Darktrace Supplier Data Processing Addendum

Between:

(1) **Darktrace Holdings Limited** or the applicable Darktrace Affiliate identified in the applicable purchase order or Order Form ("**Darktrace**"); and

(2) The supplier identified in the applicable purchase order or Order Form ("**Supplier**"),

each a "**Party**" and together the "**Parties**".

BACKGROUND

(A) The Parties have entered into Darktrace Standard Supplier Terms and one or more purchase orders or Order Forms (together, the "**Agreement**") under which the Supplier provides goods, software, services or deliverables (the "**Offering**") to Darktrace.

(B) In the course of providing the Offering, the Supplier may Process Personal Data on behalf of Darktrace.

(C) The Parties wish to establish the terms governing the Processing of Personal Data by the Supplier to ensure compliance with Data Protection Laws.

(D) This Data Processing Addendum ("**DPA**") supplements and forms part of the Agreement. In the event of any conflict between this DPA and the Agreement, this DPA shall prevail in respect of the Processing of Personal Data.

1. DEFINITIONS

Unless otherwise defined in the Agreement, all capitalized terms in this Supplier Data Processing Addendum ("**DPA**"), shall have the following meanings:

"**Cloud Provider**" means Microsoft Azure, Amazon Web Services, Google Cloud Platform or an alternative cloud provider agreed in writing between the Parties with security measures materially similar to those specified in Clause 5.1;

"**Controller**" has the meaning given to it in the GDPR Laws;

"**Data Protection Impact Assessment**" has the meaning given to it in the GDPR Laws;

"**Data Protection Laws**" means all data protection and privacy laws, including guidance issued by any applicable data protection authority, applicable to any Personal Data, as may be amended or replaced from time to time, including without limitation (and, to the extent of any inconsistency with the definition of "Data Protection Laws" in the Supplier Terms, this definition shall prevail for the purposes of this DPA):

(a) in the European Union, the General Data Protection Regulation 2016/679 (the "EU GDPR") and the Privacy and Electronic Communications Directive 2002/58/EC (as the same may be superseded by the Regulation on Privacy and Electronic Communications);

(b) in the UK, the UK General Data Protection Regulation 2016/679, as implemented by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 (the "UK GDPR"), the Data Protection Act 2018, and the Privacy and Electronic Communications (EC Directive) Regulations 2003; and

(c) in the United States of America the California Consumer Privacy Act, as amended, or any similar state or federal legislation surrounding data protection and privacy rights for consumers apply.

"**Data Subject**" has the meaning given to it in the GDPR Laws;

"**Documented Instructions**" has the meaning given to it in Clause 3 of this DPA;

"**EEA**" means the European Economic Area;

"**EU Controller-to-Controller Clauses**" means the standard contractual clauses between controllers for data transfers to Third Countries, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021;

"**EU Controller-to-Processor Clauses**" means the standard contractual clauses between controllers and processors for data transfers to Third Countries, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021;

"**EU Processor-to-Processor Clauses**" means the standard contractual clauses between processors for data transfers to Third Countries, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021;

"**GDPR Laws**" means the EU GDPR and the UK GDPR collectively;

"**International Data Transfer Addendum**" or "**IDTA**" means the International Data Transfer Addendum to the EU Processor-to-Processor Clauses, EU Controller-to-Processor Clauses and EU Controller to Controller Clauses as approved by the Information Commissioner's Office of the United Kingdom under section 119A(1) of the Data Protection Act 2018;

"**Personal Data**" has the meaning given to it in the GDPR Laws;

"**Personal Data Breach**" means any breach of security or other action or inaction leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data by Supplier, its affiliates, sub-processors, or any other identified or unidentified third party;

"**Processor**" has the meaning given to it in the GDPR Laws;

"**Protected Data**" means the Personal Data that is Processed by the Supplier on behalf of Darktrace in connection with the Offering under the Agreement;

"**Restricted Transfers**" means a transfer of Protected Data to a Third Country which is not subject to an adequacy decision by the European Commission (in respect of EEA data) or the relevant authority under UK Data Protection Laws (in respect of UK data);

"**Standard Contractual Clauses**" means the EU Processor-to-Processor Clauses, EU Controller-to-Processor Clauses, EU Controller-to-Controller Clauses and the International Data Transfer Addendum;

"**Supervisory Authority**" has the meaning given to it in the GDPR Laws;

"**Third Country**" means in respect of Personal Data originating in the:

(a) EEA, a country outside of the EEA not recognized by the European Commission as providing an adequate level of protection for Personal Data (as described in the EU GDPR); and

(b) UK, a country outside the UK not recognized by the Information Commissioner's Office as providing an adequate level of protection for Personal Data (as described in the UK GDPR).

2. SCOPE AND APPLICATION

2.1 This DPA applies when the Supplier Processes Protected Data under the Agreement. The Parties agree and acknowledge that for the purpose of the Data Protection Laws:

(c) Darktrace is a Controller of Protected Data;
(d) Supplier is a Controller or Processor, as applicable, of Protected Data;
(e) Darktrace retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Laws, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the Supplier;
(f) each party agrees that it will comply with all Data Protection Laws in exercising its rights and performing its obligations under this Agreement, as such laws apply to a Controller and Processor respectively.
(g) Annex A describes the Categories of Personal Data, Categories of Data Subjects, Nature and Purpose of the Processing and the Duration and Frequency of Processing in respect of which the Supplier may process the Personal Data.

3. INSTRUCTIONS

3.1 The Parties agree that this DPA and the Agreement (including any instructions provided by Darktrace to Supplier required for or related to the performance of the Offering) constitute Darktrace's documented instructions regarding Supplier's processing of Protected Data ("**Documented Instructions**").

3.2 The Supplier will only process Protected Data in accordance with Documented Instructions unless required to do so by applicable law, in which case Supplier will, to the extent legally permissible, inform Darktrace of that legal requirement before processing. The Supplier shall promptly inform Darktrace if, in Supplier's opinion, an instruction from Darktrace infringes the Data Protection Laws.

3.3 If Darktrace's Documented Instructions require the Supplier to perform actions that go beyond its obligations under this DPA or the scope of the Offering set out in the Agreement, the Supplier shall inform Darktrace and require Darktrace to provide different Documented Instructions, the carrying out of which will fall within the scope of the Offering or within the scope of the Supplier's obligations under this DPA.

4. CONFIDENTIALITY

4.1 The Supplier will take reasonable steps to ensure the reliability of any persons authorized to process any Protected Data and shall ensure that all such persons have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. SECURITY

5.1 Considering the nature, scope, context and purposes of Processing, The Supplier confirms that it has implemented and will maintain for the term of the Agreement, administrative, physical, technical and organizational measures (as further detailed in Annex B, where applicable), to protect any Protected Data accessed or processed by it against unauthorized or unlawful Processing or accidental loss, destruction, damage or disclosure including but not limited to the security measures, including as appropriate:
(a) the pseudonymisation and encryption of Personal Data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
(c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
(d) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

5.2 The Parties agree that for the purposes of Processing Protected Data under this DPA and the Agreement, the measures contained in Clause 5.1 (as further detailed in Annex B, where applicable) are appropriate, given the nature of the data to be Processed and the harm that might result from such unauthorised or unlawful Processing or accidental loss, destruction, disclosure, access or damage.

5.3 The Supplier must ensure the security measures comply with the requirements of the then-current versions of ISO 27001 and (where applicable) ISO 27018, or an equivalent security control standard. Suppliers will ensure that they maintain the aforementioned measures and standards (or equivalent) for the duration of the Agreement.

6. SUB-PROCESSING

6.1 Save as set out in Clause 6.2, the Supplier shall not without the prior written consent of Darktrace, engage any sub-processors for the Processing of Protected Data under the Agreement.

6.2 Darktrace consents to and authorizes the sub-processors set out in Annex A, to act as sub-processors for the Supplier in the provision of the Offering and on terms materially equivalent to those contained in this DPA. The Supplier shall be fully liable for any breach by the sub- processors of any of the obligations contained in this DPA.

6.3 The Supplier will only appoint new sub-processors pursuant to Article 28(2) of the EU GDPR. The Supplier must notify Darktrace before authorizing any new sub-processors to Process Protected Data in connection with the provision of the Offering. Darktrace may object to the appointment of any new sub-processors within thirty (30) days after notification of such appointment by Supplier. Should Darktrace object to a new sub-processor, upon prior written notice, the Supplier will make available to Darktrace a change in the Offering provided that there is no material change in the scope of the Offering under the Agreement or recommend a commercially reasonable change to Darktrace's use of the Offering to avoid the Processing of Protected Data by the objected sub-processor.

6.4 Subject to Clause 6.3, if the Supplier is unable to make available such change(s) within a reasonable time period, which shall not exceed thirty (30) days, Darktrace may terminate the Agreement. The Supplier shall refund Darktrace all pre-paid, unused fees as at the date of termination in such event.

7. CROSS-BORDER TRANSFERS

7.1 Save as otherwise set out in this Clause 7, if Protected Data originates in the EEA or the UK, the Supplier will not transfer such Protected Data to a Third Country, without the prior written consent of Darktrace and not without procuring provision of adequate safeguards (as defined by relevant Authority from time to time) in accordance with applicable Data Protection Laws.

7.2 Where applicable, Protected Data may be hosted by the agreed Cloud Provider in the hosted location agreed by the Parties. The Suppliershallonly Process Protected Data outside of the EEA and UK if it has given Darktrace reasonable notice thereof, or in any case, at least twenty-four (24) hours' notice.

7.3 Any Processing of Protected Data outside of the EEA and UK shall be solely and to the extent necessary for the Supplier to provide the Offering and for which purposes the relevant Standard Contractual Clauses shall apply as follows:

(a) Module One will apply (where Darktrace or Supplier, as applicable is the Controller of Protected Data), Module Two will apply (where Darktrace is the Controller of Protected Data), otherwise Module Three will apply (where Darktrace is a Processor of Protected Data), as appropriate;
(b) in Clause 7, the optional docking clause will apply;
(c) 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 6 of this DPA;
(d) in Clause 11, the optional language will not apply;
(e) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the laws of Ireland;
(f) in Clause 18(b), disputes shall be resolved before the courts of Ireland;
(g) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex A to this DPA;
(h) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex B to this DPA.

7.4 In relation to Restricted Transfers of Protected Data protected by UK GDPR, the UK IDTA will apply completed as follows:
(a) the IDTA will apply the EU SCCs to Restricted Transfers of Protected Data from the UK;
(b) Tables 1 – 3 of the UK IDTA shall be deemed completed with the relevant information set out in this DPA and the EU SCCs;
(c) Table 1 of the UK IDTA shall be deemed signed by Darktrace and Supplier upon the entry into force of this DPA, and the start date specified in Table 1 of the UK DPA shall be deemed completed with the date of entry into force of this DPA;
(d) In Table 4, the option "Importer" shall be deemed selected.

7.5 In relation to Protected Data that is protected by the EU Data Protection Laws of Switzerland, then the EU SCCs will apply with the following modifications: the competent supervisory authority in Annex 1.C under Clause 13 will be the Federal Data Protection and Information Commissioner; references to a "Member State" and "EU Member State" will not be read to prevent data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland); and references to "GDPR" in the EU SCCs will be understood as references to EU Data Protection Laws of Switzerland.

7.6 In the event that any provision of this DPA contradicts the SCCs (directly or indirectly), the SCCs shall prevail.

7.7 The Parties agree that, in the event where Data Protection Laws no longer allow the lawful transfer of Protected Data to the Supplier and/or require an alternative transfer solution that complies with Data Protection Laws, the Supplier will make an amendment to this DPA available to Darktrace to remedy such non-compliance and/or cease Processing of Protected Data without penalty.

8. DATA SUBJECT REQUESTS AND ASSISTANCE

8.1 The Supplier shall use reasonable efforts to promptly notify Darktrace if it receives:

(a) a request from a Data Subject to have access to that person's Personal Data;
(b) a complaint or request relating to Darktrace's obligations under the Data Protection Laws; or
(c) any other communication relating directly or indirectly to the processing of any Personal Data in connection with the Agreement.

8.2 Considering the nature of Processing and the information available to the Supplier, the Supplier will provide reasonable support to Darktrace in:

(a) complying with any legally mandated request for access to or correction of any Personal Data by a data subject under Chapter III of each of the GDPR Laws (and where such request is submitted to Supplier, Supplier will promptly notify Darktrace of it);
(b) responding to requests or demands made to Darktrace by any court or governmental authority responsible for enforcing the Data Protection Laws; and
(c) in its preparation of a Data Protection Impact Assessment and, where required, in any prior consultation with a Supervisory Authority under the Data Protection Laws.

9. PERSONAL DATA BREACH

9.1 In the event that the Supplier suffers or becomes aware of a Personal Data Breach, it will inform Darktrace without undue delay, and in any event within forty-eight (48) hours of becoming aware of the same and will take reasonable steps to mitigate the effects and to minimise any damages resulting from such breach.

9.2 In the event of a Personal Data Breach, the Supplier (to the extent reasonably possible) will provide the following information to Darktrace:

(a) a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;
(b) the name and contact details of the relevant Processor's data protection officer or another contact point where more information can be obtained;
(c) a description of the likely consequences of the incident; and
(d) a description of the measures taken and / or proposed to be taken by the relevant Processor to address the incident including, where appropriate, measures to mitigate possible adverse effects.

9.3 To the extent that Darktrace is required to notify affected Data Subjects of a Personal Data Breach under the Data Protection Laws, the Supplier shall provide Darktrace with such reasonable assistance as Darktrace may require to prepare and deliver such notifications.

10. AUDIT

10.1 At least once a year, the Supplier will conduct audits of its Personal Data processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this Agreement, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognised third-party audit firm based on recognised industry best practices.

10.2 On Darktrace's written request, the Supplier will make all of the relevant audit reports available to Darktrace for review, including as applicable any information reasonably requested by Darktrace concerning the Supplier's Processing of Protected Data under the Agreement and this DPA and a copy of the current ISO 27001 (ISO/IEC 27001:2013) and (where applicable) ISO 27018 (ISO/IEC 27018:2019) or equivalent certifications.

10.3 The Supplier will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by the Supplier's management.

10.4 Other than in the context of investigating a Personal Data Breach involving Protected Data, Darktrace will first exercise any right it may have to conduct an audit or inspection under Data Protection Laws (or the Standard Contractual Clauses, if applicable) by requesting the information outlined in Clause 10.2. If such information is insufficient to demonstrate the Supplier's compliance with this DPA, Darktrace may, on reasonable prior written notice, conduct or commission an audit or inspection of the Supplier's relevant Processing activities, not more than once per annum.

11. DATA RETURN AND DESTRUCTION

11.1 On termination or expiry of the Agreement, the Supplier shall, within thirty (30) days, delete or return to Darktrace all Protected Data in its and/or its sub-processors' possession or control, in accordance with Darktrace's written instructions.

11.2 The Supplier shall provide Darktrace with written certification of deletion upon request.

12. GENERAL PROVISIONS

12.1 **Relationship to the Agreement.** This DPA supplements and forms part of the Agreement. Save as expressly modified by this DPA, the terms of the Agreement remain in full force and effect. In the event of any conflict between this DPA and the Agreement, this DPA shall prevail in respect of the Processing of Personal Data.

12.2 **Term.** This DPA shall commence on the effective date of the Agreement and shall continue in force until the later of: (a) the expiry or termination of the Agreement; and (b) the date on which the Supplier ceases to Process Protected Data on behalf of Darktrace.

12.3 **Governing Law and Jurisdiction.** This DPA shall be governed by and construed in accordance with the governing law of the Agreement, and the Parties submit to the exclusive jurisdiction of the courts specified in the Agreement, save to the extent that the Data Protection Laws or Standard Contractual Clauses require a different governing law or jurisdiction.

12.4 **Survival.** Clauses 9 (Personal Data Breach), 10 (Audit), 11 (Data Return and Destruction) and this Clause 13 shall survive termination or expiry of this DPA.

Annex A

Data Processing Description

A. LIST OF PARTIES

Controller(s) / Data exporter(s):

Name: Darktrace Holdings Limited or the applicable Darktrace Affiliate identified in the applicable purchase order or Order Form.

Address: Maurice Wilkes Building, St John's Innovation Park, Cowley Road, Cambridge, United Kingdom CB4 0DS, or as otherwise notified in writing.

Contact person's name, position and contact details: Data Protection Officer: Iain Pye. Address: Maurice Wilkes Building, Cowley Road, Cambridge, CB4 0DS. Email: privacy@darktrace.com.

Activities relevant to the data transferred under these Clauses: Processing to carry out the Offering pursuant to the Agreement entered into between Darktrace and the Supplier.

Signature and date: By transferring Protected Data to a Third County, the data exporter will be deemed to have signed this Annex A.

Role (controller/processor): Controller or Processor, as applicable.

Processor(s) / Data importer(s):

Name: The Supplier as identified in the applicable purchase order or Order Form.

Address: The Supplier's registered office address or as otherwise notified in writing.

Contact person's name, position and contact details: As notified by the Supplier to Darktrace in writing.

Activities relevant to the data transferred under these Clauses: Processing to carry out the Offering pursuant to the Agreement entered into between Darktrace and the Supplier.

Signature and date: By receiving Protected Data on Darktrace's instructions, the data importer will be deemed to have signed this Annex A.

Role (controller/processor): Controller or Processor, as applicable.

B. DESCRIPTION OF PROCESSING/ TRANSFER

Categories of Data Subjects: As agreed in writing between the Parties or, in the absence of agreement, those categories of data subjects whose Personal Data is necessarily processed by the Supplier in the provision of the Offering.

Categories of Personal Data: As agreed in writing between the Parties or, in the absence of agreement, those categories of Personal Data necessarily processed by the Supplier in the provision of the Offering.

Sensitive data transferred (if applicable) and applied restrictions or safeguards: As agreed in writing between the Parties. In the absence of agreement, no sensitive data shall be transferred.

Nature and Purpose of Processing: Processing of Personal Data by the Supplier solely as necessary for the provision of the Offering to Darktrace, or as otherwise agreed in writing between the Parties.

Subject Matter: The provision of the Offering by the Supplier to Darktrace pursuant to this Agreement.

Duration and Frequency of Processing: For the duration of the Term, on a continuous basis as necessary for the provision of the Offering.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority in accordance with Clause 13: The Data Protection Commission of the Republic of Ireland.

D. LIST OF AUTHORISED SUB-PROCESSORS

The Supplier shall maintain a current list of its authorized sub-processors, including the name, location and processing activities of each sub-processor, and shall make such list available to Darktrace upon written request and in accordance with Clause 6 of this DPA.

Annex B

Technical and Organisational Measures

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The technical and organisational measures (including the certifications held by the data importer) are as described in Clause 5 of this DPA, and as further specified by the Supplier in writing.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

The technical and organisational measures that the data importer will impose on sub-processors shall be materially equivalent to those set out in Clause 5 of this DPA.