

11. Sub-processing

11.1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

11.2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

11.3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

11.4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data processing services

12.1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2. The data importer and the sub-processor warrant that upon request of the data exporter and/ or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature:

On behalf of the data importer: **Copper CRM, Inc.**

Name (written out in full): Ben Hance

Position: General Counsel

Address: 301 Howard St., Suite 600, San Francisco, CA 94105

Other information necessary in order for the contract to be binding (if any): N/A

Signature:

Annex C-1 to the Standard Contractual Clauses

This Annex forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this **Annex C-1**.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):	Data Exporter is the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and any affiliates.

Data importer

The data importer is (please specify briefly your activities relevant to the transfer):	Data Importer is Copper CRM, Inc., a provider of cloud-based customer relationship management software, which processes personal data upon the instruction of the Data Exporter in accordance with the terms of the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify)	The personal data that may be transferred by the Data Exporter is determined and controlled by the Data Exporter, in its sole discretion, and may include the personal data concerning the following categories of data subjects: • 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

Categories of data

The personal data transferred concern the following categories of data (please specify)	The personal data that may be transferred by the Data Exporter is determined and controlled by the Data Exporter, in its sole discretion, and may include the following categories of data: • Any Customer Content that is Personal Information.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify)	None

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify)	The personal data transferred is processed by the Data Importer to provide the Service pursuant to the Agreement.

DATA EXPORTER	**DATA IMPORTER**
Name:	Name: **Copper CRM, Inc.**
Authorised signature:	Authorised signature:

Annex C-2 to the Standard Contractual Clauses

This **Annex C-2** forms part of the Clauses and must be completed and signed by the parties.

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 below. 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.

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.