Upwind Security

—

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is incorporated by reference into, and is subject to, the Terms of Service and any order form entered by and between you, the Customer (as defined therein) (collectively, "**you**", "**your**", "**Customer**") and the Upwind entity executing such Terms of Service and order form the Agreement ("**Upwind**", "**us**", "**we**", "**our**") (collectively, the "**Agreement**") to reflect the parties' agreement with regard to the Processing of Personal Data (as such terms are defined below) by Upwind solely on behalf of the Customer. Both parties shall be referred to as the "**Parties**" and each, a "**Party**".

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. The Customer accepts this DPA by using the Services (as defined below).

In case of any conflict between certain provisions of this DPA and the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement solely concerning the Processing of Personal Data. Capitalized terms not otherwise defined herein shall have the respective meanings assigned to them in the Agreement.

1. **Definitions**.

1.1. "**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 fifty percent (50%) of the voting interests of the subject entity.

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

1.3. "**CCPA**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. seq. (as amended by the California Privacy Rights Act of 2020) and its implementing regulations, each as amended or superseded from time to time.

1.4. The terms, "**Controller**", "**Member State**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR.

1.5. "**Data Incident**" means an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data Processed by the Processor on behalf of the Customer.

1.6. "**Data Protection Laws**" means all applicable and binding privacy and data protection laws and regulations, including of the European Union, the European Economic Area and their Member States, Switzerland, the United Kingdom, 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 US Federal and States privacy laws (including the CCPA), as applicable to the Processing of Personal Data hereunder and in effect at the time of the Processor's performance hereunder.

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

1.8. "**FADP**" means the Swiss Federal Act on Data Protection (as revised and in force as of September 1, 2023), as amended from time to time.

1.9. "**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).

1.10. "**Personal Data**" 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, to the extent such information is processed by Upwind solely on behalf of the Customer, under this DPA and the Agreement.

1.11. "**Services**" means the products, services, solutions, and/or platforms (as applicable) provided to the

Customer by Upwind in accordance with the Agreement.

1.12. "**Security Documentation**" means the security documentation applicable to the Services purchased by the Customer, as updated from time to time, and made reasonably available to the Customer by Upwind.

1.13. "**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.

1.14. "**Standard Contractual Clauses**" means (i) where the GDPR applies, the standard contractual clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021 ("**EU SCCs**"), or (ii) where the UK GDPR applies, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses as issued by the Information Commissioner's Officer under S119A(1) of the UK's Data Protection Act 2018 and in force as of 21 March 2022 ("**UK Addendum**").

1.15. "**Sub-processor**" means any third party that Processes Personal Data under the instruction or supervision of Upwind while and for providing the Services.

1.16. "**Sub-processors List**" means the list of Sub-processors available at https://www.upwind.io/sub-processors and includes the identities of those Sub-processors, the location of the Processing and the type of service rendered by each Sub-processor.

1.17. "**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 the Customer, (i) the Customer is the Controller of Personal Data, and (ii) Upwind is the Processor of such Personal Data. The terms "Controller" and "Processor" below hereby signify the Customer and Upwind, respectively.

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

2.3. Processor's Processing of Personal Data. When Processing on the Customer's behalf under the Agreement, the Processor shall Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and this DPA; (ii) for the provision of the Services and in connection therewith; (iii) to comply with the 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; and/or (v) to comply with the laws applicable to the Processor, and/or as required by a court of competent jurisdiction or other competent governmental or semi-governmental authority, provided that the Processor shall inform the Customer of the legal requirement before Processing, unless such law or order prohibits such information on important grounds of public interest.

In the event that the Customer discloses or otherwise makes available to the Processor Deidentified Data (as defined by applicable Data Protection Laws), the Processor shall (a) take reasonable measures to ensure that such data cannot be associated with a natural person, and (b) maintain and use such data without attempting to re-identify it.

To the extent that the Processor cannot comply with an instruction from the Customer because, for example, in the Processor's reasonable opinion, such instruction infringes a Data Protection Law, (x) the Processor shall inform the Customer, providing relevant details of the issue, and (y) if the Parties do not agree on a resolution to the issue in question after discussing in good faith for thirty (30) business days, the Customer may, as its sole remedy, terminate the Agreement and this DPA with respect to the affected Processing.

2.4. Details of the Processing. The subject-matter of Processing of Personal Data by the Processor is the performance of the Services pursuant to the Agreement and the purposes set forth in this DPA. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed hereunder 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 the Customer wishes to use the Services to Process Sensitive Data, it must first obtain the Processor's explicit prior written consent and enter into any additional agreements as required by Upwind.

2.6. CCPA Terms. If the Customer is a "Business" under the CCPA, and Upwind Processes Personal Data hereunder that is subject to the CCPA, the terms set forth in **Schedule 3** (CCPA Terms) hereto shall apply and bind the Parties regarding such Personal Data and the Processing itself.

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

4. **Confidentiality**. The Processor shall ensure that its personnel and advisors engaged in the Processing of Personal Data have contractually committed themselves to confidentiality.

5. **Sub-Processors**.

5.1. Appointment of Sub-processors. The Customer acknowledges and agrees that (i) the Processor's Affiliates may be engaged as Sub-processors; and (ii) the Processor and the Processor's Affiliates on behalf of the Processor 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. The Sub-processors List as of the date of first use of the Services by the Customer is hereby deemed authorized upon first use of the Services. The Customer can subscribe to notifications of changes to the Sub-processors List via https://www.upwind.io/sub-processors, and, in such case, the Processor shall provide notification to the e-mail address provided for such subscription of any new Sub-processor(s) before authorizing such new Sub-processor(s) to Process Personal Data in connection with the provision of the Services and thereby allow the Customer to object to such new Sub-processor in accordance with Section 5.3 below.

5.3. Objection to New Sub-processors. The Customer may reasonably object to the Processor'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 the Processor promptly in writing within ten (10) days after receipt of notice by the Processor of such new appointment. Such written objection shall include the reasons for objecting to the Processor's use of such new Sub-processor. Failure to object to such new Sub-processor in writing within ten (10) days following the Processor's notice shall be deemed as acceptance of the new Sub-processor. In the event the Customer reasonably objects to a new Sub-processor, as permitted in the preceding sentences, the Processor will use reasonable efforts to make available to the Customer a change in the Services or recommend a commercially reasonable change to the 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 the Processor is unable to make available such change within thirty (30) days, the Customer may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those Services which cannot be provided by the Processor without the use of the objected-to new Sub-processor, by providing written notice to the Processor. All amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to the Processor. Until a decision is made regarding the new Sub-processor, the Processor may temporarily suspend the Processing of the affected Personal Data and/or suspend access to the Services, without incurring any liability. The Customer will have no further claims against the Processor due to the termination of the Agreement (including, without limitation, requesting refunds) and/or this DPA and/or the suspension of Services in the situation described in this paragraph.

5.4. Agreements with Sub-processors. The Processor or a Processor's Affiliate on behalf of the Processor has

entered into a written agreement with each Sub-processor containing appropriate safeguards to the protection of Personal Data. Where the Processor 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 written contract, in particular obligations to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of Data Protection Laws. Where a Sub-processor fails to fulfill its data protection obligations concerning its Processing of Personal Data, the Processor shall remain responsible for the performance of the Sub-processor's obligations.

6. **Security & Audits**.

6.1. Controls for the Protection of Personal Data. The Processor 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, the Processor will reasonably assist the Customer, at the 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 the Processor.

6.2. Audits and Inspections. Upon the Customer's thirty (30) days' prior written request at reasonable intervals (no more than once every twelve (12) months), and subject to strict confidentiality undertakings by the Customer, the Processor shall reasonably make available to the Customer that is not a competitor of the Processor or any of its Affiliates (or such mutually agreed independent, reputable, third-party auditor that is not a competitor of the Processor or any of its Affiliates and not in conflict with the Processor or any of its Affiliates, subject to their confidentiality and non-compete undertakings) information necessary to demonstrate compliance with Data Protection Laws and 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 the Customer to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without the Processor's prior written approval). Upon the Processor's first request, the Customer shall return all records or documentation in the Customer's possession or control provided by the Processor in the context of the audit and/or the inspection). If and to the extent that the Standard Contractual Clauses apply, nothing in this Section 6.2 varies or modifies the Standard Contractual Clauses nor affects any Supervisory Authority's or Data Subject's rights under the Standard Contractual Clauses.

6.3. In the event of an audit or inspections as set forth above, the 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 the Processor's premises, equipment, personnel and business while conducting such audit or inspection.

6.4. In the event that such audit or inspection uncovers unauthorized Processing of Personal Data, the Customer shall have the right to, upon notice, take reasonable and appropriate steps to stop and remediate such unauthorized Processing.

6.5. The audit rights set forth in Section 6.2 above shall only apply to the extent that the Agreement does not otherwise provide the 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**. The Processor maintains security incident management policies and procedures and, to the extent required under Data Protection Laws, shall notify the Customer without undue delay after becoming aware of a Data Incident. The Processor shall make reasonable efforts to identify and take those steps as the Processor 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 its reasonable control. The 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 the Processor or any Sub-processor (including, to the extent legally permissible and does not directly conflicting with Data Protection Laws, in any legal proceeding or in any notification to Supervisory Authorities, other regulatory authorities or affected individuals, and excluding disclosure to third-party consultants and advisors of the Customer that are subject to appropriate confidentiality undertakings) without the Processor's prior written approval, unless, and solely to the extent that, the Customer is compelled to do so in order to notify any competent data protection authority of a Data

Incident in a mandatory manner prescribed by such authority, or pursuant to Data Protection Laws. In the latter case, unless prohibited by such laws, the Customer shall provide the Processor with reasonable prior written notice to provide the Processor with the opportunity to object to such disclosure, and in any case, the 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, the Processor shall delete or return to the Customer all the Personal Data it Processes solely on behalf of the Customer, and the Processor shall delete existing copies of such Personal Data unless Data Protection Laws require otherwise. To the extent authorized or required by applicable law, the Processor 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. **Trans Border Data Transfers**.

9.1. Transfers from the EEA, Switzerland, and the UK to countries that offer an 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**"), Switzerland and the United Kingdom ("**UK**") 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 EU, their member countries or the European Commission, Switzerland, and/or the UK as relevant and applicable ("**Adequacy Decisions**"), without any further safeguard being necessary.

9.2. Transfers from the EEA, the UK, and Switzerland to other countries. If the Processing of Personal Data by the Processor 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 for the lawful transfer of personal data (as defined in the GDPR, the UK GDPR, or the FADP, as relevant), then: (i) the terms set forth in Part 1 of **Schedule 2** (EEA Trans-Border Transfers) shall apply to any such EEA Transfer; (ii) the terms set forth in Part 2 of **Schedule 2** (UK Trans-Border Transfers) shall apply to any such UK Transfer; (iii) the terms set forth in Part 3 of **Schedule 2** (Swiss Trans-Border Transfers) shall apply to any such Swiss Transfer; (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 this DPA, the Customer enters into this 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 the Processor 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 the Customer.

10.2. Communication. The Customer shall remain responsible for coordinating all communication with the Processor 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 the Customer's reasonable request, the Processor shall provide the Customer, at the Customer's cost, with reasonable cooperation and assistance needed to fulfil the Customer's obligation under Data Protection Laws to carry out a data protection impact assessment of data protection assessment (as applicable) related to the Customer's use of the Services, to the extent the Customer does not otherwise have access to the relevant information, and to the extent such information is available to the Processor. The Processor shall provide reasonable assistance to the 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 thirty (30) 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 Data Protection Laws, to allow Processing of Personal Data to be made (or continue to be made) without breach of those Data Protection Laws. The Parties shall promptly discuss the

proposed variations in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in a Party's notice as soon as is reasonably practicable. In the event that the Parties are unable to reach such an agreement within thirty (30) days of such notice, then the Customer or the Processor may, by written notice to the other Party, with immediate effect, terminate the Agreement and/or this DPA to the extent that it relates to the Services which are affected by the proposed variations (or lack thereof). The Customer will have no further claims against the Processor and/or its Affiliates.

Last Updated: September 2026

Schedule 1
DETAILS OF THE PROCESSING

Nature and Purpose of Processing

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

Duration of Processing.

Subject to any section of this DPA and/or the Agreement dealing with the duration of the Processing and the consequences of the expiration or termination thereof, the Processor will Process Personal Data pursuant to this DPA and Agreement for the duration of the Agreement and subject to Section 8 of this DPA, unless otherwise agreed upon in writing.

Type of Personal Data

The Customer may submit Personal Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion.

- The Company primarily retains technical metadata (e.g., vulnerability identifiers, configuration details, installed components, activity logs, system identifiers, and file paths). Depending on the Customer's configuration, such metadata may incidentally contain limited Personal Data.
- If the Customer uses the Platform's scanners hosted in the Processor's environment, Personal Data may be processed during the security scanning and assessment activities for a limited period, depending on the Customer's environment and connected sources.

Categories of Data Subjects

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

(a) employees, agents, advisors, freelancers of the Customer (who are natural persons);
(b) prospects, customers, business partners and vendors of the Customer (who are natural persons);
(c) employees or contact persons of the Customer's prospects, customers, business partners and vendors; and
(d) any other third-party individual whose Personal Data the Customer decides to have Processed through the Services.

Schedule 2
CROSS BORDER TRANSFERS

PART 1 – EEA Cross Border Transfers Addendum.

1. The Parties agree that the terms of the EU SCCs are hereby incorporated by reference and shall apply to an EEA Transfer.

2. Module Two (Controller to the Processor) of the EU SCCs shall apply where the EEA Transfer is effectuated by Customer as the data controller of the Personal Data and Upwind is the data processor of the Personal Data.

3. Module Three (Processor to the Processor) of the EU SCCs shall apply where the EEA Transfer is effectuated by Customer as the data processor of the Personal Data and Upwind is a sub-processor of the Personal Data.

4. Clause 7 of the EU SCCs (Docking Clause) shall not apply.

5. Option 2: GENERAL WRITTEN AUTHORISATION in Clause 9 of the EU SCCs 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 of this DPA.

6. In Clause 11 of the EU SCCs, the optional language will not apply.

7. In Clause 17 of the EU SCCs, Option 1 shall apply, and the Parties agree that the EU SCCs shall be governed by the laws of the Republic of Ireland.

8. In Clause 18(b) of the EU SCCs, disputes will be resolved before the courts of the Republic of Ireland.

9. Annex I.A of the EU SCCs shall be completed as follows:

    9.1. Data Exporter: The Customer.

    9.2. Contact details: As detailed in the Agreement.

    9.3. Data Exporter Role:

        9.3.1. Module Two: The Data Exporter is a data controller.

        9.3.2. Module Three: The Data Exporter is a data processor.

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

    9.5. Data Importer: Upwind.

    9.6. Contact details: As detailed in the Agreement.

    9.7. Data Importer Role:

        9.7.1. Module Two: The Data Importer is a data processor.

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

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

10. Annex I.B of the EU SCCs shall be completed as follows:

    10.1. The categories of data subjects are described in **Schedule 1** of this DPA.

    10.2. The categories of personal data are described in **Schedule 1** of this DPA.

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

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

    10.5. The nature of the processing is described in **Schedule 1** of this DPA.

10.6. The purpose of the processing is described in **Schedule 1** of this DPA.

10.7. The period for which the personal data will be retained is the duration of the Agreement and subject to Section 8 of this DPA, unless agreed otherwise in the Agreement and/or this DPA.

10.8. In relation to transfers to Sub-processors, the subject matter and nature of the processing is set forth in the Sub-processors List referred to in Section 5 of this DPA and listed in **Schedule 1** (Details of Processing) of this DPA.

11. Annex I.C of the EU SCCs shall be completed as follows:

11.1. 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 this DPA serves as Annex II of the EU SCCs.

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

PART 2 – UK Cross Border Transfers Addendum.

The Parties agree that the UK Addendum is hereby incorporated by reference and shall apply to UK Transfers as set forth in this Part 2, together with the EU SCCs as set forth in Part 1 of this **Schedule 2**.

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

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

3. **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**.

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

5. The Alternative Part 2 Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the Information Commissioner's Office (ICO) and laid before the UK Parliament in accordance with S119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18 of those mandatory clauses.

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 ("**FDPIC**") 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 FDPIC, insofar as the Swiss Transfer is governed by the FADP, and by the EU Supervisory Authority named in Part 1 of this **Schedule 2**, insofar as the Swiss Transfer is governed by the GDPR.

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:

    1.1. 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.

    1.2. 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**");

    1.3. 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:

        1.3.1. 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; and

        1.3.2. 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, (i) 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 (ii) 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 twelve (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 to the extent such disclosure is not legally prohibited, 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.

Schedule 3
CCPA TERMS

1. **Scope, Application & Interpretation**.

1.1. This **Schedule 3** shall apply and bind the Parties if and to the extent that (i) the Customer is a Business under the CCPA, and (ii) Upwind Processes Personal Information (as defined below) that is subject to the CCPA in the course of providing the Services to the Customer pursuant to the Agreement.

1.2. This **Schedule 3** prevails over any conflicting terms of the Agreement or this DPA but does not otherwise modify the Agreement or this DPA.

1.3. This **Schedule 3** shall be interpreted in favor of the Parties' intent to comply with the CCPA, and therefore any ambiguity shall be resolved in favor of a meaning that complies and is consistent with the CCPA.

1.4. Capitalized terms not specifically defined in this **Schedule 3** shall have the respective meanings ascribed to them in this DPA, as amended by this **Schedule 3**.

2. **Definitions**. For the purposes of this **Schedule 3**:

2.1. The terms "**Business**", "**Collects**" (and "**collected**" and "**collection**"), "**Consumer**", "**Business Purpose**", "**Sell**" (and "**selling**", "**sale**", and "**sold**"), "**Share**" (and "**shared**" or "**sharing**"), and "**Service Provider**" shall each have the same meaning as in the CCPA.

2.2. "**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 Consumer or household of a Consumer, which is processed by Upwind solely on behalf of the Customer under this **Schedule 3** and the Agreement.

3. **Processing of Personal Information**.

3.1. The Customer hereby appoints Upwind as a Service Provider to Process Personal Information on behalf of the Customer. The Customer, in its use of the Services, and the Customer's instructions to Upwind, shall comply with the CCPA. The Customer represents and warrants that it has provided notice consistent with Section 1798.130 of the CCPA and has obtained consents to the extent required under the CCPA for Upwind to lawfully Collect and Process the Personal Information in pursuit of the Permitted Purposes (as defined in Section 3.2 below).

3.2. Upwind shall Process Personal Information solely for the purposes set forth in Section 2.3 of this DPA and as necessary to comply with this **Schedule 3** and the CCPA, which may include, for the avoidance of doubt, the pursuit of Business Purposes such as helping to ensure security and integrity (collectively, the "**Permitted Purposes**").

3.3. Sections 3-8, 10 and 11.2 of this DPA shall apply to the Processing of Personal Information and the following terms shall be replaced as follows: "Data Protection Laws" shall mean the CCPA; "DPA" shall mean this **Schedule 3**; "Personal Data" shall mean "Personal Information"; "Data Subject" shall mean "Consumer"; "Controller" shall mean "Business"; "Processor" shall mean "Service Provider"; and Sub-processor shall refer to the concept of a subcontractor engaged by Upwind to Process Personal Information.

3.4. Upwind shall Process Personal Information in accordance with the provisions of the CCPA, and in a manner that provides the same level of privacy protection to Personal Information as required by the CCPA. Upwind certifies that it understands the rules, requirements, and definitions of the CCPA and this **Schedule 3**, and shall comply with them.

3.5. Upwind acknowledges and confirms that it does not receive nor process any Personal Information as consideration for any services or other items that Upwind provides to the Customer under the Agreement. Upwind agrees to refrain from Selling and/or Sharing any Personal Information Processed hereunder without the Customer's prior written consent, nor taking any action that would cause any transfer of Personal Information to or from Upwind under the Agreement or this **Schedule 3** to qualify as Selling and/or Sharing such Personal Information. Upwind shall not have, derive, or exercise any rights or benefits regarding the Personal Information, and shall not retain, use, or disclose any Personal Information (i) for any purpose other than the Permitted Purposes, and/or (ii) outside of the direct business relationship between the Parties.

3.6. Upwind shall not combine Personal Information with any other data if and to the extent that this would be inconsistent with the limitations on Service Providers under the CCPA.

3.7. If Upwind receives any Personal Information in Deidentified form, Upwind shall take reasonable measures to ensure that such Deidentified Personal Information cannot be associated with a Consumer or household.

3.8. Upwind shall notify the Customer if Upwind makes a determination that it can no longer meet its obligations under this **Schedule 3** and/or the CCPA.