DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is incorporated by reference into the agreement governing the use of TrustFlight's services ("**Agreement**") entered by and between you, the Customer (as defined in the Agreement) (collectively, "**you**", "**your**", "**Customer**"), and the TrustFlight entity set forth in the Agreement ("**TrustFlight**", "**us**", "**we**", "**our**") to reflect the parties' agreement with regard to the Processing of Personal Data by TrustFlight 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

1.1 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 TrustFlight but has not signed its own agreement with TrustFlight 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. (as amended by the California Privacy Rights Act) and its implementing regulations, each as amended or superseded from time to time.

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

(e) "**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, Australia 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, and the FADP, known or reasonably expected by Processor to be applicable to the Processing of Personal Data hereunder and in effect at the time of Processor's performance hereunder.

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

(g) "**FADP**" means the Federal Act on Data Protection of 19 June 1992, and as revised as of 25 September 2020, the "**Revised FADP**".

(h) "**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).

(i) "**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, which is processed by TrustFlight solely on behalf of Customer under this DPA and the Agreement.

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

(k) "**Security Documentation**" means the Security Documentation applicable to the Services purchased by Customer, as updated from time to time, and made reasonably available to Customer by TrustFlight.

(l) "**Standard Contractual Clauses**" means (a) 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 (b) where the UK GDPR applies, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses as issued by the Information Commissioner's Office under S119A(1) of the Data Protection Act 2018 and in force as of 21 March 2022 ("**UK Addendum"**).

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

(n) **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) TrustFlight is the Processor of such Personal Data. The terms "Controller" and "Processor" below hereby signify Customer and TrustFlight, respectively.

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

2.3 **Processor's Processing of Personal Data**. When Processing on Customer's behalf under the Agreement, Processor 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 its 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 Processor, and/or as required by a court of competent jurisdiction or other competent governmental or semi- governmental authority, provided that Processor shall inform Customer of the legal requirement before Processing, unless such law or order prohibit such information on important grounds of public interest.

Processor shall inform Customer without undue delay if, in Processor's opinion, an instruction for the Processing of Personal Data given by Customer infringes applicable Data Protection Laws. To the extent that Processor cannot comply with an instruction from Customer, Processor (i) shall inform Customer, providing relevant details of the issue, (ii) Processor

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 Processor all the amounts owed to Processor or due before the date of termination. Customer will have no further claims against Processor (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 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 under this DPA are further specified in **Schedule 1** (Details of Processing) to this DPA.

2.5 **CCPA Terms**. If Customer is a Business under the CCPA, and TrustFlight Process 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 with regards to such Personal Data and the Processing thereof.

3. DATA SUBJECT REQUESTS

Processor shall, to the extent legally permitted, notify Customer or refer Data Subject to Customer, if 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 their right not to be subject to automated individual decision making ("**Data Subject Request**"). Taking into account the nature of the Processing, Processor shall assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible and reasonable, for the fulfillment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. Processor may advise Data Subjects on available features for self-exercising their Data Subject Requests through the Services (where appropriate), and/or refer Data Subject Requests received, and the Data Subjects making them, directly to the Customer for its treatment of such requests.

4. CONFIDENTIALITY

Processor 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) Processor's Affiliates may be engaged as Sub-processors; and (b) Processor and Processor's Affiliates on behalf of 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**. Processor makes available to Customer the current list of Sub-processors used by Processor to process Personal Data via https://trustflight.com/privacy/sub-processors. Such Sub-processor list includes the identities of those Sub-processors, the location of the Processing and the type of service rendered by each Sub-processor ("**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.

5.3 **Objection to New Sub-processors**. Customer may reasonably object to 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 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 Processor's use of such new Sub- processor. Failure to object to such new Sub-processor in writing within ten (10) days following Processor'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, Processor 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 Processor 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 Processor without the use of the objected-to new Sub-processor, by providing written notice to Processor. All amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Processor. Until a decision is made regarding the new Sub-processor, Processor may temporarily suspend the Processing of the affected Personal Data and/or suspend access to the Account. Customer will have no further claims against Processor 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**. Processor or a Processor's Affiliate on behalf of Processor has entered into a written agreement with each Sub-processor containing appropriate safeguards to the protection of Personal Data. Where 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 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 fulfill its data protection obligations concerning its Processing of Personal Data, 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**. 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, Processor 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 Processor.

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, Processor shall make available to Customer that is not a competitor of Processor (or Customer's independent, reputable, third-party auditor that is not a competitor of Processor and not in conflict with Processor, 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 Processor's prior written approval. Upon Processor's first request, Customer shall return all records or documentation in Customer's possession or control provided by 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, 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 Processor'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

Processor 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 Processor on behalf of the Customer (a "**Data Incident**"). Processor shall make reasonable efforts to identify and take those steps as 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 Processor's reasonable control. 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 Processor (including in any legal proceeding or in any notification to regulatory or supervisory authorities or affected individuals, and excluding disclosure to third-party consultants and advisors of Customer that are subject to appropriate confidentiality undertakings) without Processor's prior written approval, unless, and solely to the extent that, 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 applicable Data Protection Laws. In the latter case, unless prohibited by such laws, Customer shall provide Processor with reasonable prior written notice to provide Processor 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

Within 30 days following termination of the Agreement and subject thereto, Processor shall, at the choice of Customer (indicated through the Services or in written notification to Processor), 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 Processor shall delete existing copies of such Personal Data unless Data Protection Laws require otherwise. To the extent authorized or required by applicable law, Processor and Customer may mutually decide whether it is required for Processor to retain any 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 or regulatory obligations.

9. TRANS-BORDER DATA TRANSFERS

9.1 **Transfers from the EEA, Switzerland and the United Kingdom 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**"), 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 European Union, the Member States or the European Commission, Switzerland, and/or the UK as relevant ("**Adequacy Decisions**"), as applicable, 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 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 as may be adopted by Processor for the lawful transfer of personal data (as defined in the GDPR, the UK GDPR, and/or 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 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; and (iv) the terms set forth in Part 4 of **Schedule 2** (Additional Safeguards) shall apply to any such transfers.

9.3 For the avoidance of doubt, Processor will transfer Personal Data originating from the EEA, UK, or Switzerland to countries that have not been subject to a relevant Adequacy Decision only subject to the Standard Contractual Clauses or an alternative recognized compliance mechanism for the lawful transfer of personal data outside the EEA, the UK, or Switzerland as set out in Article 46 of the GDPR or UK GDPR (as applicable).

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 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 Customer.

10.2 **Communication**. Customer shall remain responsible for coordinating all communication with 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 Customer's reasonable request, Processor shall provide Customer, at Customer's cost, with reasonable cooperation and assistance needed to fulfill 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 Processor. Processor shall provide 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 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, 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 Processor believes is necessary; and (b) Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Processor to protect the Processor against additional risks, or to indemnify and compensate Processor 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 Processor'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 Processor 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 Processor (including, without limitation, requesting refunds for the Services) pursuant to the termination of the Agreement and the DPA as described in this Section.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement with effect from the date first set out above.

Controller: _____	**Processor: TrustFlight**
Signature _____	Signature _____
Name _____	Name _____
Title _____	Title _____
Date _____	Date _____

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. Sharing Personal Data with third parties in accordance with Customer's instructions and/or pursuant to Customer's use of the Services (e.g., integrations between the Services and any services provided by third parties, as configured by or on behalf of Customer to facilitate the sharing of Personal Data between the Services and such third-party services);
5. Complying with applicable laws and regulations;
6. All tasks related to 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, Processor 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 where such data typically includes: The name, contact, certification and role information of Customer's personnel.

Categories of Data Subjects

Customer may submit Personal Data to the Services which mostly includes, but is not limited to, Personal Data relating to the following categories of Data Subjects: Employees, agents, advisors, clients, freelancers of Customer (who are natural persons).

SCHEDULE 2 – TRANS BORDER TRANSFERS

PART 1 – EEA Trans-Border Transfers

1. The parties agree that the terms of the EU SCCs are hereby incorporated by reference and shall apply to an EEA Transfer as set out in this Part 1.
2. Module Two (Controller to Processor) of the EU SCCs shall apply where the EEA Transfer is effectuated by Customer as the data controller of the Personal Data and TrustFlight is the data processor of the Personal Data.
3. Module Three (Processor to Processor) of the EU SCCs shall apply where the EEA Transfer is effectuated by Customer as the data processor of the Personal Data and TrustFlight is a sub-processor of the Personal Data.
4. Module Four (Processor to Controller) of the EU SCCs shall apply where the EEA Transfer is effectuated by TrustFlight as the data processor of the Personal Data and Customer is the data controller of the Personal Data.
5. Clause 7 of the EU SCCs (Docking Clause) shall not apply.
6. Option 2: GENERAL WRITTEN AUTHORISATION in Clause 9 of the EU SCCs shall apply, and the time period for prior notice of Sub-processor changes shall be as set forth in Section 5.3 of the DPA.
7. In Clause 11 of the EU SCCs, the optional language will not apply.
8. 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.
9. In Clause 18(b) of the EU SCCs, disputes will be resolved before the courts of the Republic of Ireland.
10. Annex I.A of the EU SCCs shall be completed as follows:

	Data Exporter	**Data Importer**
Module Two	Name: Customer. Contact details: as detailed in the Agreement. Activities relevant to the data transferred: as detailed in **Schedule 1** to this DPA. Signature and date: by entering into the Agreement and DPA, Data Exporter is deemed to have signed this Annex I to the EU SCCs. Role: data controller.	Name: TrustFlight. Contact details: as detailed in the Agreement. Activities relevant to the data transferred: as detailed in **Schedule 1** to this DPA. Signature and date: by entering into the Agreement and DPA, Data Importer is deemed to have signed this Annex I to the EU SCCs. Role: data processor.
Module Three	Name: Customer. Contact details: as detailed in the Agreement. Activities relevant to the data transferred: as detailed in **Schedule 1** to this DPA. Signature and date: by entering into the Agreement and DPA, Data Exporter is deemed to have signed this Annex I to the EU SCCs. Role: data processor.	Name: TrustFlight. Contact details: as detailed in the Agreement. Activities relevant to the data transferred: as detailed in **Schedule 1** to this DPA. Signature and date: by entering into the Agreement and DPA, Data Importer is deemed to have signed this Annex I to the EU SCCs. Role: sub-processor.
Module Four	Name: TrustFlight. Contact details: as detailed in the Agreement. Activities relevant to the data transferred: as detailed in **Schedule 1** to this DPA. Signature and date: by entering into the Agreement and DPA, Data Exporter is deemed to have signed this Annex I to the EU SCCs. Role: data processor.	Name: Customer. Contact details: as detailed in the Agreement. Activities relevant to the data transferred: as detailed in **Schedule 1** to this DPA. Signature and date: by entering into the Agreement and DPA, Data Importer is deemed to have signed this Annex I to the EU SCCs. Role: data controller.

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

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

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

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** to this DPA.

The purpose of the processing is described in **Schedule 1** to 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 this 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 5.2 of this DPA.

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

    The competent supervisory authority in accordance with Clause 13 is the supervisory authority in the Member State applicable to the Customer.

13. The Security Documentation referred to in the DPA serves as Annex II of the EU SCCs.

14. 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 Trans-Border Transfers

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.

Table 1: Parties: As stipulated in Section 10 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: Annex 1A: As stipulated in Section 10 of Part 1 of this **Schedule 2**; Annex 1B: As stipulated in Section 11 of Part 1 of this **Schedule 2**; Annex II: As stipulated in Section 13 of Part 1 of this **Schedule 2**; Annex III: As set forth at the link detailed in Section 5.2 of this DPA.

Table 4: Ending this Addendum when the Approved Addendum Changes: Neither Party may end this UK Addendum in the manner set out in Section 19 of the Mandatory Clauses of the UK Addendum.

Mandatory Clauses: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 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 those Mandatory Clauses.

PART 3 – Swiss Trans-Border Transfers

The Parties agree that the EU SCCs 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 EU SCCs 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 EU SCCs 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 EU SCCs;

7. Where Swiss Transfers are exclusively subject to the FADP, all references to the GDPR in the EU SCCs 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 EU SCCs are to be understood to be references to the FADP insofar as the Swiss Transfer is 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 that 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.

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) Customer is a Business under the CCPA, and (ii) TrustFlight Processes Personal Information (as defined below) that is subject to the CCPA in the course of providing the Services to Customer pursuant to the Agreement.

1.2 This **Schedule 3** prevails over any conflicting terms of the Agreement or the DPA but does not otherwise modify the Agreement or the 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 herein shall have the meanings ascribed to them in the 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 TrustFlight solely on behalf of Customer under this **Schedule 3** and the Agreement.

3. PROCESSING OF PERSONAL INFORMATION

3.1 Customer hereby appoints TrustFlight as a Service Provider to Process Personal Information on behalf of Customer. Customer, in its use of the Services, and Customer's instructions to TrustFlight, shall comply with the CCPA. Customer represents and warrants that it has provided notice consistent with Section 1798.135 of the CCPA, and has obtained consents to the extent required under the CCPA for TrustFlight to lawfully Collect and Process the Personal Information in pursuit of the Permitted Purposes (as defined in Section 3.2 below).

3.2 TrustFlight shall Process Personal Information solely for the purposes set forth in Section 2.3 of the DPA and as necessary to comply with this **Schedule 3** and the CCPA. For the avoidance of doubt, such Processing shall include the pursuit of Business Purposes, including providing Customer with TrustFlight's software and services platform incorporating Centrik, Tech Log, MEL Manager and Smart Suite, collectively digital workflows that improve compliance and streamline operational processes. (collectively: the "**Permitted Purposes**").

3.3 Sections 3-8, 10, 11.2 of the 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 Service Provider engaged by TrustFlight to Process Personal Information.

3.4 TrustFlight 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. TrustFlight certifies that it understands the rules, requirements, and definitions of the CCPA and this **Schedule 3**, and shall comply with them.

3.5 TrustFlight acknowledges and confirms that it does not receive or process any Personal Information as consideration for any services or other items that TrustFlight provides to Customer under the Agreement. TrustFlight agrees to refrain from Selling and/or Sharing 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 TrustFlight under the Agreement or this **Schedule 3** to qualify as Selling and/or Sharing such Personal Information. TrustFlight 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 TrustFlight 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 TrustFlight shall notify Customer if TrustFlight makes a determination that it can no longer meet its obligations under this **Schedule 3** and/or the CCPA