CRESTA INTELLIGENCE INC.

GLOBAL VENDOR DATA PROCESSING ADDENDUM

This Global Vendor Data Processing Addendum ("**DPA**") forms part of the agreement(s) between Cresta Intelligence Inc. and its affiliates ("**Cresta**") and Vendor and its affiliates ("**Vendor**") (hereafter the "**Parties**") (the "**Agreement**"). The DPA reflects the Parties' agreement with regard to the access, processing, and storage of Cresta Data made available to Vendor in connection with Vendor's performance of the Agreement. Capitalized terms, unless expressly defined herein, shall have those meanings set forth in the Agreement.

This DPA is in addition to, not in lieu of, any other contractual obligations and applicable legal or regulatory obligations Vendor has with respect to Cresta Data. Where there is a conflict between this DPA and any other document signed by the Parties, the provisions of this DPA shall govern with regard to Vendor's processing of Cresta Data.

1. **OWNERSHIP OF CRESTA DATA.**

    a. Vendor's performance under the Agreement or this DPA does not grant Vendor any ownership interest in or title to any Cresta Data.

2. **PERMITTED PROCESSING OF CRESTA DATA.**

    a. Vendor may only process Cresta Data in accordance with Cresta's documented, signed instructions, to provide the Services under the Agreement in the interest and on behalf of Cresta.

    b. Vendor will not publicly disseminate Cresta Data or provide (or purport to provide) to any third party the right to process Cresta Data in exchange for monetary or other valuable consideration.

    c. Vendor is prohibited from retaining, using, or disclosing Cresta Data for any purpose, including any commercial purpose, other than performing the Services under the Agreement for Cresta.

    d. Vendor will comply with the terms of any applicable regional or country specific privacy terms as included in the DPA.

3. **COMPLIANCE.**

    a. Cresta may modify this DPA to ensure the parties' compliance with applicable law.

    b. Vendor will inform Cresta in writing if, in Vendor's opinion, Cresta's instructions would be in breach of Privacy Laws.

4. **SECURITY INCIDENTS.**

    a. **Notice.** If Vendor discovers a Security Incident or has reason to believe a Security Incident is likely to have occurred or is occurring, Vendor shall promptly (in any event, without undue delay and no later than 24 hours after Vendor or any of Vendor's employees, representatives, or agents discovers the Security Incident) notify Cresta at cresta-privacy@cresta.ai. Vendor shall cooperate with Cresta in any communication efforts, including legally required notifications to law enforcement agencies, data protection authorities and/or impacted customers and individuals, resulting from or relating to a Security Incident. Any decision to notify individuals or public authorities of the Security Incident shall be made between both parties, and any notice, public or otherwise, relating to such Security Incident shall be reviewed and approved in writing in advance by Cresta.

    b. **Response.** Vendor shall use commercially reasonable efforts to cooperate with Cresta in responding to a Security Incident, including, without limitation, providing copies of all relevant log, IDS, and security event data to Cresta, making Vendor staff with information security experience available to work with Cresta in understanding the details of any Security Incident, and allowing Cresta forensic investigation personnel and/or Cresta audit personnel to work directly with Vendor staff in joint investigation activities, or to conduct audits of Cresta Data security and control measures. Vendor shall perform, or

cause to be performed, such further acts as Cresta requests in responding to the Security Incident.

c. **Costs.** Vendor will indemnify and hold Cresta harmless for any and all claims, losses, costs, expenses, damages, or other liabilities (including reasonable legal fees) suffered or incurred by Cresta as a result of the accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure of, or access to Cresta Data as caused by Vendor or Vendor Subprocessors. Any limitation of liability contained in the Agreement shall not apply to Vendor's obligations under this Section 4(c).

5. **SUBCONTRACTING AND THIRD PARTY TRANSFERS.**

a. Vendor will: (i) provide to Cresta an up-to-date list of Vendor's then-current affiliates or third party contractors ("Subprocessors") upon signature of this DPA and upon request thereafter; and (ii) provide at least forty-five (45) days' prior notice of the addition or removal of any Subprocessors, including the categories of data processed, details of the subprocessing to be performed, the location of the subprocessing, and a copy of any data protection/privacy related provisions within Vendor's contract with such Subprocessors. If Cresta refuses to consent to Vendor appointment of a Subprocessor on reasonable grounds relating to the protection of Cresta Data, then Cresta may elect to suspend or terminate this Agreement without penalty.

b. Vendor shall not subcontract any processing of the Cresta Data to any Subprocessor without entering into a written agreement with the Subprocessor that imposes upon the Subprocessor legal obligations for the processing of Cresta Data that are at least as protective of Cresta Data as the legal obligations Vendor has undertaken pursuant to this DPA.

c. Vendor shall be fully liable for any breach of this DPA caused by its Subprocessors.

d. Vendor will not disclose or transfer or allow access to Cresta Data by any third party except (i) to a Subprocessor in a manner that complies with the terms of this DPA; and (ii) as required by applicable law, provided that, Vendor will promptly notify Cresta of such a required disclosure (unless prohibited by law), make all reasonable attempts to delay disclosure to the degree necessary for Cresta to meaningfully participate in Vendor's response (unless prohibited by law), and will cooperate with Cresta to contest or minimize the scope of the disclosure.

6. **CROSS BORDER TRANSFERS.**

Vendor will provide at least thirty days' prior written notice to Cresta of the location of the processing activities Vendor or its Subprocessors carry out on behalf of Cresta and Vendor will at all times comply with any requirements applicable to cross border transfers of personal data under Privacy Laws.

7. **DISCLOSURE OF DPA.**

Cresta may disclose this DPA and any relevant privacy/data protection provisions in the Agreement (i) as required by applicable law or upon request or demand from relevant regulatory authorities, (ii) to Cresta Customers, (iii) in connection with any legal suit to which the existence and terms of this DPA are relevant, and (iv) as required and in compliance with any applicable laws. Any such disclosure shall not be deemed a breach of any confidentiality provisions contained in this DPA or the Agreement.

8. **COOPERATION.**

Vendor will provide all assistance reasonably requested by Cresta to enable Cresta to respond to, comply with, or otherwise resolve any data protection requests, questions, or complaints received from any individual, household, Cresta customer, data protection authority, law enforcement, or other regulatory body. If any such communication is received directly by Vendor, Vendor will immediately inform Cresta and will not respond to such communication unless required by law or expressly authorized by Cresta.

9. **DATA RETENTION.**

Upon termination or expiration of the Agreement, or at any time upon Cresta's request, Vendor will promptly (and in no event more than thirty (30) days post termination, expiration, or request) cease to process Cresta Data and will promptly return or destroy the Cresta Data (including all copies) in Vendor's

possession or control (including any Cresta Data held by Subprocessors) as instructed by Cresta. Upon request, Vendor will certify to Cresta in writing that all Cresta Data has been destroyed. This requirement shall not apply to the extent that Vendor is required by applicable laws to retain some or all of the Cresta Data, in which case Vendor shall isolate and protect the Cresta Data from any further processing except to the extent required by law.

10. **DATA SECURITY.**

Any person that Vendor authorizes to process the Cresta Data shall be subject to a duty of confidentiality at least as protective of the Cresta Data as the Agreement and this DPA. Vendor shall implement appropriate technical and organizational measures to protect Cresta Data from Security Incidents. At a minimum, such measures shall include those identified in Annex II.

11. **AUDITS.**

Upon Cresta's reasonable request (not to exceed one routine audit in a 12-month period), or at any time following a Security Incident, suspected non-compliance, or upon request from a data protection authority, Cresta, its appointed representatives, the ultimate Data Controller, or the competent supervisory authority may audit Vendor's compliance with this DPA.. Vendor shall make available to Cresta all information, systems, staff, and on-site facilities necessary for Cresta (or Cresta's third party auditors) to conduct such audit.

12. **MISCELLANEOUS.**

a. **Conflict.** In case of conflict between these Global Data Processing Terms and the terms of the EEA, UK and Switzerland Privacy Terms (Appendix 1) or the US Privacy Terms (Appendix 2), the latter shall prevail with regards to their respective subject matter.

b. **Consideration.** The Parties have exchanged good and valuable consideration, the sufficiency of which is acknowledged by the parties, in connection with entering into this DPA. Nothing in this DPA shall be construed to alter any amounts owed by Cresta to Vendor pursuant to the Agreement.

c. **Survivability.** This DPA shall survive the termination of the Agreement to the extent and for as long as Vendor or any Subprocessor has access to or possession of any Cresta Data.

13. **DEFINITIONS.**

a. "**Cresta Data**" means any and all Personal Data processed by Vendor as part of the performance of the services, as specified under the Master Vendor Services Agreement. Cresta Data may include customer user data, employee data, communications content data, or service usage data.

b. "**Personal Data**" shall have the meaning given to the terms "personal data" and "personal information" under Privacy Laws.

c. "**Process**" means any operation or set of operations which is performed on Cresta Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

d. "**Privacy Laws**" means all data protection and privacy laws and regulations applicable to the Processing of Personal Data under the Agreement.

e. "**Security Incident**" means any destruction, loss, alteration, disclosure of, or access to Cresta Data that is accidental, unlawful, or unauthorized.

ANNEX I - DESCRIPTION OF PROCESSING

This Annex I forms part of the Agreement and describes the processing that Vendor will perform on behalf of Cresta.

Scope, nature and purpose of the processing:

The Personal Data will be processed to perform the Services as specified in the Agreement.

Duration of the processing:

The Personal Data will be processed for the term specified under the Agreement.

Data subjects:

The Personal Data to be processed concern the categories of data subjects specified in the Agreement.

Categories of Personal Data:

The Personal Data to be processed concern the categories of data specified in the Agreement.

Special categories of Personal Data (if applicable):

Unless expressly specified in the Agreement, Vendor shall not process special categories of personal data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

The frequency of the transfer is set out in the Agreement.

Nature of the processing:
The nature of the processing activities is described in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

The retention period applicable to the personal data is specified in the Agreement.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing:
The list of the subprocessors used by the Vendor is specified in the Agreement.

ANNEX II - TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

This Annex II forms part of the Agreement and sets out the minimum technical and organizational measures that Vendor will implement to protect Cresta Data. The information provided constitutes Annex II of the EU Standard Contractual Clauses and Swiss Standard Contractual Clauses /Appendix 2 of the UK International Data Transfer Addendum, as applicable.

1. Vendor will employ appropriate technical and organizational measures to protect against unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data ("Information Security Program"), in accordance with all applicable Data Privacy Laws that govern the security of Personal Data.

2. Vendor's Information Security Program includes specific security requirements for its personnel and all subcontractors or agents who have access to Customer Personal Data ("Data Personnel"). Vendor's security requirements cover the following areas:

    a. **Information Security Policies and Standards.**
    Vendor will maintain written information security policies, standards and procedures. These policies, standards, and procedures shall be kept up to date, and revised whenever relevant changes are made to the information systems that use or store Customer Personal Data. These policies, standards, and procedures shall be designed and implemented to:
        i. Prevent unauthorized persons from gaining physical access to Customer Personal Data Processing systems (e.g. physical access controls);
        ii. Designate one or more employees to coordinate the Information Security Program;
        iii. Prevent Customer Personal Data Processing systems from being used without authorization (e.g. logical access control);
        iv. Ensure that Data Personnel gain access only to such Customer Personal Data as they are entitled to access (e.g. in accordance with their access rights) and that, in the course of Processing or use and after storage, Customer Personal Data cannot be read, copied, modified or deleted without authorization (e.g. data access controls);
        v. Ensure that Customer Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage, and that the recipients of any transfer of Customer Personal Data by means of data transmission facilities can be established and verified (e.g. data transfer controls); and
        vi. Ensure that all systems that Process Customer Personal Data are the subject of a vulnerability management program that includes without limitation regular internal and external vulnerability scanning with risk rating findings and formal remediation plans to address any identified vulnerabilities. Any critical severity vulnerabilities will be remediated within seven days of identification and high severity vulnerabilities will be remediated within fifteen days of identification.

    b. **Compliance.**
    On an annual basis, Vendor will have a reputable, independent third-party auditor perform and maintain a SOC 2 Type II audit and will provide the results of the audit to Customer. Failure to provide the audit reports will be a material breach of the Agreement for which Customer may terminate the Agreement or the applicable ordering document.

    c. **Application Security.**
    Vendor shall conduct an annual penetration test of all systems processing Customer Data. Such penetration tests must be performed by a qualified independent third party and must include authenticated, manual testing of application logic in addition to automated scanning. Tests limited to automated scanning, surface-level header analysis, or unauthenticated reconnaissance shall not satisfy this requirement. Testing must be conducted against production or a production-equivalent environment and must follow a recognized methodology such as OWASP, PTES, or NIST SP 800-115. Results, including any critical, high and medium

findings, must be remediated within timeframes consistent with Vendor's vulnerability management policy, and evidence of remediation must be made available to Customer upon request

d. **Physical Security.**
Vendor will maintain commercially reasonable security systems at all Vendor sites at which an information system that uses or stores Customer Personal Data is located ("Processing Locations") that include reasonably restricting access to such Processing Locations, and implementing measures to detect, prevent, and respond to intrusions.

e. **Organizational Security.**
Vendor will maintain information security policies and procedures addressing:
   i. Data Disposal. Procedures for when media are to be disposed or reused have been implemented to prevent any subsequent retrieval of any Customer Personal Data stored on media before they are withdrawn from the Vendor's inventory or control.
   ii. Data Minimization. Procedures for when media are to leave the premises at which the files are located as a result of maintenance operations have been implemented to prevent undue retrieval of Customer Personal Data stored on media.
   iii. Data Classification. Policies and procedures to classify sensitive information assets, clarify security responsibilities, and promote awareness for all employees have been implemented and are maintained.
   iv. Incident Response. All Customer Personal Data security incidents are managed in accordance with appropriate incident response and remediation procedures.
   v. Asset Management. Policies and procedures as well as technical controls such as mobile device management (MDM) to ensure all employees and contractors use company-managed devices with full disk encryption and patch management controls enabled.

f. **Network Security.**
Vendor maintains commercially reasonable information security policies and procedures addressing network security and intrusion detection and/or intrusion prevention capabilities are implemented on any system that handles Customer Personal Data.

g. **Access Control (Governance).**
   i. Vendor governs access to information systems that Process Customer Personal Data.
   ii. Only authorized Vendor staff can grant, modify or revoke access to an information system that Processes Customer Personal Data.
   iii. Vendor implements commercially reasonable physical and technical safeguards to create and protect passwords.

h. **Virus and Malware Controls.**
Vendor protects Customer Personal Data from malicious code and will install and maintain anti-virus and malware protection software on any system that handles Customer Personal Data.

i. **Personnel.**
   i. Vendor has implemented and maintains a security awareness program to train all employees about their security &and privacy obligations annually. This program includes training about data classification obligations, physical security controls, security practices, and security incident reporting.
   ii. Data Personnel strictly follow and acknowledge annually established security policies and procedures. Disciplinary process is applied if Data Personnel fail to adhere to relevant policies and procedures.
   iii. Vendor shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may Process Customer Personal Data.

j. **Subcontractor security.** Vendor shall only select and contract with subcontractors that are capable of maintaining appropriate security safeguards that are no less onerous than those contained in the Addendum and this Exhibit.

k. **Business Continuity.** Vendor implements disaster recovery and business resumption plans. Business continuity and/or disaster recovery plans are tested and updated regularly annually to ensure that they are up to date and effective. Vendor shall also adjust its Information Security Program in light of new laws and circumstances, including as Vendor's business and Processing change. The Information Security Program and its policies shall be updated and reviewed at least annually.

l. **Intrusion Detection.**
Vendor shall deploy and maintain an Intrusion Detection System (IDS) or equivalent technology to identify malicious activity within its infrastructure that processes Cresta Data. Vendor shall provide Cresta with the name of the tool(s) used upon request. Failure to maintain an IDS or equivalent control shall constitute a material breach of this Agreement for which Cresta may terminate the Agreement.

m. **Secrets Management.**
Vendor shall implement and maintain a formal secrets management program to protect credentials, API keys, tokens, and other sensitive configuration values used in systems processing Cresta Data. Secrets shall not be stored in plaintext in source code, configuration files, or logs or transferred unencrypted over insecure communication channels. Failure to maintain a secrets management program shall constitute a material breach of this Agreement for which Cresta may terminate the Agreement.

n. **Security Information and Event Management (SIEM).**
Vendor shall operate a SIEM or equivalent security monitoring platform that aggregates and analyzes security events from systems processing Cresta Data. Vendor shall ensure that SIEM alerts are actively monitored and that Vendor maintains a documented incident response capability with designated and qualified personnel responsible for responding to security alerts. Failure to operate a SIEM with active monitoring and incident response shall constitute a material breach of this Agreement for which Cresta may terminate the Agreement.

o. **Security Team Structure.**
Vendor shall maintain a dedicated security function with qualified personnel responsible for information security. Vendor shall, upon Cresta's request, provide written confirmation of: (i) the number of employees working in the security function; and (ii) the number of employees tasked with security operations and incident response. Failure to maintain a dedicated security function shall constitute a material breach of this Agreement for which Cresta may terminate the Agreement.

APPENDIX 1
EEA, UK, AND SWITZERLAND PRIVACY TERMS

In addition to the terms contained in the Agreement and the body of the DPA, these EEA, UK and Switzerland Privacy Terms ("European Terms") apply to the processing by the Vendor of Cresta Data originating from the European Economic Area (EEA), the United Kingdom (UK) and Switzerland. Capitalized terms used but not defined in these European Terms shall have the same meanings as set out elsewhere in the DPA.

1. PERMITTED PROCESSING OF CRESTA DATA.

a. Vendor will only:

i. Process Cresta Data on behalf of Cresta as a Processor in compliance with the terms of this DPA, or;

ii. Process Cresta Data as an independent Controller in compliance with Vendor's obligations as Controller under Privacy Laws and this DPA as applicable.

2. INTERNATIONAL TRANSFERS.

At all times, Vendor will provide an adequate level of protection for Cresta Data in accordance with the requirements of Privacy Laws. Vendor will not process or transfer, or allow any third party to process or transfer, any Cresta Data in or to a territory outside of the European Economic Area, United Kingdom, or Switzerland, without Cresta's prior written consent and unless Vendor takes such measures as are necessary to ensure the transfer is in compliance with Privacy Laws.

a. If Vendor processes Personal Data acting as a processor for Cresta:

i. if the Services involve the export of Personal Data from the European Economic Area (EEA), or Switzerland, to a country that has not been recognized by the relevant authorities as providing an adequate level of protection for personal data, Module 2 (when Vendor is acting as processor to Cresta acting as controller) or Module 3 (when Vendor is acting as sub-processor to Cresta acting as processor) of the EU Standard Contractual Clauses will apply, as applicable to the respective data transfer;

ii. if the Services involve the export of Personal Data from the UK to a country that has not been recognized by the relevant authorities as providing an adequate level of protection for Personal Data, the UK International Data Transfer Addendum to the relevant EU Standard Contractual Clauses Module 2.

b. If Vendor process Personal Data acting as a controller for Cresta:

i. If the Services involve the export of Personal Data from the European Economic Area (EEA), or Switzerland, to a country that has not been recognized by the relevant authorities as providing an adequate level of protection for Personal Data, Module 1 of the EU Standard Contractual Clauses will apply;

ii. if the Services involve the export of Personal Data from the United Kingdom, to a country that has not been recognized by the relevant authorities as providing an adequate level of protection for Personal Data, the UK International Data Transfer Addendum to Module 1 of the EU Standard Contractual Clauses will apply.

c. In respect of personal data originating from Switzerland, the EU Standard Contractual Clauses are deemed amended so that any references to the GDPR shall refer to the Federal Act on Data Protection ("FADP"), the term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with clause 18(c) of the clauses, and the clauses shall also protect the data of legal persons until the entry into force of the revised FADP.

d. The EU Standard Contractual Clauses (i) shall not include any clauses marked as optional (except as otherwise specified in this Section); (ii) in Module 2 and Module 3, Clause 9, Option 2 shall apply (as detailed in Section 5 of the Global Data Processing Terms); (ii) shall be governed by the laws of Germany (Clause 17 -

Governing Law); (iv) shall be subject to the jurisdiction of the Courts of Germany (Clause 18 - Choice of forum and jurisdiction), and (v) shall be deemed to be completed with the information provided in the Annexes I and II to these European Terms.

e. The UK International Data Transfer Addendum shall be interpreted as follows: (i) Table 1 shall be completed with the information provided in Annex I of these European Terms; (ii) Table 2 shall be completed as described in this Section 2; (iii) Table 3 shall be completed with Annexes I and II of these European Terms; and (iv) in Table 4, only the Exporter may terminate the UK International Data Transfer Addendum.

3. COOPERATION.

a. Vendor will provide all assistance reasonably requested by Cresta to enable Cresta to respond to, comply with, or otherwise resolve any data protection requests, questions or complaints received from any individual, household, Cresta customer, data protection authority, law enforcement or other regulatory body. If any such communication is received directly by Vendor, Vendor will immediately inform Cresta and will not respond to such communication unless required by law or expressly authorized by Cresta.

b. Vendor shall provide all such reasonable and timely assistance as Cresta may require in order to conduct a data protection impact assessment.

c. Vendor shall consult with any relevant data protection authority where required under applicable Privacy Laws. Where allowable under applicable law, before engaging in such consultation, Vendor shall undertake reasonable efforts to inform Cresta in a manner that reasonably allows Cresta the opportunity to dispute or narrow the scope of Vendor's consultation with any data protection authority.

4. MISCELLANEOUS

a. Unless the above explicitly states otherwise, the terms and conditions of the Agreement, and of the DPA, shall apply to these EEA, UK, and Switzerland Privacy Terms. In case of any conflict between the terms of the Agreement, the DPA, and the terms of these EEA, UK, and Switzerland Privacy Terms, these EEA, UK and Switzerland Privacy Terms prevail with regard to the processing of Cresta Data originating from the EEA, the UK and Switzerland.

b. The Standard Contractual Clauses form an integral part of these European Terms and by entering into the DPA the parties agree to be bound by the Standard Contractual Clauses as specified above in the event that the transfer of Cresta Data to a non-adequate country is required as part of the Services performed by the Vendor under the Agreement.

c. Purely for the purposes of the descriptions in the Standard Contractual Clauses and only as between Cresta and Vendor, Cresta is the "data exporter" (Controller) and Vendor is the "data importer" (Processor or Controller) as appropriate.

d. In the event of any conflict between the Standard Contractual Clauses and this DPA, the Standard Contractual Clauses shall prevail.

5. DEFINITIONS.

a. **"Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, as defined under applicable Privacy Laws.

b. **"EU Standard Contractual Clauses"** means the standard contractual clauses approved by the European Commission's Implementing Decision (EU) 2021/914 available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

c. **"Privacy Laws"** shall be defined as all data protection and privacy laws and regulations applicable to

the Processing of Personal Data originating from the EEA, UK and Switzerland, including but not limited to, the EU General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), the UK GDPR and the Swiss Federal Act on Data Protection.

d. **"Processor"** means a natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller.

e. "**Standard Contractual Clauses**" means the EU Standard Contractual Clauses, the Swiss Standard Contractual Clauses and the UK International Addendum as described in Section 2 of these European Terms, including Annexes I (description of the transfer), II (security measures) of the DPA.

f. "**UK International Data Transfer Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the Information Commissioner under S119A Data Protection Act 2018, which can be found at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance.

Annex I to the Standard Contractual Clauses

A. List of the Parties

Incorporated by reference herein the Signature Page of the Agreement. Cresta Intelligence, Inc. and its Affiliates are the data exporter and Vendor is the data importer.

B. Further descriptions of the data processing are provided below:

Scope, nature and purpose of the processing

The Personal Data will be processed to perform the Services as specified in the Agreement.

Duration of the processing

The Personal Data will be processed for the term specified under the Agreement.

Data subjects

The Personal Data to be processed concern the categories of data subjects specified in the Agreement.

Categories of Personal Data

The Personal Data to be processed concern the categories of data specified in the Agreement.

Special categories of Personal Data (if applicable)

Unless expressly specified in the Agreement, Vendor shall not process special categories of personal data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The frequency of the transfer is set out in the Agreement.

Nature of the processing

The nature of the processing activities is described in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The retention period applicable to the personal data is specified in the Agreement.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing

The list of subprocessors used by the Vendor is specified in the Agreement.

C. Competent Supervisory Authority

The competent supervisory authority for the Data Exporter is:

	EU Standard Contractual Clauses	Swiss Standard Contractual Clauses	UK IDTA

Competent supervisory authority	Competent authority for the data exporter: The competent supervisory authority shall be determined in accordance with Clause 13 of the EU SCCs. Where the Data Exporter (Cresta) is acting as a Processor on behalf of a Data Controller (whether a Cresta Affiliate, such as Cresta GmbH, or a third-party Customer), the competent supervisory authority shall be the supervisory authority of the Member State in which that ultimate Data Controller is established.	For the purposes of Annex I.C under Clause 13: 1. If the data transmission is exclusively subject to the Swiss Federal Act on Data Protection, then the Federal Data Protection and Information Commissioner, or 2. If the data transfer is subject to both the Swiss Act and the GDPR, then either the Federal Data Protection and Information Commissioner or the CNIL (as applicable)	The Information Commissioner for the United Kingdom

Annex II to the Standard Contractual Clauses

The terms of "ANNEX II - TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA" of the DPA are deemed incorporated herein to constitute Annex II of the EU Standard Contractual Clauses and Swiss Standard Contractual Clauses /Appendix 2 of the UK International Data Transfer Addendum.

APPENDIX 2

UNITED STATES PRIVACY TERMS

In addition to the terms contained in the Agreement and the body of the DPA, these United States Privacy Terms ("US Privacy Terms") apply to the processing by the Vendor of Cresta Data originating from the US. Capitalized terms used but not defined in these US Privacy Terms shall have the same meanings as set out elsewhere in the DPA. In case of any conflict between the terms of the Agreement, the body of the DPA, and these US Privacy Terms, these US Privacy Terms prevail with regard to data processing activities subject to US State Privacy Laws.

1. Definitions

a. **Personal Information** shall mean and refer to any information relating to an identified or identifiable person or individual and also includes personal data, as defined by applicable US State Privacy Laws.
b. **Cresta Personal Information** shall mean any Personal Information that the Vendor processes in the course of performing the Services under the Agreement.
c. **Sell** shall have the same meaning as set forth in the applicable US State Privacy Laws.
d. **Service(s)** shall mean the service(s) performed by the Vendor under the Agreement.
e. **Share** shall have the same meaning as set forth in California Privacy Law.
f. **Service Provider** shall mean and refer to a service provider or subcontractor, as defined by applicable US State Privacy Laws, that processes Cresta Personal Information on Cresta 's behalf.
g. **US State Privacy Laws** shall mean and refer to all United States data protection and privacy laws and their respective implementing regulations as they apply to Vendor in the processing of Cresta Personal Information, including but not limited to the California Consumer Privacy Act of 2018, the California Privacy Rights Act of 2020, the Virginia Personal Information Privacy Act of 2021, the Colorado Privacy Act of 2021.

2. Scope of US Privacy Terms

These US Privacy Terms apply to the Vendor acting as Service Provider processing Cresta Personal Information under US State Privacy Laws, where such processing is described in Annex I of the DPA.

3. Roles and Responsibilities

a. **Vendor Obligations.**
   i. **Purpose Limitation**. Vendor shall process the Cresta Personal Information solely for the purpose of performing the Services as described in the Agreement, except where otherwise required by US State Privacy Laws.

   ii. **Obligations.** Vendor will:
      (a) Operate exclusively as a Service Provider and comply with the applicable US State Privacy Law obligations.
      (b) Provide the same level of privacy protection as required by the applicable US State Privacy Law.
      (c) Notify Cresta if it can no longer meet its obligations under US State Privacy Laws.
      (d) Not Sell or Share Cresta Personal Information including not using Cresta Personal Information for cross-context behavioral advertising.
      (e) Not retain, use, or disclose Cresta Personal Information for any other purpose other than as agreed upon in the Agreement, outside the direct business relationship between the Parties, or as permitted by applicable US State Privacy Law.
      (f) Not combine Cresta Personal Information it receives from, or on behalf of, Cresta with Personal Information it receives from, or on behalf of, another person, or collects from its own interactions with the individual, subject to the exceptions under applicable US State Privacy Law.
      (g) Cooperate with Cresta, upon Cresta's reasonable notice, to determine reasonable and appropriate steps to stop and remediate unauthorized use or disclosure of Cresta Personal Information.

b. **Cresta rights**. Cresta may take reasonable and appropriate steps to ensure that Vendor uses Cresta Data in a manner consistent with Cresta's obligations under US State Privacy Laws. Vendor will make available to Cresta all information in its possession to demonstrate compliance with US State Privacy Laws.