Data Processing Agreement for Optro Suppliers

This Data Processing Agreement for Optro Suppliers ("**DPA**") forms part of the Services Agreement regarding Supplier's Services provided to and ordered by Optro in accordance with the Services Agreement. All capitalized terms not defined herein shall have the meaning set forth in the following documents, by order of precedence: (a) the DPA Terms, and (b) the Services Agreement.

APPLICATION OF THIS DPA:

If this DPA is referenced in a Services Agreement between Optro, Inc. or any of its affiliates then this DPA is an addendum to and forms a part of the Services Agreement. In that event, the Optro entity which is a Party to the Services Agreement shall be the Party to this DPA. This DPA is comprised of the following (each of which are incorporated into this DPA by reference): (i) the DPA Terms, including the **Annexes** attached thereto, and (ii) the Standard Contractual Clauses. This DPA is effective as the Effective Date of the Services Agreement of which it is part of.

Optro

DPA Terms

These Data Processing Agreement Terms, including the **Annexes** attached hereto and the Standard Contractual Clauses, (collectively, these **"DPA Terms"**) apply to the Optro entity executing the Services Agreement, which also enters into the DPA on behalf of itself and its Authorized Affiliates ("**Optro**"), and **Supplier** (as identified in the Services Agreement). Optro and Supplier may each be referred to as a "**Party**" and together as the **"Parties**". These DPA Terms form part of and is subject to the Services Agreement regarding Supplier's Services provided to and ordered by Optro in accordance with the Services Agreement.

Recitals

Supplier has entered into one or more purchase orders, contracts and/or agreements (as may be amended from time to time) (the "**Services Agreement**") with Optro and/or its Authorized Affiliates. In delivering the Services, Supplier may Process Personal Data controlled by Optro, an Authorized Affiliate and/or their respective customers, contacts or partners (as more fully defined below as "Optro Personal Data").

As part of its privacy policy and its contractual arrangements, Optro has provided certain assurances to its customers, contacts, partners and/or end-users to ensure the appropriate protection of Optro Personal Data when Optro engages a third-party supplier.

Optro's continued engagement of Supplier in the Processing of Optro Personal Data in connection with the provision of the Services is conditioned upon Supplier's agreement to the terms and conditions of the DPA.

The Parties agree as follows:

1. Definitions

"**Affiliate**" means any entity under the control of a party where **"control"** means ownership of, or the power to vote, directly or indirectly, a majority of any class of voting securities of a corporation or limited liability company, or the ownership of any general partnership interest in any general or limited partnership or as otherwise defined in the Services Agreement to which the DPA relates.

"Authorized Affiliate(s)" means any Optro Affiliate: (i) permitted to use the Services pursuant to the Services Agreement; and/or

a. (ii) that is the Controller (whether acting for itself or acting on behalf of a third-party Controller) of the Optro Personal Data that Supplier accesses or receives under the Services Agreement and the DPA. The signatory or the Optro Authorized Affiliates shall include but shall not be limited to, as applicable: (A) Optro Inc., a Delaware corporation,
b. (B) Optro UK Limited, incorporated under the laws of England and Wales, and (C) Optro Canada Inc., incorporated under the laws of Canada; and their successors and assigns, for so long as they are Optro Affiliates.

"**Authorized Personnel**" means any natural person who Processes Optro Personal Data on Supplier's behalf, including but not limited to Supplier's employees, officers, partners, principals, contractors, and Subprocessors.

"CCPA" means the California Consumer Privacy Act (California Civil Code §§1798.100 et seq.) including any amendments and implementing regulations that become effective on or after the Effective Date of the DPA.

"**Controller**", "**Processor**", "**Process**" (in its various forms), "**Data Subject**", and "**Personal Data**" shall have the meanings given to them in EU/UK Data Protection Law, and the terms "**business**", "**service provider**" and "**sale**" shall have the same meaning given to them under the CCPA.

"**Optro Personal Data**" means any Personal Data, or "personal data", "personal information" or "personally identifiable information" or similar term defined under Data Protection Legislation, provided or made available by or on

behalf of Optro to Supplier and/or collected or otherwise obtained by Supplier in connection with the performance of the Services by Supplier to Optro and Processed by Supplier as a Processor or Controller (as applicable), as more particularly described in **Annex A** attached hereto.

"**Data Protection Legislation**" means any applicable laws relating to data protection and privacy and the Processing of Optro Personal Data that may exist in any relevant jurisdiction, including (but not limited to): (i) the CCPA; (ii) any other current or future applicable U.S. state and/or U.S. federal data protection laws that may be enacted; and (iii) EU/UK Data Protection Law.

"**EU/UK Data Protection Law**" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such Personal Data (General Data Protection Regulation) (the "**GDPR**"); (ii) the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the Swiss Federal Data Protection Act of 19 June 1992 and its corresponding ordinances ("**Swiss DPA**"); (iv) the EU e-Privacy Directive (Directive 2002/58/EC); and (v) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii),(iii) and (iv) above; in each case as may be amended or superseded from time to time.

"**EEA**" means for the purposes of the DPA, the member states of the European Union and European Economic Area, the United Kingdom ("**UK**") and Switzerland.

"**Restricted Transfer**" means: (i) where the GDPR applies, a transfer (directly or via onward transfer) of Optro Personal Data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer (directly or via onward transfer)of Optro Personal Data from the United Kingdom to any other country which is not subject based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer (directly or via onward transfer) of Optro Personal Data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

"**Security Incident**" means any breach of security leading to, or reasonably believed to have led to, the accidental or unlawful destruction, loss, or alteration of, or unauthorized disclosure or access to Optro Personal Data or similar incident involving Optro Personal Data, in each case for which a Controller is required under Data Protection Legislation to provide notice to competent data protection authorities or Data Subjects.

"**Services**" means any product or service provided by Supplier to Optro pursuant to and as more particularly described in the Services Agreement.

"**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission's Implementing Decision 2021/914 of 4 June 2021.

"**Subprocessor**" means any third party that has access to the Optro Personal Data and which is engaged directly or indirectly by Supplier to assist in fulfilling Supplier's obligations with respect to providing the Services pursuant to the Services Agreement or the DPA. Subprocessors may include Supplier's Affiliates but shall exclude Supplier's employees, contractors and consultants who are natural persons.

"**Supplier**" means the entity signing the DPA on behalf of itself and its Affiliates.

"**Term**" means the term of the Services Agreement and any period after the termination or expiry of the Services Agreement during which Supplier and/or its Subprocessors Processes Optro Personal Data, until Supplier has destroyed or returned such Optro Personal Data in accordance with the terms of the DPA.

"**UK Addendum**" means the "UK Addendum to the EU Standard Contractual Clauses" issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018.

2. Scope of these DPA Terms and Relationship of the Parties

a. 2.1 Supplier as a Processor. For the purposes of the GDPR and similar Data Protection Legislation, the Parties agree that Supplier will Process Optro Personal Data as a Processor acting on behalf of Optro (whether a Controller itself or acting on behalf of (a) an Authorized Affiliate or (b) a third-party Controller) and only in accordance with Optro's written instructions, as further described in **Annex A** attached hereto, and these DPA Terms shall apply accordingly.

b. 2.2 California. For the purposes of the CCPA (to the extent the CCPA is applicable), Optro is a "business" and Supplier is a "service provider". Supplier, as service provider, will not: (a) sell Optro Personal Data; (b) retain, use, or disclose the Optro Personal Data for any purposes other than for performing Supplier's obligations under the Services Agreement; c) retain, use, or disclose Personal Data outside the direct business relationship between Optro and Supplier; (d) combine Personal Data with personal information that Supplier has received from another Supplier's customer, except as permitted under the CCPA. Optro will notify Supplier if Optro determines that Supplier can no longer comply with our obligations as a service provider. Optro has the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data that is protected under the CCPA. The Parties agree that Optro's transfer of Optro Personal Data to Supplier is not a sale, and Supplier provides no monetary or other valuable consideration to Optro in exchange for Optro Personal Data. Supplier certifies that it understands the restrictions set out in this Section 2.2 and will comply with them.

c. 2.3 Compliance with Data Protection Legislation. Each Party shall comply with its obligations under Data Protection Legislation with respect to the Processing of Optro Personal Data. Supplier shall not perform its obligations under the Services Agreement or the DPA in such a way as to cause Optro to breach any of its obligations under Data Protection Legislation.

3. Processing Instructions

a. 3.1 Supplier will Process the Optro Personal Data only in accordance with the written instructions from Optro and in compliance with Data Protection Legislation. Such instructions may be specific or of a general nature as set out in the DPA, the Services Agreement, an SOW, or as otherwise notified by Optro to Supplier in writing from time to time.Optro instructs Supplier to Process Optro Personal Data as a Processor for the following purposes: (a) Processing to provide the Services and all other Processing necessary for Supplier to perform its obligations under the Services Agreement and the DPA; (b) processing to comply with any other reasonable instructions provided by Optro (e.g., via email or support tickets) that are consistent with the terms of the Services Agreement and the DPA, (c) processing to comply with Supplier's legal obligations under applicable law, including Data Protection Legislation; and (d) any other purposes expressly authorised by Optro under the terms of the Services Agreement (collectively and individually the "**Permitted Purpose**").

b. 3.2 Supplier shall not Process Optro Personal Data for its own or for any other purposes except (i) as otherwise specified in these DPA Terms or, (ii) to the extent applicable, as required by Union or Member State law to which the Supplier is subject. If (ii) applies, Supplier shall inform Optro of the legal requirement before Processing, unless that law prohibits such information on important grounds of public interest and, where permitted, Supplier shall only Process Optro Personal Data as strictly necessary to comply with such law. Supplier certifies that it understands the restrictions set out in this Section 3.3 and will comply with them.

c. 3.3 Supplier shall make available to Optro all information necessary to demonstrate compliance with the obligations laid down in the DPA. Supplier will inform Optro prior to the Processing of Optro Personal Data unless prohibited by law from doing so if it:

d. becomes aware of or believes that any instruction from Optro violates Data Protection Legislation; and/or

e. is unable to comply with Optro's instructions for any reason.

4. Security

a. 4.1 Supplier represents and warrants that it has implemented and shall maintain appropriate technical and organisational measures to protect the Optro Personal Data against Security Incidents and to preserve the security and confidentiality of Optro Personal Data. These measures shall take into account the current industry standards, state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Without prejudice to the foregoing, such measures shall include, at a minimum, those set out in **Annex C** attached hereto. Supplier may change the measures outlined in **Annex C** attached hereto without notice to Optro so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Optro Personal Data.

b. 4.2 Supplier shall ensure that any person who processes Optro Personal Data on Supplier's behalf: (a) is required to protect and process Optro Personal Data in a manner consistent with the terms of the Services Agreement and the DPA; and (b) will receive appropriate training by Supplier regarding the protection of Optro Personal Data prior to receiving access to Optro Personal Data.

c. 4.3 Supplier will take reasonable steps to ensure the reliability and competence of any of its and its Subprocessors' Authorized Personnel, including regular training of those with access to Optro Personal Data in applicable security and data privacy measures. Supplier will ensure that all such Authorized Personnel are subject to a strict contractual or statutory duty of confidentiality and that they Process the Optro Personal Data only for the purpose of delivering the Services to Optro in accordance with the DPA.

5. Subprocessing

a. 5.1 Supplier will not give access to or transfer any Optro Personal Data to any third party (including any of Supplier's Affiliates, group companies or Subprocessors) without the prior written consent of Optro. Notwithstanding the foregoing, Optro does consent to Supplier engaging a Subprocessor to Process Optro Personal Data provided that:

b. Supplier provides at least 30 days' prior written notice to Optro of the engagement of any new Subprocessor (including details of the Processing and location) and Supplier shall update the list of all Subprocessors engaged to Process Optro Personal Data under the DPA at **Annex B** attached hereto and send such updated version to Optro prior to the engagement of the Subprocessor;

c. Supplier must ensure the reliability and competence of such Subprocessor, and of its Authorized Personnel who may have access to Optro Personal Data;

d. Supplier imposes in its contract with such Subprocessor provisions which are substantially the same as those in the DPA and the Services Agreement and as are required by Data Protection Legislation; and

e. Supplier will remain fully liable to Optro for any breach of the DPA and the Services Agreement caused by an act, error or omission of such Subprocessor including but not limited to their Authorized Personnel. If Optro objects to the engagement of any Subprocessor on data protection grounds, then either Supplier will not engage the Subprocessor to Process Optro Personal Data or Optro may elect to immediately suspend or terminate the Processing of Optro Personal Data under the Services Agreement and/or immediately suspend or terminate the Services Agreement, in each case without penalty.

6. Cooperation

a. 6.1 Supplier will take all reasonable steps to assist Optro in meeting Optro's (or its Authorized Affiliate's) obligations under Data Protection Legislation, including but not limited to Optro's obligations (a) to respond

to requests by Data Subjects to exercise their rights with respect to Optro Personal Data (including its right of access, correction, objection, erasure/deletion and data portability, as applicable), (b) to adhere to data security obligations, and (c) to consult with supervisory authorities.

b. 6.2 Supplier will promptly inform Optro in writing if it receives: (a) a request from a Data Subject concerning any Optro Personal Data; or (b) a complaint, communication, or request relating to Optro's obligations under Data Protection Legislation. Supplier shall not respond to such communication without Optro's express authorization.

c. 6.3 Supplier will provide all reasonable assistance required by Optro (or its Authorized Affiliate) to conduct a data protection impact assessment and, where legally required, consult with applicable supervisory authorities.

d. 6.4 If Supplier receives a subpoena, court order, warrant or other legal demand from a third party (including law enforcement or other governmental, regulatory or judicial authorities) seeking the disclosure of Optro Personal Data, Supplier shall not disclose any information but shall immediately notify Optro in writing of such request, and reasonably cooperate with Optro if Optro wishes to limit, challenge or protect against such disclosure, to the extent permitted by applicable laws.

7. Delete or return

a. 7.1 Supplier will not retain any Optro Personal Data for longer than is necessary to provide the Services. At the end of the Services, or upon Optro's request, Supplier will securely destroy or return to Optro (at Optro's election) the Optro Personal Data in Supplier's possession or control (including any Optro Personal Data Processed by its Subprocessors).

b. 7.2 This requirement shall not apply to the extent that Supplier is required by any applicable law to retain some or all of the Optro Personal Data, in which case Supplier shall isolate and protect the Optro Personal Data from any further Processing except to the extent required by such law. Supplier shall delete such retained data without undue delay when technically feasible and/or allowed by the applicable law.

8. Data Transfers

a. 8.1 International data transfers. Supplier shall be entitled to Process and transfer the Optro Personal Data, including by using Subprocessors, in or to a territory other than the territory in which the Optro Personal Data was first collected as permitted by and in compliance with Data Protection Legislation and the DPA.

b. 8.2 Restricted Transfers. Supplier shall not conduct a Restricted Transfer of Optro Personal Data unless it first takes all such measures as are necessary to ensure the Restricted Transfer is in compliance with EU/UK Data Protection Law. Such measures may include (without limitation) transferring Optro Personal Data to a recipient that: (a) is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for personal data; (b) has achieved binding corporate rules authorization; or (c) has executed with Supplier appropriate Standard Contractual Clauses, including the adoption of supplementary measures, if required to ensure an adequate level of protection; in each case as adopted or approved in accordance with applicable EU/UK Data Protection Law.

c. 8.3 The Parties agree that where Optro transfers (directly or via onward transfer) Optro Personal Data to Supplier, the Parties agree to be subject to the Standard Contractual Clauses, which shall be incorporated by reference as form an integral part of these DPA Terms, as follows:

d. Supplier as a Processor. In relation to Optro Personal Data that is protected by the EU GDPR and is Processed in accordance with Section 2.1 of these DPA Terms, the SCCs shall apply completed as follows: (i) Module Two will apply; (ii) in Clause 7, the optional docking clause will apply, (iii) in Clause 9, Option 2 will

apply, and the time period for prior notice of sub-processor changes shall be as set out in Section 5 (Subprocessing) of these DPA Terms; (iv) in Clause 11, the optional language will not apply; (v) in Clause 17, Option 1 will apply, and the SCCs will be governed by the law of the Ireland; (vi) in Clause 18(b), disputes shall be resolved before the courts of the Ireland; (vii) Annex I of the SCCs shall be deemed completed with the information set out in **Annex A** attached hereto; and (viii) subject to Section 4.1 of these DPA Terms, Annex II of the SCCs shall be deemed completed with the information set out in **Annex C** attached hereto.

e. UK Transfer Mechanism. For the purposes of Optro Personal Data that is subject to the UK GDPR ("**UK Data**"), the SCCs as implemented under sub-paragraphs (a) and (b) above will also apply with the following modifications:

   i. the SCCs shall be deemed amended as specified by Part 2 of the UK Addendum;

   ii. tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed respectively with the information set out in **Annexes A**, **B** and **C** attached hereto (as applicable); and

   iii. table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party".

f. Swiss Transfer Mechanism. For the purposes of Optro Personal Data that is subject to the Swiss DPA ("**Swiss Data**"), the SCCs as implemented under sub-paragraphs (a) and (b) above will also apply with the following modifications:

   i. references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;

   ii. references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the Swiss DPA;

   iii. references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" or "Swiss law";

   iv. the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (i.e., Switzerland);

   v. Clause 13(a) and Part C of Annex I are not used and the "competent supervisory authority" is the Swiss Federal Data Protection Information Commissioner;

   vi. references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland";

   vii. in Clause 17, the SCCs shall be governed by the laws of Switzerland; and

   viii. Clause 18(b) shall state that disputes shall be resolved before the applicable courts of Switzerland.

g. 8.4 In addition, Supplier agrees to implement and maintain any additional contractual, technical or organisational measures to supplement the safeguards under the SCCs which are required from time to time by Optro in order to protect the Optro Personal Data, so long as such safeguards are consistent with requirements under Data Protection Legislation. If Supplier is unable to implement and maintain such supplementary measures, Optro may immediately terminate the Services Agreement and the DPA (in whole or in part) without penalty. Supplier shall promptly notify Optro if it makes a determination that it can no longer meet its obligations under this Section 8, and in such event but without prejudice to any other right or remedy available to Optro, Supplier shall:

h. remediate (if remediable) any Processing until such time as the Processing meets the level of protection as is required by Data Protection Legislation and this Section 8; and/or

i. immediately cease (and require that all Subprocessors immediately cease) Processing such Optro Personal Data if in Optro's sole discretion, Optro determines that Supplier has not or cannot correct any non-compliance with this Section 8 within a reasonable time frame.

j. 8.5 It is not the intention of either Party, nor the effect of the DPA, to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses. Accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the DPA, the Standard Contractual Clauses shall prevail. In no event does the DPA restrict or limit the rights of any Data Subject or of any competent supervisory authority.

k. 8.6 The Parties agree that in the event that a supervisory authority and/or EU/UK Data Protection Law no longer allow the lawful transfer of Optro Personal Data to Supplier and/or requires that Optro adopt an alternative transfer solution that complies with EU/UK Data Protection Law, Supplier will fully co-operate with Optro to enter into an amendment to these DPA Terms to remedy such non-compliance and/or cease Processing of Optro Personal Data. If the Parties, acting in good faith, are unable to agree such changes within thirty (30) days, Optro may immediately terminate the Services Agreement without any further liability or obligation to Supplier, and Supplier shall refund to Optro any amounts which were paid for work not yet performed under the Services Agreement.

9. Security Reports and Inspections

a. Supplier shall maintain records in accordance with ISO 27001 or similar information security management system standards. On request, Supplier shall provide copies of relevant reports, certifications or any information reasonably requested by Optro to demonstrate compliance with the obligations set out in the DPA. Supplier shall also respond to Optro security questionnaires and address any reasonable follow up questions.
b. While it is the Parties' intention ordinarily to rely on Section 9.1 above to demonstrate Supplier's compliance with the DPA (including the Standard Contractual Clauses as applicable) and Data Protection Legislation, where Optro has reasonable concerns about Supplier's compliance, Supplier will allow Optro or an Authorized Affiliate under the DPA and their respective auditors or authorized agents to conduct audits and inspections during the term of the Services Agreement and for 12 months thereafter. Such inspections shall include, where necessary, providing access to the premises, resources and Authorized Personnel, and provide all reasonable assistance in order to assist Optro or an Authorized Affiliate under the DPA in exercising its audit rights under this Section 9.2. Inspections may only be carried out with reasonable prior notice, during normal business hours.

10. Security Incidents

a. If Supplier becomes aware of any Security Incident, it shall:

b. without undue delay (and in any event no later than 48 hours of discovery) notify Optro and provide Optro with: a detailed description of the Security Incident; the type of data that was the subject of the Security Incident; the identity of each affected Data Subjects (if determinable), and the steps Supplier has taken or intends to take in order to mitigate and remediate such Security Incident, in each case as soon as such information can be collected or otherwise becomes available (as well as periodic updates to this information and any other information Optro may reasonably request relating to the Security Incident);

c. take action immediately, at its own expense, to investigate the Security Incident and to identify, prevent and mitigate the effects of the Security Incident and, with the prior written approval of Optro, to carry out any recovery or other action necessary to remedy the Security Incident;

d. reimburse Optro for reasonable costs incurred by Optro (or an Authorized Affiliate) to draft, prepare,

generate, and send, or otherwise related to, all notifications as required by Data Protection Legislation and, if requested by Optro, provide credit monitoring and identity theft protection services to affected Data Subjects; and

e. not release or publish any filing, communication, notice, press release, or report concerning the Security Incident without Optro's prior written approval (except where it is required to do so by law).

11. Liability and Indemnity

a. Notwithstanding anything else to the contrary in the Services Agreement, Supplier agrees that:

b. it shall be liable for any unauthorized use, exposure or loss of data (including Optro Personal Data) arising under or in connection with the Services Agreement and the DPA to the extent such loss results from any failure of Supplier (or its Subprocessors) to comply with its obligations under the DPA and/or applicable law or regulation; and

c. any exclusion of damages or limitation of liability that may apply to limit Supplier's liability in the Services Agreement shall not apply to Supplier's liability arising under or in connection with the DPA, howsoever caused, regardless of how such amounts or sanctions awarded are characterized and regardless of the theory of liability, which liability shall be expressly excluded from any agreed exclusion of damages or limitation of liability.

d. To the fullest extent permitted by applicable law, Supplier shall indemnify, defend, and hold Optro, including its Authorized Affiliates, and each of its affiliates, partners, principals, officers, directors, employees, subcontractors and agents harmless against any claims, suits, or proceedings and any resulting liabilities, fines, losses, damages, costs and expenses (including reasonable attorney's fees) that Optro may suffer or incur as a result of any act or omission on the part of Supplier or its subcontractors, or anyone acting on their behalf, that leads to Optro being liable for breach of Data Protection Legislation or a third-party contract.

e. For the avoidance of doubt, nothing in the DPA is intended to limit any Data Subject rights, as third-party beneficiaries, under the Standard Contractual Clauses against any Party arising out of such Party's breach of the Standard Contractual Clauses, where applicable.

12. Documentation and Records of Processing

a. Each Party is responsible for its compliance with its documentation requirements, in particular maintaining records of Processing, where required under Data Protection Legislation. Each Party shall reasonably assist the other Party in its documentation requirements, including providing the information the other Party needs from it in a manner reasonably requested by the other Party (such as using an electronic system) in order to enable the other Party to comply with any obligations relating to maintaining records of Processing.

13. General

a. The DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Services Agreement, unless and to the extent required otherwise by the Data Protection Legislation or, where applicable, the Standard Contractual Clauses.

b. The Parties acknowledge and agree that the DPA is incorporated into and forms a part of the Services Agreement between Optro and Supplier. For matters not addressed under the DPA, the terms of the Services Agreement apply. If and to the extent the DPA conflicts with any provision of the Services Agreement, the DPA shall control and prevail. Conflicts between the terms of the DPA and the Standard Contractual Clauses are addressed in Section 8.5 above, as further subject to Section 8.6 above.

c. The Parties acknowledge and agree that any breach by Supplier of the DPA shall constitute a material breach of the Services Agreement, in which event and without prejudice to any other right or remedy available to it, Optro may elect to immediately terminate the Services Agreement (in whole or in part) in

accordance with the termination provisions in the Services Agreement.

d. The DPA shall take effect on the Effective Date and will continue to be in effect for the Term.

Optro

Annex A
Description of the Processing Activities / Transfer

CONTROLLER TO PROCESSOR TRANSFER (MODULE TWO)

Annex 1(A) List of Parties:

Data Exporter	**Data Importer**
Name: The Optro entity executing the Services Agreement and the DPA	**Name:** Supplier as this term is defined in the Services Agreement
Address: As identified in the Services Agreement	**Address:** As identified in the Services Agreement
Contact Person's Name, position and contact details: privacy@optro.ai	**Contact Person's Name, position and contact details:** As identified in the Services Agreement
Activities relevant to the transfer: See **Annex 1(B)** below	**Activities relevant to the transfer:** See **Annex 1(B)** below
Role: Controller	**Role:** Processor

Annex 1(B) Description of transfer:

	Description
Categories of data subjects:	Employees or contact persons of Optro
Categories of personal data:	Any combination of the following: Name and contact information (including work address; work telephone numbers; mobile telephone numbers; web address; IP addresses; instant messenger; work email address); business title; company, Name and contact information (including work address; work telephone numbers; mobile telephone numbers; web address; IP addresses; instant messenger; work email address); business title; company
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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	As applicable, the transferred Personal Data may comprise special categories of personal data, such as ethnicity, religious beliefs, trade union membership information and health data (employee sick leave, disability information). Taking into consideration the nature of the data and the risk of varying likelihood and severity for the rights and freedoms of natural persons, Vendor has implemented the technical and organizational measures, including specialized training of staff and system access logs, to ensure an appropriate level of protection for such sensitive data.
Frequency of the transfer:	Transfers will be made on a continuous basis.
Nature of the Processing:	The performance of the Services under the Services Agreement and the DPA. The nature and purposes of the processing is the collection, storage, duplication, deletion, and disclosure of Personal Data pursuant to providing the Services to Customer
Duration of the Processing:	The term of the Services Agreement and any period after the termination or expiry of the Services Agreement during which Supplier Processes Optro Personal Data, until Supplier has deleted, destroyed or returned such Personal Data in accordance with the terms of the DPA (the "**Processing Term**").

Purpose(s) of the data transfer and further Processing:	The Permitted Purpose (as defined in the DPA Terms) and the general purpose of the Services as defined in the Services Agreement
Retention period (or, if not possible to determine, the criteria used to determine that period):	The Processing Term
For transfers to Subprocessors, also specify subject matter, nature and duration of the Processing:	The nature is the provision of the Services as described in the Services Agreement. The subject matter is the personal data as described above. The duration will be as specified above.

Annex 1(C) Competent supervisory authority:
The competent supervisory authority, in accordance with Clause 13 of the SCCs, shall be determined in accordance with EU/UK Data Protection Law.

Annex B
List of Supplier Subprocessors

Vendor shall provide a copy of their current list of subprocessors upon execution of the Services Agreement to privacy@optro.ai within 30 days of executing the Services Agreement. Optro shall have the right to opt-out of any services should Optro have a valid objection that cannot be remediated 30 days following delivery of Vendor's updated subprocessors list via email. The Subprocessors Processing Optro Personal Data controlled by Optro, Optro Affiliates, partners of Optro and/or of the Optro Affiliates, and/or customers of any of the Subprocessors listed within the applicable Vendor's subprocessor's list shall be considered approved Subprocessors under the DPA after the 30 day objection window has passed. Supplier shall maintain a list of Subprocessors in accordance with the DPA which will be shared by Vendor upon request from Optro or Vendor shall provide Optro with a mechanism to obtain notice of updates and new Subprocessors.

Annex C
Technical and organizational measures

The technical and organizational measures implemented by Supplier (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purposes of the Processing, and the risks for the rights and freedoms of natural persons, are as follows:

Vendor maintains documented policies and procedures that include appropriate administrative, physical, technical and organizational measures designed to: (i) protect the security, confidentiality, availability and integrity of any Optro data; (ii) protect against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of Optro data: (iii) protect against threats or hazards to the security, confidentiality, availability and integrity of Optro data; and (iv) comply with Applicable Data Protection Laws by which Vendor may be regulated. Vendor shall regularly monitor, evaluate and assess the effectiveness of the administrative, physical, technical and organizational measures implemented.

Vendor's administrative, physical, organizational and technical measures shall include, at a minimum, the following:

ACCESS TO OPTRO DATA. Access controls to manage access to Optro data and system functionality, unique IDs and passwords, strong (i.e., two-factor) authentication for remote access systems, and promptly revoking or changing access in response to terminations or changes in job functions. Vendor shall prevent disclosure or dissemination of Optro data to any person not having a need to know of or access to such information. Access to Optro data must therefore respect the "need to know" and "least privilege" principles: access can only be granted to persons whose function justifies it, for a specific purpose and their privileges are restricted to the strict minimum necessary to perform their duties.

Vendor shall implement and maintain controls to ensure the proper segregation of systems and data and make sure Optro data and/or systems are properly isolated.

ACCESS CONTROL TO SYSTEMS; PASSWORD MANAGEMENT. Unauthorized access to information technology systems must be prevented, including through the use of technical and administrative measures for user identification and authentication. Vendor shall ensure appropriate password hardening standards are in place that align with accepted industry security frameworks to ensure sufficient controls, including use of passwords with sufficient length.

PHYSICAL SECURITY. Vendor shall provide technical and organizational measures to control access to premise and facilities and prevent unauthorized access. Controls are in place to protect Vendor's information technology infrastructure from environmental hazards, to manage and monitor employees into and out of Vendor's facilities where Optro data is processed, and to otherwise prevent unauthorized individuals from gaining physical access to premises, buildings or rooms where systems that process Optro data.

NETWORK SECURITY. Network security controls shall include the use of firewalls, layered DMZs, and updated Intrusion Detection and/or Prevention Systems to help protect systems from intrusion or limit the scope or success of any attack or attempt of unauthorized access.

VULNERABILITY AND PATCH MANAGEMENT. Vulnerability management procedures and technologies shall be used to identify and mitigate against security vulnerabilities. Vendor shall ensure that application system and network device vulnerabilities are evaluated and security patches are applied in a timely manner. Vendor shall also conduct periodic penetration testing of Internet facing applications and shall use a risk based approach to determine the timing for remediation of the vulnerabilities. Vendor shall remediate or mitigate critical or high risk vulnerabilities discovered under this Section promptly.

POLICY REVIEW. Vendor shall review its security requirements under this DPA at least annually and provide change management procedures to ensure all modifications to Vendor's technology and information assets are tested, approved, recorded and monitored as needed.

ADMINISTRATIVE/ORGANIZATIONAL MANAGEMENT. Organizational management shall ensure the proper development and maintenance of information security and technology policies, procedures and standards, including

these security terms.

INPUT (DATA INTEGRITY); AUDITING, LOGGING. Vendor shall retain information system log records to the extent needed to enable monitoring and reporting of unauthorized information system activity, including account logon events, account management, security events, policy change, privileged functions and administrator account creation/deletion. Vendor shall conduct regular reviews for indications of inappropriate or unusual activity, and Vendor shall protect log records from unauthorized access, unauthorized release, loss, modification, falsification, and deletion. This includes making sure it is possible to examine and establish whether, and by whom, Optro data have been entered, modified or removed from its information technology assets and infrastructure.

CONTINGENCY PLANNING. Vendor maintains policies and procedures for responding to a disaster or business continuity issue, that damages or makes unavailable Optro data or systems that contain Optro data, including a data backup plan and a disaster recovery plan.

JOB CONTROL. Processing of Optro data occurs only as permitted by Agreement. This includes implementing appropriate security and integrity procedures, such as (i) requiring Vendor employees, representatives and other personnel to sign terms and conditions requiring confidentiality and information security responsibilities, including requirements to protect Optro.data and compliance with the Agreement and with applicable laws (including Applicable Data Protection Laws), and (ii) providing appropriate privacy and information security training to such Vendor's personnel.

SECURE DESTRUCTION AND DISPOSAL. Developing, implementing and maintaining appropriate measures designed to destroy or otherwise properly sanitize Optro data prior to disposal, including release of technology infrastructure and assets used to process Optro data out of organizational control, or release of such systems for reuse. Proper destruction or sanitization methods include compliance with NIST-developed guidelines for media sanitization, to ensure that third parties cannot obtain Optro data in hardcopy form and Optro data in digital form is not recoverable by any known forensic means.

DISCLOSURE (TRANSMISSION) CONTROL; ENCRYPTION. Vendor shall encrypt all Optro data in transit and at rest using industry standard encryption protocols.

AVAILABILITY CONTROL; BUSINESS CONTINUITY; TRANSITION OF SERVICES; DATA PORTABILITY. Optro data is protected against accidental destruction or loss (including any requirements specified in Services Agreement). Comprehensive data assurance mechanisms are employed including backups, data redundancy, environmental controls (e.g., fire and smoke detectors, fire suppression and secure facilities) and the implementation, maintenance and regular testing of disaster recovery plans.