Global Brand Monitoring

REGISTER DATA PROTECTION TERMS (DPA)

1. Definitions

1.1 Any capitalised terms used but not defined herein have the meanings set forth in the Agreement (including the Master Service Agreement and Register's Terms & Conditions).

1.2 The following words and expressions have the following meanings in these Data Protection Terms:

(a) "**Affiliate**" means any entity which directly or indirectly controls, is controlled by, or is under common control with a Party. "Control" for the purpose of this definition means the direct or indirect ownership or control of more than 50% of the voting interests of the relevant entity;

(b) "**Register Brand Protection Platform"** means the Register managed platform, wherein sits the ZERO platform or Talisman Platform or any future consolidated Register platform or new platforms managed by Register, through which: (i) Register provides and the Customer receives the Services; and (ii) Register provides the Customer access to the Data. For the avoidance of doubt, the Platform is owned by Corsearch and these Data Protection Terms are entered into by Register as agent for and on behalf of Corsearch, Inc., a U.S. Delaware corporation, Business No. 5350928, with an address at: 6060 North Central Expressway, Suite 344, Dallas, Texas 75206 and Corsearch B.V., a Dutch limited company, company registration no. 54875625, with address Naritaweg 116, 1043 CA Amsterdam, the Netherlands (collectively referred to as "**Corsearch**"); therefore, the terms of these Data Protection Terms are directly enforceable by Corsearch against each Customer if necessary, to which the Customer expressly acknowledges and accepts.

(c) "**Data**" means the types of information, including but not limited to Personal Data relating to the categories of data subjects as determined by the Customer and as described in Schedule A hereto, in each case to the extent processed by or on behalf of Register for or on behalf of the Customer under or in connection with the Agreement, including in the provision the Services;

(d) "**Data Breach**" means any personal data breach in respect of the Data suffered by Register or any Subprocessor of which Register becomes aware during the Term, except to the extent that such breach is caused by the Customer or any User;

(e) "**Data Protection Laws**" means all applicable laws and regulations related to data protection, privacy and/or the processing of Personal Data to which either Party, as applicable, is subject in connection with their respective processing of the Data, including the GDPR, and all national or Member State or relevant Customer-jurisdictional legislation that implements, amends, transposes or provides for any derogations in respect of such laws;

(f) "**Data Subject Request**" means a lawful request from or on behalf of a data subject in respect of the Data to exercise such data subject's rights provided in the Data Protection Laws with respect to their Personal Data, including pursuant to Chapter III of the GDPR, such as rights of access, rectification, erasure, restriction and objection;

(g) "**EEA** means the European Economic Area;

(h) "**EU**" means the European Union;

(i) "**GDPR**" means the EU General Data Protection Regulation 2016/679;

(j) "**Member State**" means any applicable member state of the EU and EEA;

(k) "**Standard Contractual Clauses**" has the meaning specified in Clause 9;

(l) "**Standard Data Retention Period**" has the meaning specified in Clause 10.1;

(m) "**Subprocessor**" means any third party, including any Register Affiliate: (i) who is engaged by Register or by any Register Affiliate to carry out specific processing activities in respect of the Data; or (ii) to whom Register or any Register Affiliate subcontracts any of its obligations under or in connection with these Data Protection Terms;

(n) "**User**" has the meaning given to term "Authorized Persons" in Register's Terms & Conditions;

(o) "**User Personal Data**" means the Personal Data relating to Users, as required, determined and processed by Register for its own purposes, including in order to: (i) provide and ensure the security of

the Services; (ii) grant the Customer and its Users access to the Data; and (iii) process account information and invoicing; and (iv) to communicate with the Customer in order to comply with its obligations under the Agreement; and

(p) "**controller**", "**data subject**", "**international organisation**", "**process**"/"**processing**" (and any other derivations thereof), "**processor**", "**personal data breach**", "**third country**", "**special categories of personal data**" and "**supervisory authority**" each have the meanings specified in the GDPR and "**data exporter" and "data importer**" has the meaning specified in to the applicable Standard Contractual Clauses.

2. General

2.1 **Roles**: With respect to each Party's processing of the Data, the Parties agree that: (a) the Customer is and will at all times remain the controller; and (b) Register is and will all times remain the Customer's processor. Notwithstanding the foregoing, the Customer acknowledges and agrees that Register will be an independent controller in relation to the User Personal Data.

2.2 **General Compliance**. In its respective processing of the Data, each Party shall comply with, and assumes responsibility and liability under its respective obligations pursuant to, the Data Protection Laws. Register shall at all times comply with its obligations under the Data Protection Laws regarding its processing of the User Personal Data.

3. Customer Obligations

3.1 The Customer shall process the Data at all times in accordance with the Data Protection Laws and represents and warrants to Register that:

(a) it is responsible for determining the types of Personal Data and categories of data subjects comprised within the Data;

(b) it is responsible for establishing and has established a valid and lawful legal basis for Register's (and, solely in accordance with these Data Protection Terms,) processing of the Data and the associated purposes for such processing, in each case in accordance with the Data Protection Laws;

(c) its instructions to Register to process the Data are and will be lawful; and

(d) where applicable, it is entitled to transfer the User Personal Data to Register and all such transfers of the User Personal Data from or on behalf of the Customer to Register will be carried out lawfully and in accordance with the Data Protection Laws.

3.2 Customer shall ensure that each User is made aware of Register's applicable privacy practices regarding User Personal Data, as described the Register Privacy Policy as shown on its website.

3.3 Subject at all times to Register's compliance with its obligations under these Data Protection Terms and to the limitations of liability specified in the Agreement, the Customer shall hold Register harmless from any liability or losses suffered by Register or any Register Affiliate arising directly or indirectly from: (i) any processing of the Data by the Customer in breach of its obligations under these Data Protection Terms or the Data Protection Laws; and/or (ii) any breach of the Customer's warranties in Clause 3.1.

4. Subject Matter, Duration and Nature of the Data and Processing

4.1 The Customer agrees that the purposes of processing, the types of Personal Data and categories of data subjects and nature of the processing in relation to the Data are set out in Schedule A hereto. To the extent that Schedule A requires updating at any time during the Term, including to ensure either or both Parties' continued compliance with the Data Protection Laws, the Parties shall work together in good faith to update Schedule A accordingly, provided, however, no amendment to Schedule A may be made without the prior written approval of Register.

4.2 Subject to Clause 10.1., the duration of Register's processing of the Data will be the same as the Term (or, if shorter, until expiry of the relevant Services to which its processing of the Data relates), provided, however, Register acknowledges and agrees that its obligations under these Data

Protection Terms with respect to the Data will apply to Register for so long as Register or any Subprocessor processes the Data under or in connection with the Agreement.

4.3 Subject to the remainder of this Clause 4, Register shall (and shall ensure that each person it authorises to process the Data, including each Subprocessor, will) process the Data:

(a) in accordance with the Data Protection Laws;

(b) solely to the extent necessary and in such manner as is necessary in connection with the provision of the Services; and

(c) in accordance with the lawful documented instructions of the Customer, unless Register is otherwise required to do so to comply with any applicable EU or Member State law or other relevant Data Protection Law (in which case, Register shall provide prior notice to the Customer of such legal requirement, unless that law prohibits such disclosure on important grounds of public interest).

4.4 The Customer acknowledges and agrees that its instructions with respect to Register's processing of the Data are set out in the Agreement (including these Data Protection Terms) and that any additional instructions regarding the processing of the Data agreed between the Parties may be subject to additional fees, in particular to the extent that such instructions are outside the scope of the Services or are not otherwise explicitly covered in the Agreement.

4.5 Register shall immediately inform the Customer if, in its opinion, an instruction from the Customer in relation to the processing of the Data infringes the Data Protection Laws or any applicable EU or Member State data protection provisions, provided, however, the Customer acknowledges and agrees that Register is not responsible or liable for providing the Customer with any form of legal advice.

4.6 Other than expressly set out in these Data Protection Terms, Register is not and will not be liable to the Customer or any other third party for any processing of the Data not contemplated by the Agreement or these Data Protection Terms, including without limitation:

(a) any collection or other direct processing of the Data by the Customer or any Customer Affiliate;

(b) processing of the Data by Users and other third parties (other than Subprocessors); and/or

(c) processing of the Data for purposes not communicated to and agreed by Register.

5. Security and Data Breaches

5.1 Register shall ensure that all persons it authorises to process the Data for or on behalf of Register in the provision of the Services (including its employees and Subprocessors) have committed themselves to confidentiality or are otherwise under an appropriate statuary obligation of confidentiality.

5.2 Register shall take reasonable commercially reasonable steps to ensure the reliability of those of its employees and Subprocessors and use all reasonable endeavours to ensure that such persons have sufficient skills and training in the handling of Personal Data and comply with the Data Protection Laws.

5.3 Having regard to the nature of the Data, Register shall implement (and maintain throughout the Term) appropriate technical and organizational measures to secure the Data and take all measures in this regard as required pursuant to Article 32 of the GDPR, including the measures described in Appendix 2 of the applicable Standard Contractual Clauses, in accordance with European Commission Implementing Decision 2021/914. To the extent that the Customer requires Register to implement any additional technical and organisational security measures in respect of the Data that: (a) are specific to the Customer; and/or (b) differ from Register's measures in place as at the Commencement Date, Register reserves the right to do so at the Customer's sole cost and expense.

5.4 At the Customer's sole cost and expense and taking into account the nature of processing and information available to Register, Register shall provide such assistance as the Customer reasonably requests for the Customer to comply with its obligations pursuant to Article 32 of the GDPR regarding the Data.

5.5 Register shall without undue delay (and in any event within 72 hours) notify the Customer in writing after becoming aware of a confirmed Data Breach. Taking into account the information available to Register, this latter shall use reasonable endeavours to include the following information in such notification:

(a) a description of the Data Breach including, where possible, the approximate number of data subjects and Personal Data records concerned;

(b) the likely consequences of the Data Breach;

(c) the measure(s) taken or proposed to be taken by Register to address the Data Breach including and, where appropriate, to mitigate its possible adverse effects; and

(d) details of a contact point within Register where the Customer can obtain further information or updates in relation to the Data Breach,

provided, however, in the event that all such information is not available to Register or Register is otherwise unable to provide all such information at the same time, Register is permitted to provide such information in phases without undue further delay.

5.6 Register shall use commercially reasonable endeavours to identify the cause of any Data Breach and take such steps as Register deems necessary and reasonable in the circumstances to remediate the cause of and minimise any damage resulting from such Data Breach, to the extent that such remediation is within Register's control.

5.7 The Customer acknowledges and agrees that it is solely responsible under the Data Protection Laws for the notification of any Data Breaches to the affected data subjects and/or applicable supervisory authorities. Without prejudice to the foregoing and taking into account the nature of the processing and the information available to Register, Register shall provide such assistance to the Customer as the Customer reasonably requests in order for the Customer to comply with its obligations under the Data Protection Laws to notify or report Data Breaches, including pursuant to Articles 33 and 34 of the GDPR.

5.8 The Customer agrees to coordinate with Register in good faith regarding the content of any public statements and/or any required notices to the affected data subjects and/or relevant supervisory authorities, in each case which specifically refers to Register, Register's employees, any Subprocessor and/or the Services, regarding any Data Breach.

6. Data Subject Requests

6.1 In the event that the Customer receives any Data Subject Requests during the Term (including any such requests forwarded from Register to the Customer pursuant to Clause 6.2), at the Customers sole cost and expense and taking into account the nature of the processing, Register shall assist the Customer by appropriate technical and organizational measures and provide such assistance as the Customer reasonably requests, in each case in so far as this is possible, for the Customer to comply with its related obligations pursuant to the Data Protection Laws, including pursuant to Chapter III of the GDPR.

6.2 In the event that Register (or any Subprocessor) receives a Data Subject Request directly, to the extent that Register is reasonably able to identify that the Customer is the controller of the relevant data subject's Personal Data (including where the Customer is explicitly named in the Data Subject Request), Register shall use commercially reasonable endeavours to promptly forward the Data Subject Request to the Customer without responding to such request.

6.3 Unless expressly agreed otherwise by Register in writing, Register is not (and will under no circumstances be) required to respond or reply to a Data Subject Request received by the Customer, Register or any Subprocessor.

7. Data Protection Impact Assessments and Prior Consultations

At the Customer's sole cost and expense and taking into account the nature of the processing and the information available to Register, Register shall provide such assistance to the Customer as the Customer reasonably requests in order for the Customer to comply with its obligations in respect of the

Data to conduct data protection impact assessments and consult with supervisory authorities under the Data Protection Laws, including pursuant to Articles 35 and 36 of the GDPR.

8. Subprocessors

8.1 Subject to Register's compliance with the remainder of this Clause 8 and its other relevant obligations in these Data Protection Terms, the Customer hereby provides Register with a general written authorization to engage any Subprocessor(s) that Register deems desirable and necessary in connection with its processing of the Data and/or the provision of the Services, including all such Subprocessors engaged by Register as at the Commencement Date. The Customer agrees that, subject to Register's compliance with its other obligations in this Clause 8, any such Subprocessors may be engaged by Register directly or by any Register Affiliate.

8.2 Register shall comply with the requirements for subprocessing set forth in the Data Protection Laws, including to contractually impose on each Subprocessor (or procure the imposition on each Subprocessor of) data protection obligations that are no less protective that those set forth in these Data Protection Terms.

8.3 In the event that any Subprocessor fails to fulfil its data protection obligations, subject to the limitations of liability set forth in the Agreement, Register shall remain fully liable to the Customer for the performance of each Subprocessor's obligations.

8.4 Register shall provide the Customer with at least 30 days' written notice of any intended changes concerning the addition or replacement of Subprocessors hereunder.

8.5 Customer shall not unreasonably object to the appointment of any such new Subprocessor by or any Register Affiliate and if the Customer does not object in writing to the appointment of any such new Subprocessor in accordance with Clause 8.6, the Customer will be deemed to have approved such appointment.

8.6 If within seven (7) days of the Customer's receipt of the notice described in Clause 8.4, the Customer reasonably objects in writing to Register to the appointment of such new Subprocessor based on objectively justifiable grounds relating to the ability of such new Subprocessor to adequately protect or process the Data in accordance with these Data Protection Terms or the Data Protection Laws, the Parties shall work together in good faith to determine a mutually agreeable resolution to address such objection, including where possible, by Register continuing to provide the Services without the involvement of such new Subprocessor. To the extent that the Parties do no reach a mutually agreeable resolution during such seven (7) day period and Register is reasonably unable to continue to provide the Services without the involvement of such new Subprocessor, each Party will have the right to terminate the relevant portion of the Services to which such new Subprocessor is intended to relate (or if this is not possible, the Agreement) immediately on written notice to the other Party. Nothing in this Clause 8.6 will relieve the Customer of any fee payment obligations in respect of the Services rendered by Register and received the Customer until the date of termination hereunder.

9. International Transfers

9.1 Without prejudice to its other obligations in these Data Protection Terms, Register may:

(a) process the Data on or through its and its Affiliates' and Subprocessors' systems, including in the EEA, United Kingdom and United States; and

(b) transfer the Data to its Subprocessors outside the EEA, provided such transfer (and any subsequent processing) is carried out in accordance with the Data Protection Laws, including:

(i) where the country or jurisdiction in which the relevant Subprocessor is located has received an adequacy decision from the European Commission or any relevant supervisory authority under the Data Protection Laws;

(ii) or through the use of relevant standard contractual clauses approved by the European Commission or any relevant supervisory authority under the Data Protection Laws, including pursuant to the Standard Contractual Clauses, in accordance with the European Commission Implementing Decision 2021/914.

9.2 In the event that the transfer of the Data from the Customer to Register or the re-transmit of Data from Register to Customer constitutes a restricted cross-border transfer (or onward transfer) of the Data to a third country or international organization for the purposes of the GDPR, the Parties agree that, unless another adequate safeguard applies in accordance with the GDPR, subject to the remainder of this Clause 9 and any other applicable terms under the Agreement, all such transfers will be governed by the European Commission approved standard contractual clauses in accordance with the European Commission Implementing Decision 2021/914:

(a) In the event that the Customer, who is the controller with regards to the processing activities performed under this Agreement, is established in the European Economic Area, the Controller to Processor Standard Contractual Clauses (Module Two) shall take effect. For the purposes of the Controller to Processor Standard Clauses, as set forth in the Schedule B, the Customer will be the "data exporter" and Register will the "data importer".

(b) In the event that the Customer, who is the controller with regards to the processing activities performed under this Agreement, is established outside of the European Economic Area, the Processor to Controller Standard Contractual Clauses (Module Four) shall take effect. For the purposes of the Processor to Controller Standard Clauses, as set forth in the Schedule C, the Customer will be the "data importer" and Register will the "data exporter".

(c) For the processing of User Personal Data, as defined in clause 1 and 2.1, the Controller to Controller Standard Contractual Clauses (Module One) shall take effect, as set forth in the Schedule D.

Notwithstanding the foregoing, the Standard Contractual Clauses (and any obligations imposed on data exporters or data importers, whichever is applicable, thereunder) will not apply to the extent that the Data is not directly or indirectly transferred (including via onward transfer) to, or processed by, Register or any Register Affiliate outside the EEA.

9.3 Register shall enter into Processor to Processor Standard Contractual Clauses (Module Three) with any Register Affiliates and Subprocessors, to the extent that:

(a) the transfer of the Data from Register to any Register Affiliate Subprocessor; or

(b) the processing of the Data by Register or any Register Affiliate Subprocessor on behalf of the Customer,

constitutes a restricted cross-border transfer (or onward transfer) of the Data to a third country or international organization for the purposes of the GDPR. All such transfers, unless another adequacy decision or safeguards applies in accordance with the GDPR, will be governed by the Processor to Processor Standard Contractual Clauses, adopted by the European Commission Implementing Decision 2021/914.

9.4 In the event of a conflict between these Data Protection Terms and the applicable Standard Contractual Clauses, the terms of the applicable Standard Contractual Clauses will prevail, save that the Customer acknowledges and agrees:

(a) any breach of the respective Standard Contractual Clauses by any data importer or any data exporter, whichever is applicable, as listed therein will be deemed to be a breach of the respective Standard Contractual Clauses by Register and the Customer will accordingly have no direct cause of action and may not make any claim or bring any other cause of action against any Register Affiliate for such breach other than against Register;

(b) Register's aggregate liability to the Customer in relation to the respective Standard Contractual Clauses will not under any circumstances exceed the limitations of liability set forth in the Agreement;

(c) the audits described in the respective Standard Contractual Clauses will be carried out in accordance with Clause 11 of these Data Protection Terms; and

(d) copies of any Subprocessor agreements will only be provided upon the request of the Customer and may have all commercial information and any other unrelated clauses or information redacted by Register.

10. Data Retention and Return or Deletion

10.1 During the Term, to the extent that Data is maintained within any Register Brand Protection Platform, including ZERO or Talisman, Data is subject to automatic deletion or anonymization. The timing of such deletion or anonymization varies with the review and the outcome of such review performed on the Data and it is set forth in the table herein after. Register shall retain Data in accordance with the retention period outlined herein after ("**Standard Retention Period**"), unless otherwise agreed:

Listing Status	**Folders in ZERO**	**Retention Period**	**Action Upon Expiry**
Not checked/ queued for review	Unchecked	6 months	Full deletion
Listings determined not to be infringing	Verification complete	1 month	Anonymized
Listings where first check has been conducted, but waiting for client/partner client approval	Client/partner client verification	2 months	Full deletion
Listings determined to be infringing	Enforcement in progress and listing removed	2 years	Full deletion

10.2 Following expiry or termination of the Agreement for any reason, at the choice of the Customer, Register shall promptly delete or return to the Customer (or procure the deletion of or return to the Customer of) all the Data then processed by Register and/or any Subprocessor, and subject to Clause 3, delete (or procure the deletion of) existing copies of such Data, unless applicable EU or Member State law or other relevant data protection law(s) requires storage of such Data.

10.3 The Customer acknowledges and agrees that any obligation on Register to delete (or procure the deletion of) existing copies of the Data under Clause 2 shall in no way require Register to delete any copies of Personal Data relating to same data subjects as comprised within the Data, to the extent that such Personal Data was obtained by or on behalf of Register for another customer independently of its provision of the Services to the Customer.

11. Audit

11.1 Register shall make available to Customer all information necessary to demonstrate compliance with its obligations under these Data Protection Terms, and subject to remainder of this Clause 11, shall allow for and contribute to audits (including inspections) performed by the Customer (or another third-party auditor mandated by the Customer) solely in order to verify Register's compliance with its obligations as a processor under these Data Protection Terms.

11.2 If a third-party auditor is to conduct the audit or inspection (as applicable) on behalf of the Customer, the third party must be mutually agreed to by Parties (except if such third party is a competent supervisory authority). Register shall not unreasonably withhold its approval to a third-party auditor requested by the Customer; provided, however, such third party must execute a written confidentiality agreement reasonably acceptable to Register or otherwise be bound by a statutory confidentiality obligation before conducting the audit.

11.3 Regarding any audit or inspection carried out by or on behalf of the Customer pursuant to Clause 11.1:

(a) such audit or inspection may only be conducted once during each consecutive 12-month period beginning on the Commencement Date during the Term, provided, however, additional audits may be carried out by or on behalf of the Customer solely to the extent that, pursuant to the Data Protection Laws, either:

(i) the Customer is required by a supervisory authority to conduct such additional audit or inspection; and/or

(ii) Register suffers a Data Breach requiring the Customer to notify such breach to the affected data subjects and/or any applicable supervisory authority;

(b) the Customer shall provide Register at least 14 days' prior notice in writing of its intention to carry out such an audit or inspection. Such notice must specify at least the proposed date of the audit or inspection, as well as the facilities, documents, information and personnel (if any) that Customer wishes to audit or inspect. The Parties shall work together in good faith to agree on a final audit plan;

(c) the audit or inspection will be carried out at the facilities and in respect of the documents and information mutually agreed between the Parties in the final audit plan;

(d) to the extent that the agreed scope of the audit or inspection can reasonably be addressed by:

(i) Register completing an information security (or similar) questionnaire, then the Customer shall give preference to Register completing such questionnaire rather than requesting an on-site audit or inspection; or

(ii) Register providing a SOC, ISO, NIST or similar audit performed by a qualified third-party auditor within 12 months of the Customer's audit or inspection request and Register certifying in writing that there are no material changes to the controls audited, then the Customer agrees to accept such report in lieu of requesting an audit or inspection;

(e) subject to the agreed final audit plan, such audit or inspection will take place over not more than one day during Register's normal business hours and may not unreasonably interfere with or negatively impact Register's normal business operations and activities;

(f) for any audits or inspections conducted on Register's premises, the Customer shall (and shall ensure that any auditor mandated by the Customer will) comply with all applicable Register security, confidentiality, health and safety and other relevant and commercially reasonable requirements;

(g) the Customer shall provide Register with a copy of any reports generated in relation to any such audit or inspection, unless the Customer is prohibited from doing so under the Data Protection Laws or by a supervisory authority. Each Party shall treat the contents of any such report(s) as Confidential Information for the purposes of the Agreement.

SCHEDULE A – SCOPE OF PROCESSING

This Schedule A forms an integral part of the Data Protection Terms and must be completed by the Parties.

Purposes of Processing	The purposes of the processing to be carried out by the Register as a processor on behalf of Customer in respect of the Data are for the provision of the Services in accordance with the Agreement, including to enable the Customer (and, where applicable, Register on the Customer's behalf) to investigate and enforce intellectual property and other rights against sellers and advertisers of potential counterfeits of the Customer's products/services.
Nature of the Processing	Register may process the Data as necessary for the provision of the Services under the Agreement. Such processing activities may include in relation to the Data (as applicable): • receiving data, including collection, accessing, retrieval, recording and data entry; • holding data, including storage, organisation and structuring; • using data, including analysing and testing; • updating data, including correcting and rectifying; • protecting data, including restricting, encrypting and securing; • enabling access to data by the Customer and Users; and • returning the data to the Customer and erasing or destroying data.

Categories of Personal Data	The Data concerns the following categories of Personal Data, as determined by the Customer:
	• publicly available information relating to, and as published by the data subjects or otherwise accessible from public register, including:
	  ○ names;
	  ○ contact details (including phone numbers, addresses and email addresses);
	  ○ IP addresses;
	  ○ bank account numbers;
	  ○ social media accounts linked to the data subjects and related user names and posts (where applicable and if available);
	  ○ website information (including, where applicable, domain registrant information); and
	  ○ types and quantity of products/services advertised, sold or otherwise made available.
	• the assertion that the data subject may have committed a criminal offence by virtue of the advertisement, sale or making available of counterfeit products/services.

Categories of Data Subjects	The Data relates to the following categories of data subjects, as determined by the Customer: sellers and advertisers of potential counterfeits of the Customer's products/services.

SCHEDULE B -

Controller to Processor Standard Contractual Clauses (Module 2)

SECTION I

Clause 1

Purpose and scope

a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

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

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Intentionally Omitted

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

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

b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

a) The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

   (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

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

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

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

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

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

Clause 15

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

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

b) The Parties agree that those shall be the courts of Florence, Italy.

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

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

Annex I

A. LIST OF PARTIES

Data exporter(s):

The Customer, as defined in the Section 1 of the Agreement.

Data importer(s): The entities whose names and addresses are set out herein:

Entity Name	Role	Jurisdiction	Address	Contact Details
Corsearch, Inc.	Processor	US	6060 N. Central Expressway Suite 344, Dallas, TX, 75206 USA	Diane Fiddle, Chief Legal Officer Diane.Plaut@Corsearch.com +1 646-899-2806
Corsearch Intermediate, Inc.	Processor	US	1209 Orange Street Wilmington, Delaware 19801 USA	Diane Fiddle, Chief Legal Officer Diane.Plaut@Corsearch.com +1 646-899-2806
Corsearch Shanghai Co., Ltd.	Processor	CH	Room 368, Unit 302, No. 211 Futebei Road China, Shanghai Pilot Free Trade Zone Shanghai, China	Diane Fiddle, Chief Legal Officer Diane.Plaut@Corsearch.com +1 646-899-2806
INCOPRO Inc.	Processor	US	Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware 19801 USA	Diane Fiddle, Chief Legal Officer Diane.Plaut@Corsearch.com +1 646-899-2806
INCOPRO (Shanghai) Information Technology Co., Ltd.	Processor	CH	Room 1121, 968 West Beijing Road, Jing'an District Shanghai, China	Diane Fiddle, Chief Legal Officer Diane.Plaut@Corsearch.com +1 646-899-2806

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- The data subjects are described in Schedule A of the Data Protection Terms.

Categories of personal data transferred

- The categories of personal data are described in Schedule A of the Data Protection Terms.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- Not applicable.

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 continuous basis for the duration of the Term of the Agreement.

Nature of the processing

- The nature of the processing is described in Schedule A of the Data Protection Terms.

Purpose(s) of the data transfer and further processing

- The purposes of the processing are described in Schedule A of the Data Protection Terms.

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

- The personal data retention periods are described under Section 10.1 of the Data Protection Terms.

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

- The nature of the processing is described in Schedule A of the Data Protection Terms, and the retention periods are described under Section 10.1 of the Data Protection Terms.

C. COMPETENT SUPERVISORY AUTHORITY

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

The competent supervisory authority in accordance with Clause 13 is identified as the Italian Data Protection Authority: Autorità garante per la Protezione dei dati personali (GPDP)

Annex II

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

The data importer maintains an information program comprised of appropriate policies and procedures designed to protect the personal data transferred against personal data breaches, as well as to identify and minimise security risks. Such information security program includes:

- network security, including firewalls or functionally equivalent technology to protect the data importer's internet connection and network infrastructure;

- access restrictions to the data importer's premises, systems, devices, data and services, including by data importer employees, contractors and service providers. Access is granted only to those who have a legitimate business need for such access;

- data importer employees, contractors and service providers are subject to appropriate confidentiality obligations;

- appropriate secure settings for the data importer's devices and software to ensure the personal data transferred remains secure as much as reasonably possible;

- virus/malware protection to protect against external security intrusions;

- where appropriate, the data employs encryption to protect the personal data transferred when at rest and when in transit;

- software and device update installation and patching to ensure the data importer's systems remain current regarding evolving security threats; and

- regular and secure data backups enabling data restoration in the event off data loss or corruption.

SCHEDULE C -

Processor to Controller Standard Contractual Clauses (Module 4)

SECTION I

Clause 1

Purpose and scope

a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8.1 (b) and Clause 8.3(b)

(iii) Clause 9

(iv) Clause 12

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18;

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - [INTENTIONALLY OMITTED]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data (7), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.

b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

[INTENTIONALLY OMITTED]

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

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

Clause 12

Liability

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

b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

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

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

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

Clause 13

Supervision

[INTENTIONALLY OMITTED]

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

   (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

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

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

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

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

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

Clause 15

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Italy.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Florence, Italy.

Annex I

A. LIST OF PARTIES

Data exporter(s): The entities whose names and addresses are set out herein:

Entity Name	Role	Jurisdiction	Address	Contact Details
Corsearch, Inc.	Processor	US	6060 N. Central Expressway Suite 344, Dallas, TX, 75206 USA	Diane Fiddle, Chief Legal Officer Diane.Plaut@corsearch.com +1 646-899-2806
Corsearch Intermediate, Inc.	Processor	US	1209 Orange Street Wilmington, Delaware 19801 USA	Diane Fiddle, Chief Legal Officer Diane.Plaut@corsearch.com +1 646-899-2806
Corsearch Shanghai Co., Ltd.	Processor	CH	Room 368, Unit 302, No. 211 Futebei Road China, Shanghai Pilot Free Trade Zone Shanghai, China	Diane Fiddle, Chief Legal Officer Diane.Plaut@corsearch.com +1 646-899-2806
INCOPRO Inc.	Processor	US	Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware 19801 USA	Diane Fiddle, Chief Legal Officer Diane.Plaut@corsearch.com +1 646-899-2806
INCOPRO (Shanghai) Information Technology Co., Ltd.	Processor	CH	Room 1121, 968 West Beijing Road, Jing'an District Shanghai, China	Diane Fiddle, Chief Legal Officer Diane.Plaut@corsearch.com +1 646-899-2806

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- The data subjects are described in Schedule A of the Data Protection Terms.

Categories of personal data transferred

- The categories of personal data are described in Schedule A of the Data Protection Terms.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- Not applicable.

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 continuous basis for the duration of the Term of the Agreement.

Nature of the processing

- The nature of the processing is described in Schedule A of the Data Protection Terms.

Purpose(s) of the data transfer and further processing

- The purposes of the processing are described in Schedule A of the Data Protection Terms.

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

- The personal data retention periods are described under Section 10.1 of the Data Protection Terms.

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

- The nature of the processing is described in Schedule A of the Data Protection Terms, and the retention periods are described under Section 10.1 of the Data Protection Terms.

SCHEDULE D -

Controller to Controller Standard Contractual Clauses (Module 1)

SECTION I

Clause 1

Purpose and scope

a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

(iii) Clause 8.5 (e) and Clause 8.9(b);

(iv) Clause 9;

(v) Clause 12(a) and (d);

(vi) Clause 13;

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

(viii) Clause 16(e);

(ix) Clause 18(a) and (b);

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

[INTENTIONALLY OMITTED]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(iv) of the categories of personal data processed;

(v) of the right to obtain a copy of these Clauses;

(vi) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation (2) of the data and all back-ups at the end of the retention period.

8.5 Security of processing

a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and

the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (3) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

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

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

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

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

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

[INTENTIONALLY OMITTED]

Clause 10

Data subject rights

a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. (10) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

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

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

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

Clause 13

Supervision

a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[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) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[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 Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

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

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

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

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

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

Clause 15

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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

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

b) The Parties agree that those shall be the courts of Florence, Italy.

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

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

Annex I

A. LIST OF PARTIES

Data exporter(s):

The Customer, as defined in the Section 1 of the Agreement.

Data importer(s): The entities whose names and addresses are set out herein:

Entity Name	Role	Jurisdiction	Address	Contact Details
Corsearch, Inc.	Controller	US	6060 N. Central Expressway Suite 344, Dallas, TX, 75206 USA	Diane Fiddle, Chief Legal Officer Diane.Plaut@corsearch.com +1 646-899-2806
Corsearch Intermediate, Inc.	Controller	US	1209 Orange Street Wilmington, Delaware 19801 USA	Diane Fiddle, Chief Legal Officer Diane.Plaut@corsearch.com +1 646-899-2806
Corsearch Shanghai Co., Ltd.	Controller	CH	Room 368, Unit 302, No. 211 Futebei Road China, Shanghai Pilot Free Trade Zone Shanghai, China	Diane Fiddle, Chief Legal Officer Diane.Plaut@corsearch.com +1 646-899-2806
INCOPRO Inc.	Controller	US	Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware 19801 USA	Diane Fiddle, Chief Legal Officer Diane.Plaut@corsearch.com +1 646-899-2806
INCOPRO (Shanghai) Information Technology Co., Ltd.	Controller	CH	Room 1121, 968 West Beijing Road, Jing'an District Shanghai, China	Diane Fiddle, Chief Legal Officer Diane.Plaut@corsearch.com +1 646-899-2806

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- The data subjects are persons who are authorized by Register to have access to and use the Register Platform(s). Such persons may be the employees or the clients of the Customers.

Categories of personal data transferred

- The categories of personal data are full name, business email address and phone number, where applicable.

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 one-off to set up the user account of the Register Platform(s).

Nature of the processing

- Register may process the personal data as necessary for the provision of the Services under the Agreement. Such processing activities may include in relation to the personal data (as applicable): receiving data, including collection, accessing, retrieval, recording and data entry; holding data, including storage, organisation and structuring; using data, including analysing and testing; updating data, including correcting and rectifying; protecting data, including restricting, encrypting and securing; and erasing or destroying data.

Purpose(s) of the data transfer and further processing

- The purposes of the processing are for the provision of the Services in accordance with the Agreement, including in order to: (i) provide and ensure the security of the Services; (ii) grant the Customer and its Users access to the Data; and (iii) process account information and invoicing; and (iv) to communicate with the Customer in order to comply with its obligations under 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 personal data retention periods will be in line with the Agreement and Register Personal Data Retention and Destruction Policy.

C. COMPETENT SUPERVISORY AUTHORITY

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

The competent supervisory authority in accordance with Clause 13 is identified as the Italian Data Protection Authority: Autorità garante per la Protezione dei dati personali (GPDP)

Annex II

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

The data importer maintains an information program comprised of appropriate policies and procedures designed to protect the personal data transferred against personal data breaches, as well as to identify and minimise security risks. Such information security program includes:

- network security, including firewalls or functionally equivalent technology to protect the data importer's internet connection and network infrastructure;

- access restrictions to the data importer's premises, systems, devices, data and services, including by data importer employees, contractors and service providers. Access is granted only to those who have a legitimate business need for such access;

- data importer employees, contractors and service providers are subject to appropriate confidentiality obligations;

- appropriate secure settings for the data importer's devices and software to ensure the personal data transferred remains secure as much as reasonably possible;

- virus/malware protection to protect against external security intrusions;

- where appropriate, the data employs encryption to protect the personal data transferred when at rest and when in transit;

- software and device update installation and patching to ensure the data importer's systems remain current regarding evolving security threats; and

- regular and secure data backups enabling data restoration in the event off data loss or corruption.