HUNTERS

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**"), when fully executed, is entered into as of the later signature date below ("**Effective Date**") by and between you, the Customer, as identified in the Agreement (as defined below), or in the signature line below (collectively, "**you**", "**your**", "**Customer**"), and **Cyber Hunters Ltd.** or its Affiliates, as identified in the Agreement or in the signature line below ("**Hunters**", "**us**", "**we**", "**our**"). Both parties shall be referred to as the "**Parties**" and each, a "**Party**".

This DPA reflects the Parties' agreement regarding the Processing of Personal Data (as such terms are defined below) by Hunters on behalf of the Customer in connection with Customer's use of the Service (as defined below) in accordance with the applicable license agreement between the Parties ("**Agreement**").

In consideration of the mutual promises set forth herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged by the Parties, the Parties, intending to be legally bound, agree as follows:

1. DEFINITIONS

The headings contained in this DPA are for convenience only and shall not be interpreted to limit or otherwise affect the provisions of this DPA. Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement.

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity.

"**Control**", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"**Authorized Affiliate**" means any of Customer's Affiliate(s) which is explicitly permitted to use the Service pursuant to the Agreement but has not signed its own agreement with Hunters and is not a "Customer" as defined under the Agreement.

The terms, "**Controller**", "**Member State**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR. The terms "**Business**", "**Business Purpose**", "**Consumer**" and "**Service Provider**" shall have the same meaning as in the CCPA. For the purpose of clarity, within this DPA "Controller" shall also mean "Business", and "Processor" shall also mean "Service Provider", to the extent that the CCPA applies. In the same manner, Processor's Sub-processor shall also refer to the concept of Service Provider.

"CCPA" means the California Consumer Privacy Act of 2018 and its modifications and amendments.

"**Data Protection Laws**" means all applicable and binding privacy and data protection laws and regulations, including such laws and regulations of the European Union, the European Economic Area and their Member States, Switzerland, the United Kingdom, Israel and the United States of America, each as updated or replaced from time to time, as applicable to the Processing of Personal Data under the Agreement, including (without limitation) the GDPR, the UK GDPR, the Swiss FADP and the CCPA, as applicable to the Processing of Personal Data hereunder and in effect at the time.

"**Data Subject**" means the identified or identifiable person to whom the Personal Data relates.

"**GDPR**" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**Personal Data**" or "**Personal Information**" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with an identified or identifiable natural person, which is processed by Hunters solely on behalf of Customer under this DPA and the Agreement. For the avoidance of doubt, Customer's business contact information is not by itself deemed to be Personal Data subject to this DPA.

"**Service**" means Hunters' proprietary software-as-a-service products provided to Customer by Hunters in accordance with the Agreement.

"**Sensitive Data**" means Personal Data that is protected under a special legislation and requires unique treatment, such as "special categories of data", "sensitive data" or other materially similar terms under applicable Data Protection Laws, which may include any of the following: (a) social security number, tax file number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number; (c) financial, credit, genetic, biometric or health information; (d) information 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; and/or (e) account passwords in unhashed form.

"**Standard Contractual Clauses**" or "**SCC**" means (i) the standard contractual clauses for the transfer of Personal Data to Data processors established in third countries which do not ensure an adequate level of protection as set out in Regulation (EU) 2016/679 of the European Parliament and of the Council from June 4, 2021, as available here as updated, amended, replaced or superseded from time to time by the European Commission; or (ii) where required from time to time by a supervisory authority for use with respect to any specific restricted transfer, any other set of contractual clauses or other similar mechanism approved by such Supervisory Authority or by Applicable Laws for use in respect of such Restricted Transfer, as updated, amended, replaced or superseded from time to time by such Regulatory Authority or Data Protection Laws and Regulations

"**Sub-processor**" means any third party that Processes Customer Personal Data under the instruction or supervision of Hunters and/or Hunter Affiliate.

"**Swiss FDAP**" means the Swiss Federal Data Protection Act of 19 June 1992, and as revised as of 25 September 2020.

"**UK GDPR**" means the Data Protection Act 2018, as updated, amended, replaced or superseded from time to time by the ICO.

"UK Standard Contractual Clauses" or "UK SCCs" means the standard contractual clauses for the transfer of Personal Data to Data processors established in third countries which do not ensure an adequate level of protection as set out by the ICO, as available here, as updated, amended, replaced or superseded from time to time by the ICO.

2. PROCESSING OF PERSONAL DATA

2.1. **Roles of the Parties**. The Parties acknowledge and agree that this DPA shall apply where Customer acts as a Controller and Hunters as a Processor, or where Customer acts as a Processor and Hunters as a Sub-Processor.

2.2. **Hunters' Processing of Personal Data**. When Processing Personal Data on Customer's behalf, Hunters shall Process Personal Data in compliance with all applicable Data Protection Laws and for the following purposes: (i) Processing in accordance with the Agreement and this DPA; (ii) Processing for Customer as part of its provision of the Service; (iii) Processing to comply with Customer's reasonable and documented instructions, where such instructions are consistent with the terms of the Agreement, regarding the manner in which the Processing shall be performed; or (iv) Processing as required under the laws applicable to Hunters, and/or as required by a court of competent jurisdiction or other competent governmental or semi-governmental authority, provided that Hunters shall inform Customer of the legal requirement before Processing, unless prohibited to do so by any applicable laws. Hunters shall inform Customer without undue delay if, in Hunters' opinion, an instruction for the Processing of Personal Data given by Customer infringes applicable Data Protection Laws, or if it cannot comply with an instruction from Customer. In any such case, (a) Hunters may, without liability to Customer, temporarily cease all Processing of the affected Personal Data (other than securely storing such data) and/or suspend Customer's access to the Service, and (b) if the Parties do not agree on a resolution to the issue in question and the costs thereof, Customer may, as its sole remedy, terminate the affected Processing in accordance with the terms of the Agreement, and any previously accrued rights and obligations shall survive the termination. Customer will have no further claims against Hunters (including, without limitation, requesting refunds for Services) due to the termination of the Agreement and/or the DPA in the situation described in this paragraph.

2.3. **Customer Responsibilities**. Customer will ensure that it has all necessary, appropriate consents, rights, and notices in place to enable the lawful transfer of the Personal Data to Hunters for the duration and purposes of this DPA. Customer shall not cause Hunters to violate any applicable laws in its Processing of Personal Data in accordance with Customer's instructions.

2.4. **No Assessment of Customer Personal Data by Hunters**. Hunters shall have no obligation to assess the contents or accuracy of Customer's Personal Data, including to identify information subject to any specific legal, regulatory, or other requirement. Customer is responsible for making an independent determination as to whether its use of the Service will meet Customer's requirements and legal obligations under Data Protection Laws.

2.5. **Details of the Processing**. The subject-matter of Processing of Personal Data by Hunters is the performance of the Service pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are specified in Schedule 1 (Details of Processing) to this DPA.

2.6. **Sensitive Data**. The Parties agree that the Service is not intended for the processing of Sensitive Data, and if Customer wishes to use the Service to process Sensitive Data, it must first obtain the Hunters' explicit prior written consent and enter into any additional agreements as required by Hunters.

2.7. **CCPA Standard of Care; No Sale of Personal Information**. To the extent that the Personal Data is subject to the CCPA, Hunters shall not sell Customer's Personal Data. The Parties agree that any monetary consideration provided by Customer to Hunters is provided for the provision of the Service and not for the provision of Personal Data. Hunters shall not have, derive, or exercise any rights or benefits regarding Personal Information Processed on Customer's behalf, and may use and disclose Personal Information solely for the purposes for which such Personal Information was provided to it, as stipulated in the Agreement and this DPA. Hunters certifies that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from selling (as such term is defined in the CCPA) any Personal Information Processed hereunder without Customer's prior written consent, nor taking any action that would cause any transfer of Personal Information to or from Hunters under the Agreement or this DPA to qualify as "selling" such Personal Information under the CCPA.

3. ASSISTANCE

3.1. **Cooperation with Customer.** Taking into account the nature of the processing and the information available to Hunters, Hunters shall reasonably assist Customer, at Customer's expense, in responding to any request from a data subject and in ensuring compliance with Customer's obligations under the Data Protection Laws.

3.2. **Third-Party Requests.** Hunters shall inform Customer of any data subject's request or communications from a regulator, government body, or other supervisory authority relating to personal data that Hunters or its Sub-processors receive, unless applicable law prohibits such notification. Hunters will not respond to such requests except as instructed by Customer, unless otherwise required by any applicable law, in which case Hunters will inform Customer of such legal requirement prior to responding to such request.

3.3. **Data Protection Impact Assessment**. Upon Customer's reasonable written request, Hunters shall provide Customer, at Customer's cost, with reasonable cooperation and assistance needed to fulfill Customer's obligation under the Data Protection Laws to carry out a data protection impact assessment related to Customer's use of the Service, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Hunters.

4. CONFIDENTIALITY

Hunters may disclose and Process the Personal Data (a) as permitted hereunder (b) to the extent required by a court of competent jurisdiction or other Supervisory Authority and/or otherwise as required by applicable laws or applicable Data Protection Laws (in such a case, Hunters shall inform the Customer of the legal requirement before the disclosure, unless prohibited by law), or (c) on a "need-to-know" basis under an obligation of confidentiality to legal counsel(s), data protection advisor(s), accountant(s), investors or potential acquirers. Hunters shall take reasonable steps to ensure that access to the Customer Personal Data is limited on a need-to-know basis and that all Hunters personnel receiving access to Customer Personal Data are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. SUB-PROCESSORS

5.1. **Authorized Sub-Processors.** Customer provides Hunters with a general authorization to engage Sub-processors, subject to Section 5.2, as well as Hunters' current Sub-processors as of the Effective Date of this DPA (available upon email request to privacy@hunters.ai), which are hereby approved by Customer ("**Sub-Processor List**"). Customer further acknowledges and agrees that (a) Hunters' Affiliates may be engaged as Sub-processors; and (b) Hunters and its Affiliates on behalf of Hunters may each engage third-party Sub-processors in connection with the provision of the Service subject to Section 5.2. Hunters shall remain liable for each Sub-processor's compliance with the obligations under this DPA.

5.2. **Changes to Sub-Processors.** Hunters may appoint new Sub Processors and shall notify Customer (e-mail suffices) of such new Sub-processor(s) accordingly. Customer may reasonably object to Hunters' use of a new Sub-processor, for reasons relating to the protection of Personal Data intended to be Processed by such Sub-processor, by notifying Hunters promptly in writing within fourteen (14) days after receipt of Hunters' notice of any such appointment. Such written objection shall include those reasons for objecting to Hunters' use of such new Sub-processor. Failure to object to such new Sub-processor in writing within fourteen (14) days following Hunters' notice shall be deemed as acceptance of the new Sub-Processor. In the event Customer reasonably objects to a new Sub-processor, the Parties will discuss in good faith to achieve a resolution. If Customer does object to the addition of a new Sub-processor, and Hunters, in its reasonable opinion, cannot reasonably accommodate Customer's objection, within a reasonable period of time, Customer may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to the part of the Service which cannot be provided by Hunters without the use of the objected-to new Sub-processor, by providing written notice to Hunters. All amounts due under the Agreement before the effective date of termination with respect to this part of the Service which cannot be provided by Hunters without the use of the objected-to new Sub-processor shall be duly paid to Hunters. Until a decision is made regarding the new Sub Processor, Hunters may temporarily suspend the Processing of the affected Personal Data and/or suspend Customer's access to the Service.

5.3. **Agreements with Sub-processors**. Hunters or its Affiliate on behalf of Hunters has entered into a written agreement with each Sub-processor imposing data protection obligations no less protective of Customer Personal Data as Processors' obligations under this DPA to the extent applicable to the nature of the services provided by such Sub-processor.

6. DATA INCIDENT MANAGEMENT AND NOTIFICATION

Hunters maintains security incident management policies and procedures and, to the extent required under applicable Data Protection Laws, shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data Processed by Hunters on behalf of the Customer (a "**Data Incident**"). Hunters shall make reasonable efforts to identify and take those steps as Hunters deems necessary and reasonable in order to remediate and/or mitigate the cause of such Data Incident to the extent the remediation and/or mitigation is within Hunters' reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or anyone who uses the Service on Customer's behalf. Customer will not make, disclose, release, or publish any finding, admission of liability, communication, notice, press release, or report concerning any Data Incident which directly or indirectly identifies Hunters (including in any legal proceeding or in any notification to regulatory or supervisory authorities or affected individuals) without Hunters' prior written approval, unless, and solely to the extent that, Customer is compelled to do so pursuant to applicable Data Protection Laws. In the latter case, unless prohibited by such laws, Customer shall provide Hunters with reasonable prior written notice to provide Hunters with the opportunity to object to such disclosure, and in any case, Customer will limit the disclosure to the minimum scope required.

7. RETURN AND DELETION OF PERSONAL DATA

Subject to the Agreement, following the termination or expiration of the Agreement, and at the written direction of Customer, Hunters shall delete or return to Customer all the Personal Data it Processes on behalf of the Customer. Hunters shall delete copies of such Personal Data unless Data Protection Laws require or allow otherwise.

8. CROSS-BORDER DATA TRANSFERS OF PERSONAL DATA

8.1. **Transfers to countries that offer adequate level of data protection**: Personal Data that originates from the European Economic Area ("EEA"), Switzerland or the United Kingdom may be transferred to countries that offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities ("**Adequacy Decisions**"), without any further safeguard being necessary.

8.2. **Transfers to other countries:** If the Processing of Personal Data includes transfers from the EEA, Switzerland, or the United Kingdom to countries that do not offer an adequate level of data protection or which have not been subject to an Adequacy Decision ("**Other Countries**"), the Parties shall comply with the terms below:

a) With respect to transfer of Personal Data from the EEA or Switzerland, Customer as a Data Exporter (as defined in the SCCs) and Hunters on behalf of itself and each Hunters' Affiliates (as applicable) as a Data Importer (as defined in the SCCs) hereby enter into the SCC set out in Schedule 2. To the extent that there is any conflict or inconsistency between the terms of the SCC and the terms of this DPA, the terms of the SCC shall take precedence.

b) With respect to transfer of Personal Data from the United Kingdom, Customer as a Data Exporter (as defined in the UK Addendum) and Hunters on behalf of itself and each Hunters' Affiliates (as applicable) as a Data Importer (as defined in the UK Addendum), hereby enter into the UK Addendum set out in Schedule 2.

c) Unless Hunters notifies Customer to the contrary, if the European Commission or ICO subsequently amends the SCC or UK Addendum, as applicable, at a later date, such amended terms will supersede and replace any SCC or UK Addendum executed between the parties.

9. SECURITY & AUDITS

9.1. **Controls for the Protection of Personal Data**. Hunters shall maintain appropriate technical and organizational measures designed to protect Customer's Personal Data Processed hereunder (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data, confidentiality and integrity of Personal Data). Such measures shall, at minimum, meet the requirements in Schedule 3. Upon the Customer's reasonable written request, Hunters will reasonably assist Customer, at Customer's cost, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the Processing and the information available to Hunters.

9.2. **Reports & Audits**. Upon Customer's written request, at reasonable intervals, Hunters shall provide written responses (subject to confidentiality obligations) to reasonable requests for information made by Customer related to its Processing of Customer Personal Data, including responses to information security and audit questionnaires that are reasonably necessary to demonstrate Hunters' compliance with this DPA. If Customer reasonably believes that the information provided by Hunters is insufficient to demonstrate compliance with this DPA, Hunters will allow an audit by Customer (or auditors appointed by Customer and reasonably acceptable to Hunters) in relation to Hunters' Processing of Customer Personal Data. Any such audit will be at Customer's cost and expense, with thirty (30) days prior written notice, conducted during normal business hours, carried out no more than once every 12 months and subject to Hunters' reasonable security and confidentiality requirements. Notwithstanding anything to the contrary, such audits and/or inspections shall not relate to any information, including without limitation, personal data that does not belong to Customer. Such audit (and any data, report, or summary derived from the audit) shall not be used for any other purpose or disclosed to any third party without Hunters' prior written approval and may not allow Customer to review data pertaining to Hunters' other customers or partners. Without prejudice to the rights granted under this section, if the requested audit scope is addressed in a SOC report or similar audit report issued by a qualified third-party auditor within the prior twelve months, and Hunters provides such report to Customer upon request, Customer agrees to accept the findings presented in such third-party audit report in lieu of requesting an audit of the same controls covered in the report. If and to the extent that the Standard Contractual Clauses apply, nothing in this section varies or modifies the Standard Contractual Clauses nor affects any Supervisory Authority's or Data Subject's rights under the Standard Contractual Clauses.

9.3. The audit rights set forth in 9.2 above shall only apply to the extent that the Agreement does not otherwise provide Customer with audit rights that meet the relevant requirements of Data Protection Laws (including, where applicable, article 28(3)(h) of the GDPR or the UK GDPR).

9.4. Nothing in this DPA will require Hunters either to disclose to Customer (and/or its authorized auditors), or provide access to: (i) any data of any other customers of Hunters; (ii) Hunters' internal accounting or financial information; (iii) any trade secret of Hunters; or (iv) any information that, in Hunters' sole reasonable discretion, could compromise the security of any of Hunters' systems, premises or customers or cause Hunters to breach obligations under any applicable law or its obligations to any third party.

10. AUTHORIZED AFFILIATES

10.1. **Contractual Relationship**. The Parties acknowledge and agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, in which case each Authorized Affiliate agrees to be bound by the Customer's obligations under this DPA, if and to the extent that Hunters Processes Personal Data on the behalf of such Authorized Affiliates, thus qualifying them as the "Controller". All access to and use of the Service by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions therein by an Authorized Affiliate shall be deemed a violation by the Customer.

10.2. **Communication**. Customer shall remain responsible for coordinating all communication with Hunters under the Agreement and this DPA and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized.

11. MISCELLANEOUS

This DPA: (i) is the entire agreement of the Parties pertaining to the subject matter of this DPA and supersedes all prior oral discussions and/or written correspondence or agreements between the Parties with respect thereto; (ii) may only be modified by a written agreement signed by persons duly authorized to sign agreements on behalf of the Parties; (iii) is governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws; (iv) is subject to the exclusions and limitations of liability set out in the Agreement and (v) will terminate simultaneously and automatically with the termination or expiry of the Agreement. In the event of any conflict between this DPA and the Agreement, the DPA shall prevail over the conflicting provisions of the Agreement solely with respect to the Processing of Personal Data.

WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement with effect as of the Effective Date.

Hunters:	**Customer:**
By _____	**By** _____
Name _____	**Name** _____
Title _____	**Title** _____
Date _____	**Date** _____

SCHEDULE 1 - DETAILS OF THE PROCESSING

A. LIST OF PARTIES

Data exporter(s):

Name: Customer and its Authorized Affiliates (as identified in the DPA or in the Agreement).

Address: as identified in the DPA or in the Agreement.

Role: Controller.

Contact person's details: to be provided by data exporter to privacy@hunters.ai upon signature of the DPA.

Data importer(s):

Name: Cyber Hunters Ltd. and its Affiliates (as identified in the DPA or in the Agreement).

Address: as identified in the DPA or in the Agreement.

Role: Processor.

Contact person's details: privacy@hunters.ai

***

Activities relevant to the data transferred under these SCCs: The data importer will provide services to the data exporter involving the transfer of personal data as detailed under the Agreement.

B. DESCRIPTION OF TRANSFER

Nature and Purpose of Processing

Hunters will process Customer's personal data as necessary to perform the Services pursuant to the Agreement, as further instructed by Customer (as expressly set forth in this DPA) in its use of the Services.

Duration of Processing

Subject to any section of the DPA and the Agreement dealing with the duration of the Processing and the consequences of the expiration or termination thereof, Hunters will Process Personal Data pursuant to the DPA and Agreement for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, the following categories of Personal Data: Direct identifying information including first name, last name, job title, email address; Indirect identifying information supplied by IT logs including IP address, MAC address, device ID and hostnames; Inferable identifiers provided in logs, potentially including network access, browsing information or business system access.

Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects: users of Customer's IT infrastructure and systems that produce logs which are ingested into Hunters' SOC Platform.

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

Continuous basis.

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

As described in this DPA and/or the Agreement.

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

Subject matter and nature of the processing, as set out at Sub-Processor List, for the duration required for the data importer to provide the Services to the data exporter.

C. COMPETENT SUPERVISORY AUTHORITY

The Supervisory Authority is determined as follows:

Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with the GDPR as regards the data transfer 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 the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to the GDPR: The supervisory authority of the Member State in which the representative is established 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 the GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of the GDPR: The Dutch Data Protection Authority, PO Box 93374, 2509 AJ DEN HAAG, Netherlands, will act as the competent Supervisory Authority.

SCHEDULE 2 – CROSS-BORDER TRANSFERS

1. EU SCCs. If the Processing of Personal Data includes transfers from the EEA to countries outside the EEA that do not offer an adequate level of data protection or which have not been subject to an Adequacy Decision, the Parties shall comply with Chapter V of the GDPR. The Parties hereby execute the Standard Contractual Clauses as follows:

1.1 The Standard Contractual Clauses (Controller-to-Processor) and/or Standard Contractual Clauses (Processor-to-Processor) will apply with respect to restricted transfers between Customer and Hunters that are subject to the EU GDPR. Where Customer acts as a controller and Hunters as processor (as applicable), both parties agree that Module Two will apply. Where Customer acts as a processor and Hunters as a sub-processor (as applicable), both parties agree that Module Three will apply.

1.2 The Parties agree that for the purpose of transfer of Personal Data between Customer (as Data Exporter) and Hunters (as Data Importer), the following shall apply: (i) Clause 7 of the Standard Contractual Clauses shall not apply; (ii) In Clause 9, option 2 shall apply and the method described in Section 5 of the DPA (Sub-Processors) shall apply; (iii) Clause 11(a) of the Standard Contractual Clauses shall not be applicable; (iv) In Clause 17, where the GDPR applies to processing under the Agreement and the country of establishment of the data exporter, as specified in Annex I.A of such SCCs, is a Member State of the European Union whose law allows for third party beneficiary rights, the governing law shall be that country of establishment of the data exporter. Where the GDPR applies to processing under the Agreement and the country of establishment of the data exporter, as specified in Annex I.A of such SCCs, is not a Member State of the European Union, then the governing law shall be the law of the Netherlands; and (v) In Clause 18(b) any disputes arising from the EU Clauses will be resolved by the courts determined in the Agreement, if they are the courts of an EU Member State, otherwise the courts of the Netherlands will resolve such disputes.

1.3 Annex I.A: (1) With respect to Module Two: (i) Data Exporter is Customer as a data controller and (ii) the Data Importer is Hunters and its Affiliates as a data processor; (2) With respect to Module Three: (i) Data Exporter is Hunters as a data processor and (ii) the Data Importer is service provider as a sub-processor. Data Exporter and Data Importer Contact details: As detailed in the Agreement. Signature and Date: By entering into the Agreement and this DPA, each Party is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the DPA.

1.4 Annex I.B of the Standard Contractual Clauses shall be completed as described in Schedule 1 (Details of the Processing) of this DPA.

1.5 Annex I.C of the Standard Contractual Clauses shall be completed as described in Schedule 1 (Competent Supervisory Authority) of this DPA.

1.6 Annex II of the Standard Contractual Clauses shall be completed as described and agreed between the parties in the Agreement and/or this DPA.

1.7 Annex III of the Standard Contractual Clauses shall be completed with the authorized sub-processors as described in Section 5 of this DPA.

2. **UK Addendum**. If the Processing of Personal Data includes transfers from the United Kingdom to countries that do not offer an adequate level of data protection or which have not been subject to an Adequacy Decision, the Parties shall comply with Article 45(1) of the UK GDPR and Section 17A of the Data Protection Act 2018. The Parties hereby agree to execute the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses as follows:

a) The UK Standard Contractual Clauses (Controller-to-Processor and Processor to Processor) if applicable, will apply with respect to restricted transfers between Customer and Hunters that are subject to the GDPR.
b) The Parties agree that for the purpose of transfer of Personal Data between Customer (as Data Exporter) and Hunters (as Data Importer), the following shall apply: (i) Clause 7 of the Standard Contractual Clauses shall be not applicable; (ii) In Clause 9, option 2 shall apply and the method described in Section 5 of the DPA (Authorization Regarding Sub-Processors) shall apply; (iii) Clause 11 of the Standard Contractual Clauses shall be not applicable; (iv) In Clause 17, option 1 shall apply. The Parties agree that the Standard Contractual Clauses shall be governed by the laws of England and Wales; and (v) In Clause 18(b) the Parties choose the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts in the UK. The Parties agree to submit themselves to the jurisdiction of such courts, as their choice of forum and jurisdiction. Which Parties may end this Addendum as set out in Section 19: Importer and/or Exporter, in accordance with the agreed terms of the DPA.
c) Annex I.A: With respect to Module Two: Data Exporter is Customer as a data controller and the Data Importer is Hunters as a data processor. With respect to Module Three: Data Exporter is Customer as a data processor and the Data Importer is Hunters as a data processor (sub-processor). Data Exporter and Data Importer Contact details: As detailed in the Agreement. Signature and Date: By entering into the Agreement and this DPA, each Party is deemed to have signed these UK Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the DPA.
d) Annex I.B of the UK Standard Contractual Clauses shall be completed as described in Schedule 1 (Details of the Processing) of this DPA.
e) Annex I.C of the UK Standard Contractual Clauses shall be completed as follows: The competent supervisory authority is the ICO supervisory authority.

f) Annex II of the UK Standard Contractual Clauses shall be completed as described in the Security Documentation.
g) Annex III of the UK Standard Contractual Clauses shall be completed with the authorized sub-processors available upon email request to privacy@hunters.ai.

3. **Swiss SCCs.** If the Processing of Personal Data includes transfers from Switzerland to countries outside the EEA which do not offer adequate level of data protection or which have not been subject to an Adequacy Decision, where the FADP applies to Swiss Transfers, the Parties hereby agree to execute the Swiss Standard Contractual Clauses as follows:

a) The Swiss Federal Data Protection and Information Commissioner shall be the sole Supervisory Authority for Swiss Transfers exclusively subject to the FADP;
b) The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the Standard Contractual Clauses shall be interpreted to include the FADP with respect to Swiss Transfers;
c) References to Regulation (EU) 2018/1725 are removed;
d) Swiss Transfers subject to both the FADP and the GDPR, shall be dealt with by the EU Supervisory Authority named above;
e) References to the "Union", "EU" and "member state" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 (c) of these Standard Contractual Clauses.
f) Insofar as the data transfers underlying these Standard Contractual Clauses are exclusively subject to the FADP, references to the GDPR are to be understood as references to the FADP. Insofar as the data transfers underlying these Standard Contractual Clauses are subject to both the FADP and the GDPR, the references to the GDPR are to be understood as references to the FADP insofar as the data transfers are subject to the FADP. Any obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter or Data Subject is established shall refer to an obligation under Swiss Data Protection Laws.

SCHEDULE 3 - TECHNICAL AND ORGANISATIONAL MEASURES

In the event of a conflict between this Schedule and any other agreement that Customer has entered into with Hunters governing information security, technical and organizational measures, the protection of data and/ or privacy, or similar, the provisions more protective of the data, shall prevail.

Measures:	Description:
1. Measures of pseudonymisation and encryption of personal data	Hunters shall maintain encryption in transit and at rest in accordance with sections 5 and 6 below.
2. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Business Continuity Management. Hunters will, establish and maintain (i) business continuity and disaster recovery plans ("Contingency Plans") for critical functions, technology and systems in support of the Services herein to enable recovery of said Services within the agreed upon Recovery Time and Recovery Point objectives in the event of a disaster or other unexpected disruption in Services. (ii) Hunters will review, update and exercise the operability of applicable Contingency Plans in support of the Services herein by conducting recovery exercises of Contingency Plans at least annually.
3. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Hunters shall maintain processes for testing, assessing and evaluating the effectiveness of technical and organizational controls at a minimum on an annual basis. The results of such assessments shall be documented and remediation actions monitored by Hunters management responsible for the information security governance. This may include accreditations to provide independent assurance that Hunters programs, products and services meet industry standards for security.
4. Measures for user identification and authorization	Identification and Authentication. All access to any personal data shall be identified and authenticated. For access to personal data, Hunters shall require authentication by the use of an individual, unique user ID and an individual password and/or other appropriate authentication technique (e.g. soft token, pin, etc.). Hunters shall maintain procedures to ensure the protection, integrity, and soundness of all passwords created by Hunters and/or used by Hunters in connection with the Agreement.
5. Measures for the protection of data during transmission	Encryption in transit. Hunters shall maintain encryption, in accordance with industry standards, for all transmission of Hunters personal data via public networks (e.g., the Internet).
6. Measures for the protection of data during storage	Encryption at rest. Hunters shall maintain encryption, in accordance with industry standards, for all Hunters' personal data stored on any of Hunters storage services.

7. Measures for ensuring physical security of locations	Hunters shall take reasonable measures to (i) prevent unauthorized persons from gaining access to Hunters premises, and (ii) guard against environmental hazards such as heat, fire, and water damage. Office access points are controlled through the requirement of physical badges and access cards to prevent unauthorized entry.
8. **Measures for ensuring events logging**	Vulnerabilities Management. Hunters will establish and maintain vulnerabilities management program to identify, log and remediate vulnerabilities based on industry standards such as ISO 27001.
9. Measures for internal IT and IT security governance and management	- Risk Management. Hunters shall maintain an information security risk management program, with the results being included in the annual mitigation plan, which is presented to and monitored by Hunters Management. - Account Administration. Hunters shall maintain appropriate processes for requesting, approving, and administering accounts and access privileges for Hunters resources and personal data. These processes shall include procedures for granting and revoking emergency access to Hunters' personal data. - Access Control. Hunters shall maintain appropriate access control mechanisms to prevent all access to Hunters personal data. The access and privileges granted shall be limited to the minimum necessary to perform the assigned functions. - Authorized Access. Hunters shall only access Customer's personal data for providing services to Customer. Hunters shall not attempt to access any applications, systems or data which Hunters is not required in order to perform services. - Endpoint protection. Hunters shall ensure that any endpoint, to whom Hunters provides access to Customer's personal data has malware protection installed; in addition, Hunters shall ensure that malware protection cannot be disabled by the end users and has periodic updates of new malware signatures. - Network Security Authorized Access. Hunters shall only access Customer's personal data for providing services to Customer. Hunters shall not attempt to access any applications, systems or data which Hunters is not required in order to perform services.
10. Measures for ensuring data integrity	Hunters shall maintain processes to prevent unauthorized or inappropriate modification of personal data, for both data in transit and data at rest.