# Data Processing Addendum

This Data Processing Addendum (together with the Attachments and Appendix, this "**DPA"**) governs the manner in which HaystackID processes Personal Data and only applies to the extent that HaystackID processes such Personal Data. This DPA supplements and is made an integral and binding part of the Master Services Agreement or Engagement Agreement (the "**Principal Agreement**") and is effective as of the Effective Date of the Principal Agreement (the "**DPA Effective Date**"). In the event of a conflict between this DPA and any other portion of the Principal Agreement, the provision imposing the stricter data processing requirements of any conflicting provision shall control.

Capitalized terms are as defined in the Principal Agreement, herein and in Section 13 below**.**

**Processing Of Personal Data**

**1.1.** Customer will be solely responsible for determining the purposes for which and the manner in which Personal Data are processed**.** The parties agree that Customer acts as the Data Controller of the Personal Data processed by HaystackID in its provision of services to Customer, and HaystackID acts as a Data Processor of the Client Personal Data. The types of Personal Data, purposes of Processing and categories of Data Subjects which may be Processed under this DPA are further specified in Attachment 1 (*Details of Data Processing)*.

**1.2.** Customer instructs HaystackID and each HaystackID Affiliate (and authorizes HaystackID to instruct each Subprocessor) to Process Personal Data subject to complying with the terms of the Principal Agreement and this DPA, as reasonably necessary to provide the Services and consistent with the Principal Agreement.

**1.3.** Each Party shall comply with, and provide the level of privacy protection required by, the Data Protection Laws in performing its obligations under the Principal Agreement and this DPA. HaystackID will inform Customer if, in its opinion, an instruction does not comply with, and will notify Customer if it determines it cannot meet its obligations under, any Data Protection Laws. Customer may take reasonable and appropriate steps to ensure, and HaystackID will provide all information and assistance reasonably necessary for Customer to assess, Customer's compliance with its obligations under the Data Protection Laws, the Principal Agreement and this DPA. Customer may, upon reasonable notice to HaystackID, take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data or terminate the Principal Agreement and this DPA. HaystackID will upon reasonable request of Customer, make available to Customer all information in its possession necessary to demonstrate HaystackID's compliance with the obligations of Data Protection Laws.

**1.4.** Customer represents, undertakes, and warrants that during the term of the Principal Agreement all Personal Data to be Processed by HaystackID, Customer has handled all such data in accordance with all Data Protection Laws. Without limiting the foregoing, Customer shall take all steps necessary, including providing notices to Data Subjects required by the Data Protection Laws and if required by Data Protection Laws shall ensure that there is a lawful basis for HaystackID to process Customer Personal Data.

**1.5.** HaystackID will only Process Personal Data for the specific business purpose of providing the Services specified in the Principal Agreement and only in accordance with Customer's documented instructions unless otherwise required under applicable Data Protection Laws. The Principal Agreement and this DPA and any exhibits, schedules, attachments and amendments or additional agreements constitute Customer's documented instructions regarding HaystackID's Processing of Customer Data.

**1.6.** HaystackID and its Affiliates will not (i) sell, share, collect, rent, release, disclose, disseminate, make available, transfer or otherwise communicate Personal Data to any third party for monetary or other valuable consideration, (ii) retain, use or disclose Personal Data (A) for any purpose, including but not limited to a commercial purpose, other than for the business purpose specified in the Principal Agreement, this DPA or the Data Protection Laws or other laws (B) outside of the direct business relationship between HaystackID and Customer, or (iii) combine Personal Data received from or on behalf of Customer with Personal Data HaystackID receives from or on behalf of another person or business, or collects from its own interaction with the Data Subject, in each of (i) through (iii) other than as permitted by the Principal Agreement, this DPA, Data Protection Laws or other laws.

**2. Data Subject Requests.** HaystackID shall inform Customer promptly following receipt of a Data Subject Request and in a manner consistent with HaystackID's role as Processor/Service Provider shall assist Customer in fulfilling its obligations to respond to Data Subjects' requests to exercise their rights under the Data Protection Laws. Taking into account the nature of the processing and information available to it, HaystackID will take additional technical and organizational measures, to the extent possible, as reasonably requested by Customer to assist Customer in fulfilling its obligations under any Data Protection Laws to respond to Data Subject Requests. Customer shall be responsible for any reasonable costs of such assistance and taking such measures. Notwithstanding its obligations under this Section, unless required by the Data Protection Laws, HaystackID is not obligated to respond to a Data Subject Request made directly to HaystackID from a Data Subject and does not otherwise assume any liability or responsibility for responding to Data Subject Requests

3. **Destruction or Return of Customer Data.** Upon the earlier of termination of the Services or the Principal Agreement and this DPA or at Customer's request, subject to the Data Protection Laws, HaystackID will, at Customer's option either (a) return all Customer Data to Customer, or (b) securely destroy all Customer Data. HaystackID shall upon request provide a signed certification that Customer Data has been returned or destroyed. Regardless of whether the Principal Agreement has terminated or expired, the Principal Agreement and this DPA shall remain in effect until, and automatically expire when, HaystackID deletes or returns all Customer Data.

4. **Disclosure of Customer Data.**

**4.1.** Subject to Section 10, HaystackID may disclose Personal Data only to (i) HaystackID's Subprocessors and its Affiliates acting in such capacity as necessary to perform the Services, and (ii) HaystackID's employees with a need to know to provide the Services. HaystackID shall inform its personnel and Subprocessors engaged in the Processing of Personal Data of the confidential nature of the Personal Data and ensure that they are subject to binding confidentiality obligations.

**4.2.** Both Parties will assist the other in addressing any communications and complying with any instructions or orders of any Supervisory Authority under any applicable Data Protection Laws relating to Customer Data provided to HaystackID. If HaystackID receives an access request from any Supervisory Authority in relation to Customer Data transferred to it or becomes aware that a Supervisory Authority has directly accessed such Customer Data, HaystackID shall use every reasonable effort to redirect the Supervisory Authority to request Customer Data directly from Customer.

**4.3.** If HaystackID is compelled to disclose Customer Data to a Supervisory Authority, HaystackID will promptly notify Customer so that it can seek a protective order or other appropriate remedy, if HaystackID is legally permitted to do so. Where HaystackID is prohibited by law from notifying Customer of such request or access, it shall use all reasonable and lawful efforts to obtain a waiver of the prohibition. HaystackID will at Customer's expense challenge any overbroad or inappropriate request for access to Customer Data where in conflict with applicable law. If after exhausting the procedures described above, HaystackID remains compelled to disclose Customer Data, HaystackID will disclose only the minimum amount of Customer Data necessary to satisfy the request.

5. **Impact Assessments and Prior Consultation.** To the extent required by Data Protection Laws, HaystackID will provide reasonable cooperation and assistance to Customer, at Customer's expense, to carry out data impact or protection assessments of Client's use of the Services taking into account the nature of the Processing and the information available to HaystackID; and will provide reasonable assistance to Customer in the cooperation or consultation with the applicable Supervisory Authority as required by applicable Data Protection Laws.

6. **De-identified Data.** HaystackID shall comply with all laws regarding data that cannot reasonably identify, be related to, describe, be capable of being associated with or be linked directly or indirectly to a Data Subject, including without limitation taking reasonable measures to ensure that the de-identified data cannot be associated with a Data Subject or its household and except as required by law will not re-identify the de-identified data other than as required by law or to verify that de-identification processes satisfy applicable law.

7. **Audits.** Customer may audit HaystackID's compliance with its obligations under this DPA to the extent required by the Data Protection Laws ("**Audit**"), subject to the following:

**7.1.** Customer may, no more frequently than annually (unless required by Data Protection Laws or following a Security Incident) and to the extent required by Data Protection Laws conduct an Audit using an appropriate and accepted control standard or framework pursuant to an agreed audit procedure.

**7.2.** Prior to the commencement of any Audit or inspection, HaystackID and Customer will discuss and agree on: (i) the security and confidentiality controls applicable to any inspection or audit, and (ii) the start date, scope and duration of, and security and confidentiality controls applicable to, any audit. Customer shall give at least thirty (30) days' notice of an Audit, identifying in that notice the Audit scope, purpose and the qualified third party auditor to perform the Audit. HaystackID may object in writing to an auditor appointed by Customer if in HaystackID's reasonable discretion the auditor is not suitably qualified or independent, is affiliated with or retained by a competitor or is otherwise unsuitable. All audits shall be conducted off site of HaystackID's premises during normal business hours. HaystackID shall not be required to breach any duties of confidentiality to its customers, employees, contractors or third parties. The Auditor shall sign a confidentiality agreement reasonably satisfactory to HaystackID.

**7.3.** Customer shall provide HaystackID with a copy of the final Audit report and findings without charge. Customer may use the Audit reports only for the purposes of confirming compliance with the requirements of this DPA. The Audit reports shall be Confidential Information of the parties under the Principal Agreement. The Audit expenses including any additional Services required in relation to the Audit shall be the responsibility of Customer. If additional HaystackID services are required, Customer shall reimburse HaystackID the cost of performing such services.

**7.4.** If an Audit report indicates that HaystackID is not in compliance with its obligations under this DPA or otherwise, HaystackID shall have sixty (60) days to cure the non-compliance. If HaystackID remedies the non-compliance within the applicable cure period there shall be no breach of its obligations under this DPA or the Principal Agreement.

**7.5.** Where the requested Audit scope was addressed in a similar Audit report performed by a qualified third-party auditor for Haystack ID within twelve (12) months of Customer's request; Customer agrees to accept those findings in lieu of requesting an Audit if (i) permitted by the Data Protection Laws; and (ii) there are no known material changes in the controls audited.

**8. Security Measures.** Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity of a Security Incident to the rights and freedoms of natural persons, HaystackID shall implement appropriate technical and organizational measures to help ensure a level of security appropriate to the risk to protect Customer's Personal Data from a Security Incident, including without limitation compliance with the requirements set out in Annex II of the Appendix (Attachment 2) (*Technical and Organizational Measures).*

**9. Security Incident Notification.**

**9.1.** HaystackID shall notify Customer without delay after becoming aware of a Security Incident and shall co-operate and with Customer and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation, and remediation of a Security Incident and meet Customer's obligations under applicable Data Protection Laws.

**9.2.** Notifications made pursuant to this Section 9 will describe to the extent possible and known if required by the Supervisory Authority, details of the Security Incident, a description of its likely consequences including the number of Data Subjects affected, a HaystackID contact with whom Customer can communicate about the Security Incident and steps taken by HaystackID and recommended steps for Customer to mitigate the Security Incident.

**9.3.** Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Security Incident.

**9.4.** The Parties will cooperate in preparing public statements and/or required notices to Supervisory Authorities and the affected Data Subjects.

**10. Subprocessors.** Subject to and in addition to the terms set forth in the Principal Agreement regarding subcontractors (which include Subprocessors) and the other provisions of this DPA and the SCCs related to Subprocessors:

**10.1.** HaystackID may use its Affiliates to Process Personal Data on Customer's behalf and may use third party Subprocessors including but not limited to those listed on Annex III of the Appendix (Attachment 2). HaystackID shall enter into written agreements with such Subprocessors (i) requiring their compliance with Personal Data protection obligations set forth herein if and to the extent required by applicable law, and (ii) permitting access to and use of Customer Data to the extent and for the period required to perform such Services. HaystackID will remain liable to Customer for Subprocessor's performance of such Personal Data protection obligations as required by applicable law. HaystackID shall make available to Customer a mechanism by which to obtain a current list of Subprocessors, subject to the notice obligations set forth in Section 10.2.

**10.2.** HaystackID shall notify Customer in writing including by email or other electronic means of its intention to add or replace a Subprocessor. If Customer reasonably objects to HaystackID's use of a new Subprocessor, then Customer shall within fourteen (14) days following such notification provide written notice of such objection to HaystackID. If HaystackID intends to retain the Subprocessor to which Customer objects to process Customer's Customer Data, HaystackID shall notify Customer before authorizing the Subprocessor to Process Customer's Customer Data and Customer shall have the option to terminate the portions of the Services for which HaystackID has engaged such Subprocessor within thirty (30) days. HaystackID shall have a right to terminate the Master Services Agreement if Customer unreasonably objects to a Subprocessor or does not agree to a written amendment to the Agreement implementing changes in fees and/or Services resulting from the inability to use such Subprocessor.

## **11.** Restricted **Transfers**

**11.1. Cross-border Transfers.** HaystackID will not transfer data across national borders without the consent of Customer except as necessary to provide the Services or as necessary to comply with the law or binding order of a government or Supervisory Authority.

**11.2. Transfer Mechanism(s) for Personal Data Transfers & Standard Contractual Clauses.** Where a cross-border transfer is necessary from the European Union, Switzerland, the European Economic Area and/or their member states, and/or the United Kingdom to a jurisdiction that does not ensure an adequate level of data protection within the meaning of Data Protection Laws, and to the extent such transfers are subject to such Data Protection Laws, such transfer will be made pursuant to the relevant Standard Contractual Clauses ("SCCs") in accordance with the below terms so long as such transfer mechanism is approved by the applicable supervisory authority. Customer and (if applicable) each Customer Affiliate and/or Customer Third Party (each a "data exporter") and HaystackID and (if applicable) HaystackID Affiliate (each a "data importer") hereby enter into and shall be deemed to have executed the applicable Standard Contractual Clauses, which may be the Controller to Processor SCCs, the Processor to Processor SCCs or any Module of the SCCs applicable to the Customer and HaystackID. The SCCs shall be incorporated by reference herein and the SCC Appendix and Annexes to the SCC Appendix shall be deemed to be pre-populated with the information contained in the Principal Agreement and this DPA including Attachment 1, Attachment 2 including the Appendix, Annexes I.A, I.B., I.C, II and III. The applicable SCCs shall be deemed effective on the latest of:

**11.2.1.** data exporter becoming a party to this DPA by signing the Principal Agreement, which will be deemed to be signature on and acceptance of the SCCs and their Appendix by data exporter and in the role of controller or processor;

**11.2.2.** data importer becoming a party to this DPA by signing the Principal Agreement, which will be deemed to be agreement to and acceptance of the SCCs and their Appendix by data importer and in the role of Processor or Subprocessor; and

**11.2.3.** the commencement of an EU, UK or Swiss Restricted Transfer (as applicable) to which the Standard Contractual Clauses relate.

**11.3. EU SCCs.** With respect to an EU Restricted Transfer, the Parties agree:

**11.3.1.** When Customer is acting as the controller and HaystackID is the Processor, the EU Controller-to-Processor Clauses will apply to a Restricted Transfer;

**11.3.2.** When Customer is acting as Processor and HaystackID is a Subprocessor, the EU Processor-to-Processor Clauses will apply to a Restricted Transfer;

**11.3.3.** In Clause 7 the Docking Clause, shall not apply;

**11.3.4.** In Clause 9, Option 2 shall apply and the time period for prior notice of Subprocessor changes will be in accordance with the notification process in Section 10 of this DPA;

**11.3.5.** in Clause 11, the optional redress language shall not apply;

**11.3.6.** in Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by the law specified in the Principal Agreement, provided that law is an EU Member State law recognizing third party beneficiary rights, otherwise the laws of the Republic of Ireland apply; and

**11.3.7.** in Clause 18(b) disputes shall be resolved before the courts of an EU Member State specified in the Principal Agreement; otherwise if none is specified, the Courts of the Republic of Ireland.

**11.4. UK SCCs.** With respect to a UK Restricted Transfer, the EU SCCs (as incorporated by reference pursuant to Section 11.2) shall apply as described in Section 11.3 read in accordance with, and deemed amended by, the provisions of Part 2 (UK Mandatory Clauses) of the UK Addendum, and the Parties confirm that the information required for the purposes of Part 1 (Tables) of the UK Addendum is as set out in the Principal Agreement and this DPA including its Attachments.

**11.5. Swiss SCCs.**

**11.5.1.** With respect to a data transfer subject to both the Swiss Data Protection Laws and the EU GDPR, the Parties shall comply with the Swiss Data Protection Laws and the EU GDPR, as applicable (and the UK Data Protection Laws if applicable and if required by such laws and permitted by the FADP), and the EU SCCs as incorporated by reference pursuant to Section 11.2 shall apply as described in Section 11.3 read in accordance with and deemed amended as follows ("Clause" wherever used shall mean "Clause of the SCCs"):

11.5.1.1. the term "member state" in the SCCs shall 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 (Switzerland) in accordance with Clause 18(c); and

11.5.1.2. the SCCs shall protect the data of legal entities to the extent of and as long as such data is protected under the FADP.

**11.5.2.** With respect to a Swiss Restricted Transfer exclusively subject to the Swiss Data Protection Laws, the EU SCCs as incorporated by reference pursuant to Section 11.2 shall apply as described in Section 11.3 read in accordance with and deemed amended as follows:

11.5.2.1. the applicable law under Clause 17 shall be Swiss law or the law specified in the Principal Agreement, provided that law is of an EU Member State law recognizing third party beneficiary rights; otherwise, the law of the Republic of Ireland applies;

11.5.2.2. the place of jurisdiction under Clause 18(b) for legal actions between the Parties for data transfers pursuant to the FADP shall be as specified in the Principal Agreement, or if none is specified, the courts of the Republic of Ireland;

11.5.2.3. the term "member state" in the SCCs shall 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 (Switzerland) in accordance with Clause 18(c);

11.5.2.4. The SCCs shall protect the data of legal entities to the extent and as long as such data is protected under the FADP; and

11.5.2.5. references to the GDPR in the SCCs shall be understood to be references to the FADP.

**11.6. Additional Safeguards.** If at any time a Supervisory Authority or a court with competent jurisdiction over a party mandates that data transfers from the UK, Switzerland or the EAA must be subject to specific additional safeguards (including but not limited to specific technical and organizational measures), the parties shall work together in good faith to implement such safeguards and ensure that any transfer of Customer Personal Data is conducted with the benefit of such additional safeguards

## 12. General Provisions

**12.1.** The Parties each represent, warrant and certify to the other that they have read, understand and will comply with the requirements of this DPA and all applicable Data Protection Laws and will be responsible for their own compliance with them.

**12.2.** Each party and its respective Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort (including negligence), or under any other theory of liability, will be subject to the limitations and exclusions of liability in the Principal Agreement, and any reference in provisions to the liability of a party means the aggregate liability of that party and all of its Affiliates under and in connection with the Principal Agreement, this DPA and any other agreement subject to such limitations.

**12.3.** The Parties acknowledge that Customer is the Controller or Business and HaystackID is the Processor or Service Provider as described in the Data Protection Laws.

**12.4.** HaystackID may, upon notice to and in cooperation with Customer, update and amend this DPA and its Attachments as may be required from time to time to comply with Data Protection Laws.

**12.5.** A person who is not a party to this DPA shall otherwise have no right to enforce any term of this DPA, except to the extent set out in the relevant Standard Contractual Clauses. The rights of the parties to rescind or vary this DPA are not subject to the consent of any other person.

**12.6.** This DPA shall be governed by the laws of the jurisdiction(s) set forth in the Principal Agreement including this DPA, unless otherwise required by Data Protection Laws including without limitation, the SCCs.

**12.7.** Wherever the provisions of this DPA or the Principal Agreement are inconsistent with any provisions of Data Protection Laws, the provisions of the Data Protection Laws shall supersede. Wherever the provisions of the Standard Contractual Clauses, if applicable as provided in Section 11, are inconsistent with this DPA or the Principal Agreement, the Standard Contractual Clauses shall supersede.

**13. Definitions.** The following terms, including any derivatives thereof, will have the meanings set forth below (capitalized terms not defined herein shall have the meaning given to them in the Principal Agreement):

**13.1.** "**Affiliate**" means in relation to either Customer or HaystackID, an entity that owns or controls, is owned or controlled by or is or under common control or ownership of such entity, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity.

**13.2.** **"Controller to Processor SCCs**" means the Module 2 of the EU Standard Contractual Clauses set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended or replaced from time to time by a competent authority under the relevant Data Protection Laws.

**13.3.** "**Customer**" means Customer, Customer Affiliates and Customer Third Parties as defined in the Principal Agreement.

**13.4.** "**Customer Data**" shall mean all information processed for Customer by HaystackID, its Affiliate or a Subprocessor including but not limited to Personal Data.

**13.5.** "**Data Protection Laws**" means any applicable data protection laws, regulations, guidelines, government issued rules and directives that apply to the performance of the Services under the Principal Agreement and any amendments thereto, including without limitation (i) EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council including implementing or supplementing laws (the "**EU GDPR**"), (ii) the EU GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications Regulations 2019 (**"UK GDPR**") and together with the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended) (together "**UK Data Protection Laws**"**);** (iii) the Switzerland Federal Act of June 19, 1992 on Data Protection and its Ordinance ("**FADP**") and laws implementing or supplementing FADP ("**Swiss Data Protection Laws**" or "**FADP**"), (iv) (the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020,(v) the Colorado Privacy Act,(vi) the Virginia Consumer Data Protection Act, (vii) the Utah Consumer Privacy Act, (viii) the Connecticut Data Privacy Act and (ix) the data protection laws of the United States and any other state or country, all as enacted or amended from time to time and any associated regulations or instruments and any other data protection laws, regulations, regulatory requirements or codes of practice applicable to Processor's Processing of Customer's Personal Data.

**13.6.** "**Data Subject**" means any living identified or identifiable natural person, or where applicable, household, to which Personal Data relates or identifies or as otherwise provided in the Data Protection Laws**."**

**13.7.** "**Data Subject Request**" means a Data Subject's request to access, correct, amend, transfer, rectify, restrict, limit use of, opt out of or delete a Data Subject's Personal Data or otherwise act within a Data Subject's rights under Data Protection Laws.

**13.8. "EU Restricted Transfer**" means, where the EUGDPR applies, a transfer of Customer Personal Data by Customer to HaystackID or any HaystackID affiliate or (or any onward transfer), in each case where such transfer would be prohibited by the EU GDPR in the absence of the protection for the transferred Customer Personal Data provided by the EU SCCs.

**13.9.** **"EU SCCs"** mean the standard contractual clauses for the transfer of Personal Data to processors established in third countries outside the European Economic Area (**"EEA"**), as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 as may be amended or replaced from time to time.

**13.10.** **"Processor-to-Processor Clauses"** means Module 3 of the EU Standard Contractual Clauses set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended or replaced from time to time by a competent authority under the relevant Data Protection Laws.

**13.11.** "**Personal Data**," "**Personal Information**," **"Sensitive Data,"** and **Sensitive Personal Information"** shall have the meaning(s) provided in the Data Protection Laws and may be together referred to herein as Personal Information or Personal Data (and "Sensitive Data" shall include "Special Categories of Personal Data" as defined under the EU GDPR, as applicable).

**13.12.** **"Security Incident**" means any Personal Data Breach (as defined in the EU GDPR) or other security event that has compromised or adversely impacted the confidentiality, privacy, security, integrity, availability or resilience of any Personal Data, including without limitation its unauthorized accidental, unintended or unlawful acquisition, processing, access to, exfiltration, theft, disclosure, destruction, loss or alteration.

**13.13.** **Standard Contractual Clauses**" or "**SCCs"** means (i) the EU SCCs, (ii) the UK SCCs and/or (iii) the Swiss SCCs, as applicable and as updated, amended, replaced or superseded from time to time by the European Commission, the UK Information Commissioner's Office ("**ICO**") or the Swiss Federal Data Protection and Information Commission ("**FDPIC**"); or (ii) where required from time to time by a Supervisory Authority for use with respect to any specific EU, UK or Swiss Restricted Transfer, any other set of contractual clauses or other similar mechanism approved by such Supervisory Authority or by applicable laws for use in respect of an EU, UK or Swiss Restricted Transfer, as applicable and as updated, amended, replaced or superseded from time to time by such regulatory authority or applicable laws.

**13.14.** **"Subprocessor"** means a subcontractor engaged by HaystackID or its Affiliates to Process Personal Data as part of the performance of the Services and otherwise as defined in the Data Protection Laws.

**13.15.** "**Supervisory Authority**" means (a) an independent public authority established by an EU Member State pursuant to Article 51 EU GDPR, the ICO or FDPIC; and (b) any regulatory authority of any state country responsible for the enforcement of Data Protection Laws.

**13.16.** "**Swiss Restricted Transfer"** means where the Swiss Data Protection Laws apply, a transfer of Personal Data by Customer to HaystackID or a HaystackID Affiliate (or any onward transfer), in each case, where such transfer would be prohibited by Swiss Data Protection Laws in the absence of the protection for the transferred Customer Personal Data provided by the Swiss SCCs.

**13.17.** "**Swiss SCCs"** means the EU SCCs as amended by the Swiss Federal Act on Data Protection ("**FADP")** for transfers from Switzerland to countries without an adequate level of data protection.

**13.18.** **"UK Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office under S119A(1) of the Data Protection Act 2018.

**13.19.** **"UK Mandatory Clauses"** means the Mandatory Clauses of the UK Addendum, as updated from time to time and replaced by any final version published by the ICO.

**13.20.** "**UK Restricted Transfer"** means, where the UK Data Protection Laws apply, a transfer of Personal Data by Customer to HaystackID or any HaystackID Affiliate (or any onward transfer), in each case, where such transfer would be prohibited by UK Data Protection Laws in the absence of the protection for the transferred Customer Personal Data provided by the UK SCCs.

**13.21.** "**UK SCCs**" means the EU SCCs as supplemented by the UK Addendum.

The following terms shall have the meanings given them in the Data Protection Laws: “**Business,” “Controller,” “Consumer,” “Member State,” “Process,” “Processing,” “Processor”** and **“Service Provider.**

## ATTACHMENT 1

## DETAILS OF DATA PROCESSING

The details of Processing to be carried out under the Principal Agreement are as follows:

| | |
|---|---|
| Roles of the Parties | Customer, and if applicable Customer Affiliate and/or Customer Third Party (data exporter) will be the business/controller and/or Processor.<br>HaystackID and if applicable HaystackID Affiliate (data importer), will be the Service Provider and/or/ Processor. |
| Subject Matter of Processing | The subject matter of the processing is Customer Data received to provide the Services and Deliverables set forth in the Principal Agreement and Statement(s) of Work. |
| Duration of Processing | The duration of the data processing is determined by Customer within the term of the Principal Agreement, subject to early termination or extension. |
| Nature and Purpose of Processing | The nature and purpose of Processing Personal Data is the provision of Services and Deliverables described in the Principal Agreement and the Statements of Work, including without limitation, preparing for eDiscovery, hosting, organizing, adapting or altering, project management, storing, analyzing, computing, consulting, retrieving, investigating, collecting and recording. Disclosing or transferring of data or otherwise satisfying the legitimate interests of Customer or Customer Affiliates, Customer Third Parties or Customer's clients. The Customer Data Processed by HaystackID (or its Affiliates) may be subject to, but is in no way limited to, the Processing operations as described above. |
| Types (categories) of Personal Data Processed | Types (categories) of Personal Data Processed may include the following:<br>• Personal Data processed for the purpose of seeking, receiving or giving legal advice,<br>• Personal data in respect of which a claim of privilege could be made for the purpose of or in the course of legal proceedings including personal data consisting of communications between a client and his or her legal advisors or between those advisors.<br>• Personal Data necessary for the establishment, exercise or defense of legal claims;<br>• Personal Data subject to an obligation of professional secrecy;<br>• Personal Data relating to pending litigation;<br>• Personal Data that are part of law enforcement/licensing agency records of complaints and investigative and security files;<br>• Personal Data contained in records disclosing the deliberations of agency officials.<br>The foregoing categories may include the following types of Personal Data:<br>• Basic personal information, e.g. birth place, address, postal code, city and country of residence(s) phone numbers, name, initials, email address, gender, birth date, family members and children, social media identifiers, emergency contact details, title, employer, personal life data, geographic information;<br>• Authentication data, e.g., username, password or PIN code, security question;<br>• Contact information such as addresses, email, phone numbers;<br>• Government assigned unique identification numbers, e.g. Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology, and signatures;<br>• Pseudonymous identifiers;<br>• Financial and insurance information, e.g., credit card name and number, credit reports and ratings, insurance number and documentation, bank account name and number, income, type of assurance, payment behavior;<br>• Government filings, including tax returns, social security correspondence and applications; individual reports of government payments; government assistance information;<br>• Commercial Information, e.g., purchases, orders, dates, spending and consumption information, payment history);<br>• Biometric Information, e.g., DNA, fingerprints and iris scans; |

| | |
|---|---|
| | • Digital and analog photos, video, social media data, audio; video meeting information and recordings;<br>• Internet activity including search and browsing history, times online, sites visited, use patterns, reading, television viewing, radio and podcast listening activities);<br>• Device identification (for example IMEI-number, SIM card number, MAC address);<br>• Profiling information, e.g., observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or marketing preference profiles;<br>• Employment data e.g., past, present employment status and employment searches, employment status, recruiting data, resumes, employment history, education, visa and work permit status, tax information, compensation, benefits, salary, bonuses, terms of employment, employment agreements, unemployment insurance, insurance claims filed, union membership and activity;<br>• Information related to disabilities, including Worker's Compensation and social security claims, diagnoses, investigations, assessments, learning disabilities;<br>• Citizenship and residency information, immigration and naturalization status, marital status, nationality, passport information, residency;<br>• Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;<br>• Special categories of data, i.e., sensitive data, e.g., racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, family history data, biometric data for the purpose of uniquely identifying a natural person, health information, sex life or sexual orientation, or criminal or arrest records and investigations; or<br>Any other Personal Data identified in the EU GDPR, the UK GDPR or the FDAP, where applicable. |
| Categories of Data Subjects Whose Personal Data Is Processed | • Customer's or Customer Affiliates' employees, contractors, suppliers, vendors or temporary workers (current, prospective, former), their family members and dependents, acquaintances, friends, co-workers or professional colleagues;<br>• Users and other data subjects who are users of Customer's services;<br>• Individuals who collaborate, communicate or otherwise interact with employees of Customer and/or use communication tools such as apps and websites provided by the data exporter;<br>• Individuals who interact passively with data exporter (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the data exporter);<br>• Minors;<br>• Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).<br>• Parties to litigation, litigation support and related staff and forensic personnel. |

## ATTACHMENT 2

## APPENDIX

## (to the Standard Contractual Clauses)

### ANNEX I

### A. LIST OF PARTIES

**Data exporter(s):** Customer signing the Principal Agreement.
**Name and address:** Customer's name and address listed in the Principal Agreement.
Contact person's name, position, and contact details: Customer's contact person listed in the Principal Agreement.
**Activities relevant to the data transferred under the Standard Contractual Clauses**: Services and Deliverables described in the Principal Agreement.
**Signature and date**: Please see Section 11.2.1 of the Data Processing Addendum.
**Role (controller/processor)**: Controller

**Data importer(s):** HaystackID LLC.
**Name and address:** 200 W. Jackson Blvd, Suite 250, Chicago, IL 60606.
**Contact person's name, position, and contact details**: HaystackID's contact person listed in the Principal Agreement.
**Activities relevant to the data transferred under the Standard Contractual Clauses**: Services and Deliverables described in the Principal Agreement.
**Signature and date**: Please see Section 11.2.2 of the Data Processing Addendum.
**Role (controller/processor)**: Processor

### B. DESCRIPTION OF TRANSFER

***Categories of data subjects whose personal data is transferred***

See Attachment I – Details of Data Processing.

***Categories of Personal Data transferred***

See Attachment 1- Details of Data Processing

***Sensitive data transferred (if applicable) and applied restrictions or safeguards.*** Personal Data transferred may include Sensitive Data concerning health, race or ethnic origin, religion or philosophic beliefs, union membership, criminal records, political affiliation, social security, driver's license, state identification card, passport number, log-in, financial and credit information, debit and credit card numbers, passwords, usernames, security access codes or account access credentials, personal mail, e-mail text and other electronic message content, genetic data, biometric information, data concerning a natural person's sex life or sexual orientation. Sensitive data transferred (if applicable) shall be subject to restrictions or safeguards that take into consideration the nature of the data and the risks involved, such as defining strict purpose limitation, applied access restrictions and safeguards (including access only for staff with specialized training), keeping a record of access to the data, restrictions on onward transfers or additional security measures. Customer may submit special categories of data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion. See Annex II to the Appendix in this Attachment 2 for applied restrictions or safeguards.

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

As necessary under the Principal Agreement and determined by Customer in its sole discretion.

***Nature of the processing***

*The nature of Processing is described in the Principal Agreement, the DPA and Attachment 1.*

***Purpose(s) of the data transfer and further processing***

The purpose of data transfer and processing is described in the Principal Agreement, the DPA and Attachment 1.

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

*The period for which the personal data will be retained is described in the Principal Agreement, the DPA and Attachment 1.*

***For transfers to Subprocessors, also specify subject matter, nature and duration of the processing***

Each Subprocessor will receive all or a portion of the foregoing listed subject matter for the duration set forth in the Subprocessor Agreements depending on their contracted function, with the same nature of Processing as Processor.

## C. COMPETENT SUPERVISORY AUTHORITY

***Identify the competent supervisory authority/ies in accordance with Clause 13 of the SCCs.***

***EU SCCS***

Where the data exporter is established in an EU Member State, the Supervisory Authority of the EU Member State(s) where the data exporter is established shall be the competent Supervisory Authority (Customer to supply).

Where the data exporter is not established in an EU Member State but falls within the territorial scope of application of the EU GDPR in accordance with Article 3(2), and has appointed a representative pursuant to Article 27(1) of the EU GDPR, the Supervisory Authority in the EU Member State where such representative is established shall be the competent Supervisory Authority (Customer to supply).

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without, however, having to appoint a representative pursuant to Article 27(2) of the EU GDPR, the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under EU SCCs in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, shall act as competent supervisory authority (Customer to Supply).

**UK SCCs**

Where the data transfer is subject to the UK Data Protection Laws, the Information Commissioner shall be the supervisory authority.

**SWISS SCCS**

Where the data transfer is subject exclusively to the FADP and not the EU GDPR, the competent supervisory authority is the Swiss FDPIC.

Where the transfer is subject to both the FADP and the EU GDPR, the competent supervisory authority is the FDPIC in so far as the data transfer is governed by the FADP, and the EU competent Supervisory Authority (described under EU SCCs above) in so far as the data transfer is governed by the EU GDPR (the criteria of Clause 13a for the selection of the competent authority must be observed.

## ANNEX II TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF CUSTOMER DATA

These technical and organisational measures are attached to and made part of the Standard Contractual clauses and are incorporated in and made a part of the Data Processing Addendum (DPA) between HaystackID and Customer. These measures are designed, implemented and maintain the security of Customer's information and cover all areas of HaystackID's business operations and information systems. HaystackID maintains written policies, practices and controls to help ensure information security, which are published and communicated to employees and relevant external parties, and which are reviewed and updated periodically to ensure their continuing suitability, adequacy and effectiveness. (Capitalized terms are defined in the DPA.)

### Security Program

HaystackID has in place and will maintain a comprehensive, written information security program of policies, procedures and controls with administrative, technical and physical safeguards applicable to the storage, transmission, processing and security of Customer Data. This security program is designed to ensure the confidentiality, integrity, availability and security of Customer Data; protect against any foreseeable threats, unauthorized, accidental or unlawful access, destruction, loss, alteration, encryption or misuse of Customer Data and ensure proper training of personnel and subcontractors to maintain the confidentiality, integrity, availability and security of Customer Data, consistent with the terms of the DPA, these Security Terms, any Statement or Scope of Work, the Principal Agreement and all applicable laws and regulations. HaystackID employs physical, technical and administrative measures to protect Customer Data from unauthorized access, destruction, alteration, loss or disclosure, to secure physical facilities, to secure network links between offices and data centers and to protect hosted applications from unauthorized access.

### Physical Security

*Data Centers.* HaystackID uses colocation data centers meeting critical infrastructure standards, including N+1 (parallel redundancy) cooling and electrical configurations with maintainability. Haystack's data centers are designed to protect against physical security issues and natural disasters such as fires, floods, earthquakes, explosions, civil unrest, and other potential disasters (In Accordance With SSAE-16 SOC 2 Type 2 Compliance Requirements Data Centers are protected by perimeter Security and portals (mantraps), individual access control to Customer cabinets and cages and carrier-neutral-meet-me areas. Both data center and office security include (i) critical infrastructure with uninterruptible power sources and early detection and suppression fire systems; (ii) network security and connectivity and (iii) technical security including video surveillance, a government issued photo ID requirement, visitor logs with a year's retention, badge activity logs (or proprietary badging system), and biometric authorization in key areas.

*Media, Systems, Machines and Devices.* HaystackID has restrictive protocols for removable media and physical assets, and adheres to strict data removal, storage and destruction standards to protect data through the entire lifecycle. HaystackID maintains an inventory of all physical and information assets in its configuration management systems. Detailed procedures are implemented for the life cycle of removable media including protection against unauthorized access through encryption, key handling, and, when no longer required, the destruction of data and secure disposal of media. All items of equipment containing storage media are verified to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal or re-use. Haystack follows industry standard destruction of sensitive materials before disposition and destruction of hard disk drives containing Customer Data.

### Technical Security

*Network Security**.*** HaystackID employs numerous levels of security to ensure all data is protected from unauthorized access. Security measures include redundant firewalls with intrusion detection systems (IDS) and intrusion protection systems (IPS); both are tied into Haystack's Security Information and Event Management (SIEM) monitored continuously by a third party Security Operations Center (SOC). HaystackID implements network segmentation for performance and security purposes. HaystackID uses multiple monitoring servers to monitor all Internet lines, firewalls (all ports), routers, switches, and servers. Critical application servers are also monitored. HaystackID follows a formal information transfer policy and controls the available information transfer tools. Each department that transfers or receives data has standard operating procedures and controls in place to protect the transfer of information via electronic or physical media.

*Encryption**.*** HaystackID encrypts all Customer data in transit, digital signing and at rest using current industry-standard algorithms and key lengths to protect Customer Data against accidental or unlawful destruction, loss, alteration, access, disclosure or theft. During any electronic or logical transfer, HaystackID transports and receives personal data through highspeed transport applications and environments that are compliant with Federal Information Processing Standard (FIPS) 140-2. During any physical media transfer, HaystackID encrypts all media with Bitlocker or other customer-specified encryption software. HaystackID configures applications to use encrypted communication channels.

While data is at rest, HaystackID's Network Storage (SAN and NAS devices) use either self-encrypting drives (SED) or O/S based encryptionand self-encrypting drives employing industry leading encryption. HaystackID enforces full disk drive encryption on all user hardware and mobile devices. HaystackID has an encryption key management policy covering the full lifecycle of cryptographic keys.

*Access control.* HaystackID line management, security teams, and privacy teams create role-based rights profiles for the business requirements listed in the job descriptions according to the principle of least privileged access. HaystackID has a documented user onboarding (User Access Provisioning) and user offboarding / termination (User Access Deprovisioning) system. Role- based Access Control (RBAC) restricts network access based on the roles of individuals users. RBAC profiles are audited at least annually; user rights are audited against RBAC profiles at least annually.

HaystackID follows NIST Special Publication 800-63B for identity management. Key elements are a minimum of 18 characters, or longer for privileged, shared, or service accounts. Other key elements are minimizing Periodic Resets; enabling "Show Password While Typing"; allowing Password "Paste-In" from the enterprise password management (EPM) system; "blacklisting" weak, previously used, and known compromised passwords; disabling "Password Hints"; and limiting failed attempts before lockout.

HaystackID enforces multi-factor authentication (MFA) and enables SSO wherever possible. The enterprise password management (EPM) system generates strong passwords, provides a secure method of transmitting passwords, manages privileged, shared, or services accounts and integrates with the remote desktop manager (RDM) to enable the use of privileged and shared accounts without the end user knowing the password and automating password changes upon check-in.

HaystackID enforces O/S based encryption, screen lock, pass code, remote wipe, control of application using MDM. HaystackID has policy and supporting security measures to protect information accessed, processed, or stored at teleworking sites. HaystackID enforces O/S based encryption, screen lock, pass code, remote wipe, control of USB ports, Bluetooth and control of application installation on physical windows and devices using configuration management tools

*Change Management.* HaystackID employs a change management system (CMS) to help ensure that changes to the organization, business processes, information processing facilities, and systems that affect information security, privacy, and availability are controlled. HaystackID monitors the use of resources, and management makes projections of future use to ensure adequate future capacity to meet business requirements. HaystackID has a configuration management system that inventories devices, installs software, prevents the installation of blacklisted software, installs certificates, applies security configurations, and applies security and other Microsoft and third party patches.

**Administrative Security**

*Personnel and contractor security.* HaystackID conducts background verification checks proportional to the business requirements, the classification of the information to be accessed, and the perceived security risks associated with a position.

Haystack enters into NDAs and confidentiality agreements with all employees, contractors, Subprocessors and third parties, each of whom accesses systems and services only on a need to know basis with activities segregated from each other. Critical vendors must have recognized third party security certifications. Vendors that provide software or development services must submit documentation of a Security Software Development Lifecycle (SSDLC).

All employees of HaystackID and, where appropriate, contractors receive security and privacy awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function, and are contractually obligated to observe information security procedures, policies and protocols.

*Accountability.* HaystackID implements organizational requirements under the accountability principle, including compliance with the data protection laws through a strong culture of compliance, accountability for compliance with the data security protocols including establishment, documentation and maintenance of business processes and controls. HaystackID maintains an organizational reporting structure that reviews individual and system performance against criteria designed to ensure and enhance security and quality measures, with periodic review against these criteria being an organizational priority.

**Testing and Evaluating Security Measures**

HaystackID performs regular vulnerability identification tests and assessments against all systems that are Processing Customer Data and performs regular penetration tests against any Internet-facing systems. HaystackID performs regular risk assessments of the physical and logical security measures and safeguards it maintains to protect Customer Data.

HaystackID has a vulnerability management system that scans internal systems, external systems and web applications for known vulnerabilities and automatically evaluates and rank risksHaystackID periodically conducts third party reviews of controls to protect security, availability, processing integrity, confidentiality, and privacy and also conducts annual third party penetration tests of internal systems, external systems, and web applications. HaystackID has a third party Managed Threat Response (MTR) team for the detection, prevention, and recovery controls to protect against malware and other hacking attempts. HaystackID also has a third party Security Operation Center (SOC) team that monitors the centralized SIEM that collect data from our firewalls, switches, domain controllers, SAN/NAS devices, and

**Incident Management.**

HaystackID has an Incident Management Plan that establishes management responsibilities and procedures documenting the necessary steps and channels of communication to be followed.to ensure a quick, effective and orderly response to information security incidents. Haystack logs all security incidents and reviews logs and logging procedures periodically to help ensure that incident reporting is complete and timely.

The HaystackID security team will coordinate with the third party MTR and SOC teams to collect evidence, forensically protect evidence and evaluate information security events to decide if they are to be classified as information security incidents. Information security incidents are responded to in accordance with the documented procedures.

**Restoration and Access after a Physical or Technical Incident**

HaystackID has developed and maintains a business continuity impact analysis plan and a disaster recovery plan, which are designed to prevent Customer information and personal data loss as well as to maintain HaystackID's delivery of its services with minimal interruption. HaystackID also implements and regularly tests and updates its disaster recovery and business continuity plans to support the availability, security, integrity and (where necessary) restoration of data. Each plan details measures to support the effective restoration of services, to resume operations as soon as possible after an emergency.

HaystackID implements redundant logical and physical assets where needed to meet availability requirements. Periodic tests help ensure smooth failover. HaystackID ensures that backups are taken offsite, to support the recoverability of HaystackID systems in the event of a disaster. The data is replicated between a minimum of two fully redundant facilities with regional geographic separation of at least 300 miles, which are connected by two 10GB point to point fiber circuits with fully independent non-crossing paths including separate build entry points. Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are detailed in the company's storage management policies and align with the company's business risk management objectives.

HaystackID uses SAN/NAS device snapshots of information, software, and system images at a frequency based on change rates to ensure the ability to recover from accidental or malicious deletion or corruption. HaystackID used SAN/NAS device replication of information, software, and system images at a frequency based on change rates to ensure the ability to recover from temporary or permanent loss of a data center. Haystack's SQL systems have additional protections such as availability groups for key data bases and SQL backups to alternate network storage. Backup copies of information, software, and system images are taken and tested regularly in accordance with a backup policy.

**System configuration, planning and management**

HaystackID maintains processes and procedures for effective management of its systems and their configuration. HaystackID uses advanced hardware and software components and processes within its systems and regularly monitors operating system settings and defaults to assure the systems operate in a stable manner using utilities that allow administrators to change the system configuration.

**Certifications**

HaystackID has adopted strict data security and privacy policies and controls based on industry recognized standards in accordance with the risk of the categories of personal information processed and the likelihood of attempts from public authorities to access it, including, among others: (i) International Traffic in Arms Regulations (ITAR) Compliance; (ii) SSAE-16 SOC II Compliance, ( (iii) ISO 14001 Compliance (Germany), (iv) ISO 9001 Compliance (Germany), (v) PCI DSS Compliance, (vi) HIPAA Security Rule, and  (vii) EU-US and Swiss-US Privacy Shield Certifications.

**Customer Responsibilities**

Customer shall (i) ensure that Customer's approved users follow the same terms of service that apply to Customer; (ii) secure computer systems or devices in Customer's possession, custody, or control from threats that might impact the security, confidentiality, availability, and privacy of data (iii) if Customer directs the use of data transfer tools or methods, Customer is responsible for securing the portion of the chain of custody that Customer controls, including any onward transfers Customer directs which are outside the control of HaystackID; (iv) direct the transfer of data between jurisdictions, including to approve or deny EU country to EU country data replication for disaster recovery and business continuity (v) protect the confidentiality of each Customer user's login and password and managing each Customer user's access to the Services, and prohibiting the sharing of accounts and/or passwords; (vi) take appropriate action to secure, protect and backup Customer Data in a manner that will provide appropriate security and protection, including encryption to protect Customer Data; and (vii) Employing best practices to prevent uploading data containing malicious code into HaystackID's systems.

**Subprocessors**

Subprocessors are obligated to take the same or substantially similar measures described in this Annex II and are regularly monitored to help ensure that such measures are in place to provide assistance to HaystackID as Processor and Data Importer. Subprocessors are listed in Annex III below.

**ANNEX III - LIST OF SUBPROCESSORS**

Customer authorizes use of the following Subprocessors:

| Name of Sub-processor | Address | Description of Service |
|---|---|---|
| HaystackID International Limited | The Ormond Building<br>Suite 4.03, 31-36 Ormond Quay Upper<br>D07R6H0, Dublin, Ireland | HaystackID's EU subsidiary, typically used when client prefers that data stay in the EU or outside of the US |
| Relativity | 231 South LaSalle Street, 8th Floor<br>Chicago, IL 60604 | eDiscovery processing and hosting |
| Amazon Workspaces - AWS | Amazon Web Services, Inc.<br>410 Terry Avenue North<br>Seattle, WA 98109-5210 USA | Terminal-hosting platform for HaystackID's document review teams |
| Veritone -- US | 575 Anton Blvd, Suite 100<br>Costa Mesa, CA, 92626-7672 USA | Video / Audio transcription analysis / redaction, document translation, and document transcoding |
| Veritone -- UK | Parnell House<br>25 Wilton Rd, Pimlico<br>London, UK | Video / Audio transcription analysis / redaction, document translation, and document transcoding |
| Intelligent Voice | 5th Floor, 555 Madison Avenue, New York, 10022 | Video / Audio transcription services |
| Linguistics Systems Inc. | 260 Franklin St<br>Suite 230<br>Boston, MA 02110 USA | Machine translation services |
| Iconic Translation Machines Ltd., an RWS Company | INVENT Building, DCU Campus<br>Glasnevin, Dublin 9, Ireland | Machine translation, with options for translation to be done US or Ireland |
| ModeOne | 14811 Featherhill Road<br>Tustin, CA 94780 | Remote collection of mobile data |
| Azure Compute/Storage Resources - Microsoft Azure | One Microsoft Way<br>Redmond, Washington 98052 USA | Hosts certain instances of Relativity for breach investigations |
| First Watch Technologies, Inc. | 2708 Teron Trace, Suite 250<br>Dacula, GA 300019 | Data breach response services |
| TransUnion | 555 West Adams Street<br>Chicago, IL 60661 | Identity Theft Protection - Credit monitoring |

## Attachment 3

## Additional Terms for the People's Republic of China

The following provisions apply to all transfers of Personal Data subject to the Data Protection Laws of the People's Republic of China (excluding, for these purposes, the Hong Kong and Macau Special Administrative Regions, the "**PRC**"):

1. For the avoidance of doubt, "Applicable Law" includes the Cyber Security Law, the Data Security Law and the Personal Information Protection Law, which shall include implementing measures to comply with these laws, as may be amended or supplemented from time to time.

2. Capitalized words and expressions used in this Exhibit not defined in the legal terms and conditions of this Rider shall have the meanings given under Applicable Law or as defined below:

   a) "**Data Exporter**" means a Party that exports Personal Data to a Data Importer in circumstances where the Personal Data are transferred from the PRC to another country;

   b) "**Data Importer**" means a Party that imports Personal Data to a Data Exporter in circumstances where the Personal Data are transferred from the PRC to another country;

   c) "**Data Subject**" shall mean a natural person who may be identified by reference to Personal Data; and

   d) "**Personal Information Handler**" shall have the same meaning as set out under Applicable Law in the PRC.

3. Data Exporters shall ensure appropriate separate consent has been obtained from Data Subjects and will be maintained for the duration of the transfer of Personal Data from the PRC, including any additional separate consents required in respect of any onward transfers of Personal Data it consents.

4. Data Exporters shall ensure that the transfer of Personal Data from the PRC meets all requirements of Applicable Law, including, as determined by the Data Exporter: (a) the completion of any applicable security review (including repeating and updating such security reviews as required by Applicable Law from time to time); (b) the completion and maintenance of any personal information protection certification in accordance with Applicable Laws; or (c) the entering into by the Data Exporter and Data Importer of standard contractual clauses required by Applicable Law.

5. If at any time, Applicable Law requires the Parties to enter into any standard contractual clauses in respect of transfers of Personal Data from the PRC or the Data Exporter elects standard contractual clauses as a means of complying with Applicable Law, the Parties shall agree such amendments to this Agreement or enter into such additional agreements concerning transfers of Personal Data as may be required.

The Parties agree that the description of transfer set out in Section B of Annex I of Attachment 2, and the description of technical and organisational security measures set out in Annex II, shall apply *mutatis mutandis* for the benefit of any transfer of Personal Data from the PRC, and in relation to any onward transfer of the Personal Data by that Data Importer to another data importer, the receiving data importer shall comply with the same data importer obligations.