DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is incorporated by reference into the Master Service Agreement and/or Order Form and/or the commercial agreement governing the use of Tufin's services ("**Agreement**") entered by and between you, the Customer (as defined in the Agreement) (collectively, "**you**", "**your**", "**Customer**"), and Tufin Software North America, Inc. ("**Tufin**", "**us**", "**we**", "**our**") to reflect the parties' agreement with regard to the Processing of Personal Data by Tufin solely on behalf of the Customer. Both parties shall be referred to as the "**Parties**" and each, a "**Party**".

Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement. By using the Services, Customer accepts this DPA and you represent and warrant that you have full authority to bind the Customer to this DPA. If you cannot, or do not agree to, comply with and be bound by this DPA, or do not have authority to bind the Customer or any other entity, please do not provide Personal Data to us.

In the event of any conflict between certain provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement solely with respect to the Processing of Personal Data.

1. **DEFINITIONS**

(a) "**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.

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

(c) "**CCPA**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. seq., and its implementing regulations, as may be amended from time to time, including the California Privacy Rights Act ("CPRA").;

(d) 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.

(e) 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.

(f) "**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, Canada, Israel and the United States of America, as applicable to the Processing of Personal Data under the Agreement including (without limitation) the GDPR, the UK GDPR, the FADP and the CCPA, as applicable to the Processing of Personal Data hereunder and in effect at the time of Processor's performance hereunder.

(g) "**Data Subject**" means the identified or identifiable person to whom the Personal Data

relates.

(h) "**FADP**" means the Swiss Federal Act on Data Protection of 19 June 1992.

(i) "**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).

(j) "**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 or Consumer, to the extent such information is processed by Tufin solely on behalf of Customer, under this DPA and the Agreement between Customer and Tufin.

(k) "**Services**" means the services provided to Customer by Tufin in accordance with the Agreement.

(l) "**Security Documentation**" means the Security Documentation applicable to the Services purchased by Customer, as updated from time to time and as made reasonably available by Tufin upon Customer's request.

(m) "**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.

(n) "**Standard Contractual Clauses**" shall mean the standard contractual clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

(o) "**Sub-processor**" means any third party that Processes Personal Data under the instruction or supervision of Tufin.

(p) "**UK GDPR**" means the Data Protection Act 2018, as well as the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties**. The Parties acknowledge and agree that with regard to the Processing of Personal Data solely on behalf of Customer, (i) Customer is the Controller of Personal Data, (ii) Tufin is the Processor of such Personal Data; or, if Customer uses the Services on behalf of a third-party data controller, then (iii) Customer is a Processor of the Personal Data, (iv) and Tufin is a Processor of the Personal Data Processing it on behalf of Customer and under its instructions.

2.2 **Customer's Processing of Personal Data**. Customer, in its use of the Services, and Customer's instructions to Tufin, shall comply with Data Protection Laws. Customer shall establish and have any and all required legal bases in order to collect, Process and transfer to Tufin the Personal Data, and to authorize the Processing by Tufin, and for Tufin's Processing activities on

Customer's behalf, including the pursuit of 'business purposes' as defined under the CCPA.

2.3 **Tufin's Processing of Personal Data**. When Processing on Customer's behalf under the Agreement, Tufin shall Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and this DPA; (ii) Processing for Customer as part of the provision of the Services; (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; (iv) rendering Personal Data fully anonymous, non-identifiable and non-personal in accordance with applicable standards recognized by Data Protection Laws and guidance issued thereunder; (v) Processing as required under the laws applicable to Tufin, and/or as required by a court of competent jurisdiction or other competent governmental or semi-governmental authority, provided that Tufin shall inform Customer of the legal requirement before Processing, unless such law or order prohibit such information on important grounds of public interest.

Tufin shall inform Customer without undue delay if, in Tufin's opinion, an instruction for the Processing of Personal Data given by Customer infringes applicable Data Protection Laws. To the extent that Tufin cannot comply with an instruction from Customer, Tufin (i) shall inform Customer, providing relevant details of the issue, (ii) Tufin 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 Services, and (iii) 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 Agreement and this DPA with respect to the affected Processing, and Customer shall pay to Tufin all the amounts owed to Tufin or due before the date of termination. Customer will have no further claims against Tufin (including, without limitation, requesting refunds for Services) pursuant to the termination of the Agreement and the DPA as described in this paragraph.

2.4 **Details of the Processing**. The subject-matter of Processing of Personal Data by Tufin is the performance of the Services 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 further specified in Schedule 1 (Details of Processing) to this DPA.

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

2.6 **CCPA Standard of Care; No Sale of Personal Information**. Tufin acknowledges and confirms that it does not receive or process any Personal Information as consideration for any services or other items that Tufin provides to Customer under the Agreement or this DPA. Tufin shall not have, derive, or exercise any rights or benefits regarding Personal Information Processed on Customer's behalf, nor shall it combine the Personal Information Processed on Customer's behalf with any information it processes on behalf of any other parties, 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. Tufin 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 Tufin under the Agreement or this DPA to qualify as "selling" such Personal Information under the CCPA.

3. DATA SUBJECT REQUESTS

Tufin shall, to the extent legally permitted, notify Customer or refer Data Subject or Consumer to Customer, if Tufin receives a request from a Data Subject or Consumer to exercise their rights (to the extent available to them under applicable Data Protection Laws) of access, right to rectification, restriction of Processing, erasure, data portability, objection to the Processing, their right not to be subject to automated individual decision making, to opt-out of the sale of Personal Information, or the right not to be discriminated against ("**Data Subject Request**"). Taking into account the nature of the Processing, Tufin shall assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible and reasonable, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. Tufin may respond to Data Subject Requests in order to refer Data Subject Requests received, and the Data Subjects making them, directly to the Customer for its treatment of such requests.

4. CONFIDENTIALITY

Tufin shall ensure that its personnel and advisors engaged in the Processing of Personal Data have committed themselves to confidentiality.

5. SUB-PROCESSORS

5.1 **Appointment of Sub-processors**. Customer acknowledges and agrees that (a) Tufin's Affiliates may be engaged as Sub-processors; and (b) Tufin and Tufin's Affiliates on behalf of Tufin may each engage third-party Sub-processors in connection with the provision of the Services.

5.2 **List of Current Sub-processors and Notification of New Sub-processors**. Tufin shall make available to Customer the current list of Sub-processors used by Tufin to process Personal Data upon Customer's written request. Such Sub-processor list shall include the identities of those Sub-processors and the entity's country ("**Sub-Processor List**"). The Sub-Processor List as of the date of first use of the Services by Customer is hereby deemed authorized upon first use of the Services. Customer may reasonably object to Tufin's use of an existing Sub-processor for reasons relating to the protection of Personal Data intended to be Processed by such Sub-processor, by providing a written objection to privacy@tufin.com within three (3) business days following the first use of the Services or receipt of the Sub-processor List following an appropriate request. In the event Customer reasonably objects to an existing Sub-processor, as permitted in the preceding sentence, Customer may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those Services which cannot be provided by Tufin without the use of the objected-to Sub-processor, by providing written notice to Tufin; provided that all amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Tufin. Customer will have no further claims against Tufin due to (i) past use of approved Sub-processors prior to the date of objection or (ii) the termination of the Agreement (including, without limitation, requesting refunds) and the DPA in the situation described in this paragraph.

5.3 **Objection to New Sub-processors**. Tufin shall notify Customer if Tufin updates the Sub-processor List. Customer may reasonably object to Tufin's 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 Tufin promptly in writing within seven (7) days after receipt of a notification. Such written objection shall include the reasons for objecting to Tufin's use of such new Sub-processor. Failure to object to such new Sub-processor in writing within seven (7) days following Tufin's notice shall be deemed as acceptance of the new Sub-Processor. In the event Customer reasonably objects to a new Sub-processor, as permitted in the preceding sentences, Tufin will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without

unreasonably burdening the Customer. If Tufin is unable to make available such change within thirty (30) days, Customer may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those Services which cannot be provided by Tufin without the use of the objected-to new Sub-processor, by providing written notice to Tufin. All amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Tufin. Until a decision is made regarding the new Sub-processor, Tufin may temporarily suspend the Processing of the affected Personal Data and/or suspend access to the Services. Customer will have no further claims against Tufin due to the termination of the Agreement (including, without limitation, requesting refunds) and/or the DPA in the situation described in this paragraph.

5.4 **Agreements with Sub-processors**. Tufin or a Tufin's Affiliate on behalf of Tufin has entered into a written agreement with each Sub-processor containing appropriate safeguards to the protection of Personal Data. Where Tufin engages a Sub-processor for carrying out specific Processing activities on behalf of the Customer, the same or materially similar data protection obligations as set out in this DPA shall be imposed on such new Sub-processor by way of a contract, in particular obligations to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the GDPR. Where a Sub-processor fails to fulfil its data protection obligations concerning its Processing of Personal Data, Tufin shall remain responsible for the performance of the Sub-processor's obligations.

6. SECURITY & AUDITS

6.1 **Controls for the Protection of Personal Data**. Tufin shall maintain industry-standard technical and organizational measures for protection of 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, including those measures set forth in the Security Documentation), as may be amended from time to time. Upon the Customer's reasonable request, Tufin will reasonably assist Customer, at Customer's cost and subject to the provisions of Section 11.1 below, 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 Tufin.

6.2 **Audits and Inspections**. Upon Customer's 14 days prior written request at reasonable intervals (no more than once every 12 months), and subject to strict confidentiality undertakings by Customer, Tufin shall make available to Customer that is not a competitor of Tufin (or Customer's independent, reputable, third-party auditor that is not a competitor of Tufin and not in conflict with Tufin, subject to their confidentiality and non-compete undertakings) information necessary to demonstrate compliance with this DPA, and allow for and contribute to audits, including inspections, conducted by them (provided, however, that such information, audits, inspections and the results therefrom, including the documents reflecting the outcome of the audit and/or the inspections, shall only be used by Customer to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without Tufin's prior written approval. Upon Tufin's first request, Customer shall return all records or documentation in Customer's possession or control provided by Tufin in the context of the audit and/or the inspection).

6.3 In the event of an audit or inspections as set forth above, Customer shall ensure that it (and each of its mandated auditors) will not cause (or, if it cannot avoid, minimize) any damage, injury or disruption to Tufin's premises, equipment, personnel and business while conducting such audit or inspection.

6.4 The audit rights set forth in 6.2 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).

7. DATA INCIDENT MANAGEMENT AND NOTIFICATION

Tufin 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 Tufin on behalf of the Customer (a "**Data Incident**"). Tufin shall make reasonable efforts to identify and take those steps as Tufin 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 Tufin's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or anyone who uses the Services 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 Tufin (including in any legal proceeding or in any notification to regulatory or supervisory authorities or affected individuals) without Tufin's 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 Tufin with reasonable prior written notice to provide Tufin with the opportunity to object to such disclosure and in any case, Customer will limit the disclosure to the minimum scope required.

8. RETURN AND DELETION OF PERSONAL DATA

Following termination of the Agreement and subject thereto, Tufin shall, at the choice of Customer, delete or return to Customer all the Personal Data it Processes solely on behalf of the Customer in the manner described in the Agreement, and Tufin shall delete existing copies of such Personal Data unless Data Protection Laws require otherwise. To the extent authorized or required by applicable law, Tufin may also retain one copy of the Personal Data solely for evidence purposes and/or for the establishment, exercise or defense of legal claims and/or for compliance with legal obligations.

9. CROSS-BORDER DATA TRANSFERS

9.1 **Transfers from the EEA, the United Kingdom and Switzerland to countries that offer adequate level of data protection**. Personal Data may be transferred from EU Member States, the three other EEA member countries (Norway, Liechtenstein and Iceland) (collectively, "**EEA**"), the United Kingdom ("**UK**") and Switzerland to countries that offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the European Union, the Member States or the European Commission, the UK, and/or Switzerland ("**Adequacy Decisions**"), as applicable, without any further safeguard being necessary.

9.2 **Transfers from the EEA, the United Kingdom and Switzerland to other countries**. If the Processing of Personal Data by Tufin includes a transfer (either directly or via onward transfer) from the EEA ("**EEA Transfer**"), the UK ("**UK Transfer**"), and/or Switzerland ("**Swiss Transfer**") to other countries which have not been subject to a relevant Adequacy Decision, and such transfers are not performed through an alternative recognized compliance mechanism as may be adopted by Processor for the lawful transfer of personal data (as defined in the GDPR, the UK GDPR, the FADP, as relevant) outside the EEA, the UK or Switzerland, as applicable, then (i) the terms set forth in Part 1 of **Schedule 2** (EEA Cross Border Transfers) shall apply to any such EEA Transfer; (ii) the terms set forth in part 2 of **Schedule 2** (UK Cross Border Transfers) shall apply to any such UK Transfer ("**UK Addendum**"); (iii) the terms set forth in Part 3 of **Schedule 2**

(Swiss Cross Border Transfers) shall apply to any such Swiss Transfer; and (iv) the terms set forth in Part 4 of **Schedule 2** (Additional Safeguards) shall apply to any such transfers.

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 Tufin Processes Personal Data on the behalf of such Authorized Affiliates, thus qualifying them as the "**Controller**". All access to and use of the Services 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 Customer.

10.2 **Communication**. Customer shall remain responsible for coordinating all communication with Tufin 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 Affiliates.

11. OTHER PROVISIONS

11.1 **Data Protection Impact Assessment and Prior Consultation**. Upon Customer's reasonable request, Tufin shall provide Customer, at Customer's cost, with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR or the UK GDPR (as applicable) to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Tufin. Tufin shall provide, at Customer's cost, reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 11.1, to the extent required under the GDPR or the UK GDPR, as applicable.

11.2 **Modifications**. Each Party may by at least forty-five (45) calendar days' prior written notice to the other Party, request in writing any variations to this DPA if they are required as a result of any change in, or decision of a competent authority under, any Data Protection Laws, to allow Processing of Customer Personal Data to be made (or continue to be made) without breach of those Data Protection Laws. Pursuant to such notice: (a) The Parties shall make commercially reasonable efforts to accommodate such modification requested by Customer or that Tufin believes is necessary; and (b) Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Tufin to protect Tufin against additional risks, or to indemnify and compensate Tufin for any further steps and costs associated with the variations made herein at Customer's request. The Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's or Tufin's notice as soon as is reasonably practicable. In the event that the Parties are unable to reach such an agreement within 30 days of such notice, then Customer or Tufin may, by written notice to the other Party, with immediate effect, terminate the Agreement to the extent that it relates to the Services which are affected by the proposed variations (or lack thereof). Customer will have no further claims against Tufin (including, without limitation, requesting refunds for the Services) pursuant to the termination of the Agreement and the DPA as described in this Section.

SCHEDULE 1 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

1. Providing the Services to Customer;
2. Performing the Agreement, this DPA and/or other contracts executed by the Parties;
3. Acting upon Customer's instructions, where such instructions are consistent with the terms of the Agreement;
4. Complying with applicable laws and regulations;
5. All tasks related with any of the above.

Duration of Processing

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

Type 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.

Categories of Data Subjects

Customer may submit Personal Data to the Services which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects:

- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Any other third-party individual whose Personal Data Customer decides to have Processed through the Services.

SCHEDULE 2 – CROSS BORDER TRANSFERS

PART 1 – EEA Cross Border Transfers

1. The parties agree that the terms of the Standard Contractual Clauses are hereby incorporated by reference and shall apply to an EEA Transfer.
2. Module Two (Controller to Processor) of the Standard Contractual Clauses shall apply where the EEA Transfer is effectuated by Customer as the data controller of the Personal Data and Tufin is the data processor of the Personal Data.
3. Module Three (Processor to Processor) of the Standard Contractual Clauses shall apply where the EEA Transfer is effectuated by Customer as the data processor of the Personal Data and Tufin is a Sub-processor of the Personal Data.
4. Clause 7 of the Standard Contractual Clauses (Docking Clause) shall not apply.
5. Option 2: GENERAL WRITTEN AUTHORISATION in Clause 9 of the Standard Contractual Clauses shall apply, and the method for appointing and time period for prior notice of Sub-processor changes shall be as set forth in Section 5.2 of the DPA.
6. In Clause 11 of the Standard Contractual Clauses, the optional language will not apply.
7. In Clause 17 of the Standard Contractual Clauses, Option 1 shall apply, and the Parties agree that the Standard Contractual Clauses shall be governed by the laws of the Republic of Ireland.
8. In Clause 18(b) of the Standard Contractual Clauses, disputes will be resolved before the courts of the Republic of Ireland.
9. Annex I.A of the Standard Contractual Clauses shall be completed as follows:

   Data Exporter: Customer.

   Contact details: As detailed in the Agreement.

   Data Exporter Role:

   Module Two: The Data Exporter is a data controller.

   Module Three: The Data Exporter is a data processor.

   Signature and Date: By entering into the Agreement and DPA, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

   Data Importer: Tufin.

   Contact details: As detailed in the Agreement.

   Data Importer Role:

   Module Two: The Data Importer is a data processor.

   Module Three: The Data Importer is a sub-processor.

   Signature and Date: By entering into the Agreement and DPA, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

10. Annex I.B of the Standard Contractual Clauses shall be completed as follows:

    The categories of data subjects are described in **Schedule 1** (Details of Processing) of this DPA.

    The categories of personal data are described in **Schedule 1** (Details of Processing) of this DPA.

    The Parties do not intend for Sensitive Data to be transferred.

    The frequency of the transfer is a continuous basis for the duration of the Agreement.

    The nature of the processing is described in **Schedule 1** (Details of Processing) of this DPA.

    The purpose of the processing is described in **Schedule 1** (Details of Processing) of this DPA.

    The period for which the personal data will be retained is for the duration of the Agreement, unless agreed otherwise in the Agreement and/or the DPA.

    In relation to transfers to Sub-processors, the subject matter, nature, and duration of the processing is set forth at the link detailed in Section 5 of the DPA.

11. Annex I.C of the Standard Contractual Clauses shall be completed as follows:

    The competent supervisory authority in accordance with Clause 13 is the supervisory authority in the Member State stipulated in Section 7 above.

12. The Security Documentation referred to in the DPA serves as Annex II of the Standard Contractual Clauses.

13. To the extent there is any conflict between the Standard Contractual Clauses and any other terms in this DPA or the Agreement, the provisions of the Standard Contractual Clauses will prevail.

PART 2 – UK Cross Border Transfers

Table 1: The Parties: as stipulated in Section 9 of Part 1 of this **Schedule 2**.

Table 2: Selected SCCs, Modules and Selected Clauses: as stipulated in Part 1 of this **Schedule 2**.

Table 3: Appendix Information: means the information which must be provided for the selected modules as set out in the Appendix of the Standard Contractual Clauses (other than the Parties), and which for this Part 2 is set out in Part 1 to this **Schedule 2**.

Table 4: Ending this Addendum when the Approved Addendum Changes: neither Party may end this Part 2 as set out in Section 19 of this Part 2.

Entering into this Part 2:

1. Each Party agrees to be bound by the terms and conditions set out in this Part 2, in exchange for the other Party also agreeing to be bound by this Part 2.
2. Although Annex 1A and Clause 7 of the Standard Contractual Clauses require signatures by the Parties, for the purpose of making UK Transfers, the Parties may enter into this Part 2 in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Part 2. Entering into this Part 2 will have the same effect as signing the Standard Contractual Clauses and any part of the Standard Contractual Clauses.

Interpretation of this Part 2:

3. Where this Part 2 uses terms that are defined in the Standard Contractual Clauses, those terms shall have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:

Addendum EU SCCs	The version(s) of the Standard Contractual Clauses which this Part 2 is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when the Parties are making a UK Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Standard Contractual Clauses	As defined in the DPA
ICO	The information commissioner.
Part 2	This Part 2 which is made up of this Part 2 incorporating the Addendum EU SCCs.
UK Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of this Part 2.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in Section 3 of the Data Protection Act 2018.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Transfer	A transfer which is covered by Chapter V of the UK GDPR.

4. This Part 2 must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Standard Contractual Clauses in any way which is not permitted under the Standard Contractual Clauses or this Part 2, such amendment(s) will not be incorporated by this Part 2 and the equivalent provision of the Standard Contractual Clauses will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Part 2, UK Data Protection Laws apply.
7. If the meaning of this Part 2 is unclear or there is more than one meaning, the meaning that most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted, and/or replaced after this DPA has been entered into.

Hierarchy:

9. Although Clause 5 of Standard Contractual Clauses sets out that the Standard Contractual Clauses prevail over all related agreements between the Parties, the Parties agree that, for a UK Transfer, the hierarchy in Section 10 below will prevail.

10. Where there is any inconsistency or conflict between this Part 2 and the Addendum EU SCCs (as applicable), this Part 2 overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the provisions of this Part 2.

11. Where this Part 2 incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Part 2 impacts those Addendum EU SCCs.

Incorporation and changes to the Standard Contractual Clauses:

12. This Part 2 incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Standard Contractual Clauses; and

    c. this Part 2 (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed on alternative amendments which meet the requirements of Section 12 above, the provisions of Section 15 below will apply.

14. No amendments to the Standard Contractual Clauses other than to meet the requirements of Section 12 above may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12 above) are made:

    a. References to the "Clauses" mean this Part 2, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

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

where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. To the extent applicable, Clause 8.7(i) of Module One is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules Two and Three is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. To the extent applicable, the reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module One, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by 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 of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Standard Contractual Clauses do not form part of this Part 2, except for footnotes 8, 9, 10 and 11.

Amendments to this Part 2:

16. The Parties may agree to change Clause 17 and/or 18 of this Part 2 to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Tables 1, 2 or 3 of this Part 2, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised UK Addendum which:

    a. makes reasonable and proportionate changes to the UK Addendum, including correcting errors in the UK Addendum; and/or

    b. reflects changes to UK Data Protection Laws;

    The revised UK Addendum will specify the start date from which the changes to the UK Addendum are effective and whether the Parties need to review this Part 2 including the Appendix Information. This Part 2 is automatically amended as set out in the revised UK Addendum from the start date specified.

19. If the ICO issues a revised UK Addendum under Section 18, if any Party, will as a direct result of the changes in the UK Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under this Part 2; and/or

    b. its risk under this Part 2,

    and in either case, it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Part 2 at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised UK Addendum.

20. The Parties do not need the consent of any third party to make changes to this Part 2, but any changes must be made in accordance with its terms.

Part 3 – Swiss Cross Border Transfers

The Parties agree that the Standard Contractual Clauses as detailed in Part 1 of this **Schedule 2**, shall be adjusted as set out below where the FADP applies to Swiss Transfers:

1. References to the Standard Contractual Clauses mean the Standard Contractual Clauses as amended by this Part 3;

2. The Swiss Federal Data Protection and Information Commissioner shall be the sole Supervisory Authority for Swiss Transfers exclusively subject to the FADP;

3. 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;

4. References to Regulation (EU) 2018/1725 are removed;

5. Swiss Transfers subject to both the FADP and the GDPR, shall be dealt with by the EU Supervisory Authority named in Part 1 of this **Schedule 2**;

6. References to the "Union", "EU" and "EU Member State" shall 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 the Standard Contractual Clauses;

7. Where Swiss Transfers are exclusively subject to the FADP, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the FADP;

8. Where Swiss Transfers are subject to both the FADP and the GDPR, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the FADP insofar as the Swiss Transfers are subject to the FADP;

PART 4 – Additional Safeguards

1. In the event of an EEA Transfer, a UK Transfer or a Swiss Transfer, the Parties agree to supplement these with the following safeguards and representations, where appropriate:

    a. The Processor shall have in place and maintain in accordance with good industry practice measures to protect the Personal Data from interception (including in transit from the Controller to the Processor and between different systems and services). This includes having in place and maintaining network protection intended to deny attackers the ability to intercept data and encryption of Personal Data whilst in transit and at rest intended to deny attackers the ability to read data.

    b. The Processor will make commercially reasonable efforts to resist, subject to applicable laws, any request for bulk surveillance relating to the Personal Data protected under GDPR or the UK GDPR, including under section 702 of the United States Foreign Intelligence Surveillance Act ("**FISA**");

    c. If the Processor becomes aware that any government authority (including law enforcement) wishes to obtain access to or a copy of some or all of the Personal Data, whether on a voluntary or a mandatory basis, then unless legally prohibited or under a mandatory legal compulsion that requires otherwise:

        I. The Processor shall inform the relevant government authority that the Processor is a processor of the Personal Data and that the Controller has not authorized the Processor to disclose the Personal Data to the government authority, and inform the relevant government authority that any and all requests or demands for access to the Personal Data should therefore be notified to or served upon the Controller in writing;

        II. The Processor will use commercially reasonable legal mechanisms to challenge any such demand for access to Personal Data which is under the Processor's control. Notwithstanding the above, (a) the Controller acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended government authority access, and (b) if, taking into account the nature, scope, context and purposes of the intended government authority access to Personal Data, the Processor has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual or entity, this subsection (c)(II) shall not apply. In such event, the Processor shall notify the Controller, as soon as possible, following the access by the government authority, and provide the Controller with relevant details of the same, unless and to the extent legally prohibited to do so.

2. Once in every 12-month period, the Processor will inform the Controller, at the Controller's written request, of the types of binding legal demands for Personal Data it has received and solely to the extent such demands have been received, including national security orders and directives, which shall encompass any process issued under section 702 of FISA.