Last Updated: 9-28-21

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**"), the General Data Protection Regulation 2016/679 as it forms part of the law of the UK by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"), 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) "**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.

(g) "**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.

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

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

(j) "**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.

(k) "**Third-Party Provider**" or "**Subprocessor**" 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, including this DPA.

(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 and UK Data Transfers.** Copper will not transfer Personal Information outside the European Economic Area ("**EEA**") or the United Kingdom unless it takes such measures as are necessary to provide adequate protection for such Customer Personal Information consistent with the requirements of the Applicable Data Protection Laws. To the extent Copper Processes, or causes to be Processed, any Personal Information originating from the EEA or the United Kingdom in a country that has not been designated by the European Commission or the UK Information Commissioner's Office, or other relevant UK governing body, as the case may be, 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 (i) the EU Standard Contractual Clauses attached hereto as **Annex C**, in the case of Customer Personal Information originating in the EEA, or (ii) the UK Standard Contractual Clauses attached hereto as **Annex D**, in the case of Customer Personal Information originating in the United Kingdom. The EU Standard Contractual Clauses and the UK Standard Contractual Clauses are together referred to as the "**Standard Contractual Clauses**." 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 the Applicable Data Protection Laws; 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. Without limiting the foregoing, Customer agrees that Copper's obligations under Section 8.5 of the EU Standard Contractual Clauses and Section 12.1 of the UK Standard Contractual Clauses to delete and/or to return personal data processed on Customer's behalf after the provision of processing services shall be subject to, and satisfied by Copper's performance of, its obligations under Section 8.6 of the Agreement and Section 7 of this DPA. Nothing in this Section 8 shall limit Copper's revocation rights under Section 16(e) of the EU Standard Contractual Clauses.

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 to the DPA

Data Processing Details

1. Copper's activities	Provision of customer relationship management (CRM) software.
2. 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.
3. 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.
4. The types of Customer Personal Information to be Processed:	Any Customer Content that is Personal Information, processed to deliver the Service pursuant to the Agreement. Customers control the types of Personal Information that they store in our CRM. Typically, CRM Data consists of: ● Contact information about their customers, leads and contacts ● Financial and other information related to sales opportunities and project implementation ● Copies of emails and calendar information that is synced from Customer's GMail account The Agreement prohibits customers from using Copper's CRM to Process Sensitive Information (as defined in the Agreement), including special categories of data under the GDPR.
5. 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
6. Authorised Subprocessors:	Customer authorizes Copper to appoint the Subprocessors listed at https://support.copper.com/hc/en-us/articles/360001006747, or a publicly available successor website.

7. The obligations and rights of Customer:	The obligations and rights of Customer are set out in the Agreement and this DPA.
8. Data retention	Customer Content that is Personal Information will be retained during the time periods set forth in the Agreement as may be amended from time to time.

Annex B to the DPA
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 below. Copper may update or modify the Safeguards from time to time provided that such updates and modifications do not result in any material reduction of the overall effectiveness of the 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

EU STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in **Annex I.A** (hereinafter each **'data exporter'**), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in **Annex I.A** (hereinafter each **'data importer'**)

have agreed to these standard contractual clauses (hereinafter: **'Clauses'**).

(c) These Clauses apply with respect to the transfer of personal data as specified in **Annex I.B**.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in **Annex I.B**.

Clause 7

[*Reserved*]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in **Annex I.B**, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in **Annex II** and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in **Annex I.B**. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter **'personal data breach'**). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of

pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in **Annex II**. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter '**sensitive data**'), the data importer shall apply the specific restrictions and/or additional safeguards described in **Annex I.B**.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter '**onward transfer**') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least a reasonable period of time in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in **Annex I.C**, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Republic of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I TO THE EU SCCS

Particulars of the transfer

A. LIST OF PARTIES

Data exporter	Customer. Contact person's name, position and contact details: [*]
Data importer	Copper CRM, Inc. Contact person's name, position and contact details: Ben Hance, General Counsel, legal@copper.com

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects	As set out in Annex A to the DPA (*Data Processing Details*).
Categories of Data	As set out in Annex A to the DPA (*Data Processing Details*).
Sensitive Data	As set out in Annex A to the DPA (*Data Processing Details*).
Frequency of Transfer	Continuous for the term of the Agreement.
Nature of Processing	Storing, copying, accessing, sharing, modifying.
Purposes of the Transfer	The provision of the Service by data importer to data exporter pursuant to the Agreement.
Data Retention	Data importer will delete the personal data from its systems on expiry or termination of the Service in accordance with its usual data retention practices.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority should be the Data Protection Commissioner of the Republic of Ireland.

ANNEX II TO THE EU SCCS

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) are those set out in Annex B to the DPA (Safeguards).

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

See Section 3 of the DPA.

Annex D

UK Standard Contractual Clauses for Restricted Transfers Originating in the UK (Processors)

Clause 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;

(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 his behalf after the transfer in accordance with his 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 subprocessor"* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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 his 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.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 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. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 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 subprocessor shall be limited to its own processing operations under the Clauses.

4. 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.

Clause 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 Appendix 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 subprocessor 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

Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

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

Clause 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 Appendix 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 subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 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 subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

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

Clause 6

Liability

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 subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

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 his subprocessor 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 of 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 subprocessor of its obligations in order to avoid its own liabilities.

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 subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

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.

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.

Clause 8

Cooperation with supervisory authorities

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.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, 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.

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

Clause 9

Governing Law

The Clauses shall be governed by the laws of the jurisdiction in which the data exporter is established (being either a jurisdiction within the United Kingdom or a Member State of the EEA).

Clause 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 Clause.

Clause 11

Subprocessing

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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor 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 subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 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 subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in

paragraph 1 shall be governed by the laws of the jurisdiction in which the data exporter is established (being either a jurisdiction within the United Kingdom or a Member State of the EEA).

4. The data exporter shall keep a list of subprocessing 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.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor 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.

2. The data importer and the subprocessor 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.

APPENDIX 1 TO THE UK SCCS

Particulars of the Transfer

Data exporter	Customer.
Data importer	Copper CRM, Inc.
Categories of Data Subjects	As set out in Annex A to the DPA (*Data Processing Details*).
Categories of Data	As set out in Annex A to the DPA (*Data Processing Details*).
Special categories of data	As set out in Annex A to the DPA (*Data Processing Details*).
Processing Operations	Storing, copying, accessing, sharing, modifying.

APPENDIX 2 TO THE UK SCCS

Data Security

The technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) are those set out in Annex B to the DPA (Safeguards).