

AURASCAPE DATA PROCESSING AGREEMENT

This Data Processing Agreement (this “**DPA**”) is entered into by and between Aurascape, Inc. and its Affiliates (collectively, “**Aurascape**”) and the entity or organization, including any participating Affiliates of such entity or organization (collectively, “**Customer**”), that has executed a License Agreement or other software subscription agreement with Aurascape in connection with the provision of Aurascape Solutions (as applicable, the “**Agreement**”), and reflects such parties’ agreement with respect to the Processing of Personal Data by Aurascape solely on behalf of Customer. Aurascape and Customer are hereinafter referred to individually as a “**Party**” and collectively as the “**Parties**”. This DPA is deemed to be entered into as of the applicable effective date of the Agreement (the “**Effective Date**”).

1. Definitions.

1. “**Affiliate**” of a Party means, as of the applicable date of determination, any other entity that, directly or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with, such Party. The term “control” (including the terms “controlled by” and “under common control with”) means the direct or indirect ownership of more than 50% of the voting securities, or the power in fact to direct or cause the direction of the management, of an entity.
2. “**Controller**” means any natural or legal person, business, entity or authority which determines the purposes and the means of the Processing of Personal Data, within the meaning of the applicable Data Protection Laws.
3. “**Data Breach**” means any Personal Data incident or breach, within the meaning of the applicable Data Protection Laws.
4. “**Data Privacy Framework**” means, as applicable, the EU-US Data Privacy Framework, the UK Extension to the EU-US Data Privacy Framework and/or the Swiss-US Data Privacy Framework self-certification programs operated by the US Department of Commerce, in each case as respectively amended or replaced from time to time.
5. “**Data Protection Laws**” means all applicable privacy, security and data protection laws and regulations, as applicable to the Processing of Personal Data hereunder including, without limitation, the “**GDPR**” (Regulation (EU) 2016/679), the UK Data Protection Act of 1998 and the “**UK GDPR**” (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), the “**FADP**” (the Swiss Federal Act on Data Protection of 19 June 1992, as revised as of 25 September 2020), and the “**CCPA**” (California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020), in each case as respectively amended or replaced from time to time.
6. “**Data Subject**” means any natural person, individual or consumer to whom the Personal Data relates, within the meaning of the applicable Data Protection Laws.
7. “**EU SCCs**” means the Standard Contractual Clauses between Controllers and Processors, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
8. “**Household**” means a group, however identified, of Data Subjects, within the meaning of the applicable Data Protection Laws.
9. “**Personal Data**” or “**Personal Information**” means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, to an identified or identifiable Data Subject or, where applicable, a Household, within the meaning of the applicable Data Protection Laws.
10. “**Processing**” means any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, within the meaning of the applicable Data Protection Laws.
11. “**Processor**” means any natural or legal person, service provider, entity or authority which Processes Personal Data on behalf of the Controller, within the meaning of the applicable Data Protection Laws.
12. “**Sensitive Data**” means Personal Data that is protected under a special law or regulation requiring 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 offenses; and/or (e) account passwords in unhashed form.
13. “**Solutions**” means Aurascape’s proprietary cybersecurity and IT management products which are made available to Customer from time to time by Aurascape under the Agreement, whether as a hosted software-as-a-service, an instance installed on site, installed on Customer’s private cloud or otherwise. Any such

“Solution” includes any applicable technical support and “add-ons” (in each case, as and to the extent expressly purchased by Customer), as well as any updates/upgrades made available by Aurascape.

14. “**Sub-processor**” means any natural or legal person, service provider or entity engaged by Aurascape to Process Personal Data under Aurascape’s supervision, within the meaning of the applicable Data Protection Laws.
 15. “**Supervisory Authority**” means the authority, entity or agency established in each applicable territory to implement, advise, investigate and/or enforce applicable Data Protection Laws.
 16. “**UK Addendum**” means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses of 21 March 2022, as issued by the Information Commissioner of the United Kingdom.
- 2. Roles of the Parties.** Customer authorizes Aurascape to Process Personal Data on Customer’s behalf for the purpose of providing the Solutions as further specified in Schedule 1 attached hereto. The Parties acknowledge and agree that in this regard (i) Customer is the Controller of Personal Data, (ii) Aurascape is the Processor of Personal Data, and (iii) providing the Solutions is the business purpose under the CCPA, where applicable.
- 3. Obligations of the Controller.**
1. **Compliance and Instructions.** Customer represents and warrants that it complies and will comply with applicable Data Protection Laws in its use of the Solutions and in accordance with its obligations as a Controller, and that it will be solely responsible for such compliance including, without limitation, the lawful Processing of Personal Data, the accuracy and quality of Personal Data, and the lawfulness of any instructions to Aurascape.
 2. **Provision of Personal Data.** Customer agrees that it will only provide Aurascape with the Personal Data necessary for Aurascape to provide the Solutions, and that Customer will not provide (or otherwise allow Aurascape to access) any Sensitive Data.
 3. **Data Subject and Supervisory Authority Requests.** Customer will be responsible for the exercise of any Data Subjects rights and all communications with any Supervisory Authority.
- 4. Obligations of the Processor.**
1. **Scope of Processing.** Aurascape will Process Personal Data on behalf of Customer only on documented instructions from Customer and for the purpose of providing the Solutions under the Agreement, and/or as required under the laws applicable to Processors, and/or as required by a court of competent jurisdiction or other competent governmental or semi-governmental authority, provided that Aurascape shall inform Customer of such legal requirement unless such notice is prohibited by law.
 2. **CCPA.** With respect to Personal Information to which the CCPA applies: (i) Aurascape acknowledges and confirms that it will not receive or Process any Personal Information as consideration for the Solutions; (ii) Aurascape shall not have, derive, or exercise any rights or benefits regarding Personal Information Processed on Customer’s behalf; (iii) Aurascape certifies that it understands the rules, requirements and definitions of the CCPA, and will refrain from selling or sharing (as such terms are defined in the CCPA) any Personal Information Processed hereunder without Customer’s prior written consent; (iv) Aurascape shall not Process Personal Information for any purpose other than for the business purpose specified in this DPA or outside the business relationship provided in the Agreement, or combine Personal Information other than as permitted by the CCPA; and (v) Customer is enabled to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information.
 3. **Compliance.** Aurascape shall promptly inform Customer if, in its opinion, the execution of an instruction could violate any applicable Data Protection Laws, or when any applicable law or legal requirement prevents Aurascape from fulfilling its obligations under this DPA or from complying with the instructions received from Customer. As a result, Aurascape may in part or as a whole, without liability to Customer, suspend the Processing of Personal Data until such issue has been resolved. If the Parties do not agree on a resolution to the issue within a reasonable period of time, not to exceed sixty (60) calendar days, each Party may, as its sole remedy, terminate the applicable provisions of the Agreement and this DPA, in each case to the limited extent necessary to eliminate the affected Processing.
 4. **Cooperation and Data Subject Requests.** Where required by applicable Data Protection Laws and in particular by articles 32 to 36 of the GDPR, Aurascape shall provide cooperation and assistance to Customer in fulfilling its legal obligations, including responding to Data Subjects’ requests for exercising data protection rights, the adoption of appropriate security measures, responding to a Data Breach, performing data protection impact assessments or consulting with or responding to a Supervisory Authority’s requests. Aurascape shall, to the extent legally permitted and required, promptly inform Customer if Aurascape receives a request from a Data Subject to exercise their rights or a request from a Supervisory Authority directed to Customer.
 5. **Government Requests.** Where permitted by applicable laws, Aurascape shall promptly inform Customer if it receives a legally binding request from a governmental or law enforcement authority, including judicial authorities, relating to the Processing of Personal Data under this DPA, and shall review the legality of such request. If, after careful assessment, Aurascape concludes that there are reasonable grounds to believe that the request is unlawful under applicable Data Protection Laws or any other applicable laws, Aurascape shall use commercially reasonable efforts where possible to challenge the request and seek interim measures,

where appropriate, to suspend the effects of the request until the competent judicial authority has decided on its merits. In any event, Aurascape shall not disclose Personal Data requested until required to do so under the applicable procedural rules. When responding to such a request for disclosure, Aurascape shall only provide the minimum amount of Personal Data permissible based on a reasonable interpretation of the request.

6. **Data Security.** Aurascape shall maintain technical and organizational measures for the protection of Personal Data appropriate to the nature, scope, context, risks and purposes of the Processing thereof, including those measures set forth in Schedule 2 attached hereto.
7. **Confidentiality.** Aurascape shall ensure that its personnel engaged in the Processing of Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation and are properly instructed on Personal Data Processing in accordance with applicable Data Protection Laws.

5. Sub-processors.

1. **Appointment of Sub-processors.** Customer acknowledges and agrees that Aurascape may engage Sub-processors to Process Personal Data in connection with the provision of the Solutions. A list of Aurascape's current Sub-processors is located at www.aurascape.ai/subprocessor-list and, as of the Effective Date, is hereby deemed authorized. Aurascape will provide notification of any new Sub-processor(s) at least thirty (30) calendar days before authorizing any such new Sub-processor(s) to Process Personal Data. To receive such notifications, Customer shall sign up at [subprocessor-list](http://www.aurascape.ai/subprocessor-list).
2. **Objections.** To object to a new Sub-processor, Customer shall notify Aurascape in writing within fifteen (15) calendar days of receipt of the notification of such Sub-processor's planned engagement, setting forth the reasonable data protection grounds for the objection. In response to any such objection, Aurascape undertakes to provide Customer with evidence of the new Sub-processor's safeguards and its compliance with applicable Data Protection Laws. If Aurascape is unable to provide such evidence within a reasonable time period, the Parties will work together in good faith to resolve the remaining ground for the objection, and if such common effort fails, Customer may terminate the applicable provisions of the Agreement and this DPA, in each case to the limited extent necessary to eliminate the affected Processing, by providing written notice to Aurascape.
3. **Agreement with Sub-processors.** Aurascape will enter into written agreements with each Sub-processor containing substantially similar data protection obligations as set out in this DPA, including obligations to implement appropriate technical and organizational measures in accordance with applicable Data Protection Laws. Aurascape shall remain responsible to Customer hereunder if a Sub-processor fails to fulfill its data protection obligations concerning its Processing of Personal Data.

6. Cross-border Data Transfers.

1. **Transfers by Customer.** The Parties agree that if Customer transfers Personal Data to Aurascape within the scope of this DPA from European Union (the "EU") member states and/or the three other European Economic Area member countries (Norway, Liechtenstein and Iceland) (collectively, the "EEA"), Switzerland or the United Kingdom (the "UK") to countries which have not been subject to an adequacy decision published by the European Commission or any other relevant data protection authority of the EEA, the EU, the EU member states, Switzerland, and/or the UK ("**Adequacy Decision**"): (i) the terms set forth in Part 1 of Schedule 3 attached hereto shall apply to any such transfer from the EEA ("**EEA Transfer**"); (ii) the terms set forth in Part 2 of Schedule 3 attached hereto shall apply to any such transfer from the UK ("**UK Transfer**"); (iii) the terms set forth in Part 3 of Schedule 3 attached hereto shall apply to any such transfer from Switzerland ("**Swiss Transfer**"); and (iv) the terms set forth in Part 4 of Schedule 3 attached hereto shall apply to any such transfers.
2. **Transfers by Aurascape.** Personal Data may be transferred by Aurascape from the EEA, Switzerland or the UK to: (i) countries that offer an adequate level of data protection under or pursuant to an Adequacy Decision, as applicable, without any further safeguard being necessary; and/or (ii) other countries provided that Aurascape puts in place an alternative recognized compliance mechanism for the lawful transfer of Personal Data pursuant to applicable Data Protection Laws (e.g., EU SCCs, UK Addendum).

7. Data Breach Management.

1. **Notification.** Aurascape shall notify Customer of any Data Breach of Personal Data Processed by Aurascape on behalf of Customer of which Aurascape becomes aware, without undue delay and consistent with the measures necessary to determine the scope of the breach as required by applicable Data Protection Laws. Aurascape will use commercially reasonable efforts to investigate the Data Breach and take actions that are reasonably necessary in an effort to remediate and/or mitigate the Data Breach, in each case as required by applicable Data Protection Laws and as appropriate under the circumstances. The obligations set forth herein do not apply to incidents caused by Customer or anyone using the Solutions on Customer's behalf.
2. **Disclosure.** Customer will not make, disclose, release or publish any finding, admission of liability, communication, notice, press release or report concerning any Data Breach, which directly or indirectly identifies Aurascape (including in any legal proceeding or in any notification to Data Subjects, Supervisory Authorities, and/or any other applicable authority or entity), without Aurascape's prior written approval,

unless, and solely to the extent that, Customer is compelled to do so pursuant to applicable Data Protection Laws. In any such case, (i) unless prohibited by applicable laws, Customer shall provide Aurascape with reasonable prior written notice to give Aurascape the opportunity to object to such disclosure, and (ii) Customer will limit the disclosure to the minimum scope legally required.

8. **Audits.** Following Customer's thirty (30) calendar days prior written requests, but no more often than once every twelve (12) months (except in the event of a Data Breach), and subject to strict confidentiality undertakings by Customer, Aurascape shall (i) make available to Customer information necessary to demonstrate compliance with this DPA, and (ii) allow for and reasonably contribute to records audits conducted by a mutually-agreed accredited third-party auditor acting on Customer's behalf and at Customer's expense to enable Customer to verify Aurascape's compliance with its obligations under this DPA. Any such audits will be carried out at mutually agreed times during regular business hours, and Customer shall ensure that it and its auditors will not cause any damage, injury or disruption to Aurascape's premises, equipment, personnel and business while conducting such audits. Upon Aurascape's request, Customer shall return, or cause to be returned, all records and/or documentation provided by or on behalf of Aurascape in the context of any such audit(s).
9. **Return and/or Deletion of Personal Data.** Customer's deployed Solution instance(s) shall be promptly disabled following the termination/expiration of Customer's license subscriptions to such Solutions under the Agreement. Following Customer's written request, Aurascape shall either return or delete any Personal Data Processed by Aurascape solely on behalf of Customer which at the time of such written request still remains available to Aurascape if any (in each case, unless (i) such deletion is otherwise prohibited by applicable laws, and/or (ii) further retention is required or permitted by applicable laws or is otherwise agreed to by the Parties in writing, including pursuant to the Agreement). To the extent and for so long as any such Personal Data continues to be so retained by Aurascape, such retention and any further necessary Processing shall be performed in accordance with the obligations set forth in this DPA.
10. **Miscellaneous.**
 1. **Incorporation of Agreement Terms.** Subject to Section 10.2 below, all of the terms and conditions of the Agreement that are applicable to this DPA are hereby incorporated herein by reference, *mutatis mutandis*, including without limitation any confidentiality, effective duration, termination, indemnification, exclusions and limitations of liability, and general/miscellaneous terms.
 2. **Hierarchy.** 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.

Schedule 1 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

1. Providing the Solutions to Customer in accordance with the Agreement, this DPA and Customer's instructions.
2. Complying with applicable laws and regulations.

Duration of Processing

Aurascape will Process Personal Data for the effective duration of the Agreement and Customer's license subscriptions to Aurascape Solutions thereunder, as well as any further period either required or permitted by applicable laws or agreed to by the Parties in the Agreement and/or this DPA.

Types of Personal Data

Customer may submit Personal Data to the Solutions, the extent of which is determined and controlled by Customer in its sole discretion. More specifically, the following categories of Personal Data may be Processed:

1. Business Contact Data, including full name, employer or Customer name, Customer department, Customer address, e-mail address, mobile phone number and/or job title (Identifiers).
2. Communication Data, including Personal Data contained in correspondence with Aurascape, support tickets, history of interactions with Aurascape, chats, surveys, feedbacks and analyses thereof (Electronic Network Activity Information, Commercial Information, and related Inferences).
3. Asset (e.g., Device, User, SaaS Application, etc.) Identifiers, including user, device and SaaS ID, log in, IP address, device/browser/applications/operating system/browser extension identifiers (e.g., version, type, etc.), approximate

geolocation, locale and language settings used, network activity metadata (e.g., accessed domain, time, etc.) (Identifiers, Electronic Network Activity Information, and related Inferences).

No Sensitive Data may be submitted by Customer.

Categories of Data Subjects

Customer may transmit Personal Data to the Solutions relating to the following categories of Data Subjects: Customer's employees and users who use Customer's network.

Schedule 2 - TECHNICAL AND ORGANIZATIONAL MEASURES

Aurascape maintains a formal cybersecurity program to safeguard the Processing of Personal Data. The program is structured according to the ISO 27001 standards and is certified on a regular basis by independent external auditors for compliance with ISO 27001 or an equivalent cybersecurity management framework. The program enables Aurascape to establish comprehensive and risk-informed security measures that span the following areas and address the confidentiality and integrity of Personal Data:

1. **Physical Security:** Aurascape maintains appropriate physical security measures to protect tangible items, such as physical computer systems and devices, that Process Personal Data.
2. **Logical Access Controls:** Aurascape restricts access to Personal Data and related logical infrastructure and applications using formal authentication and authorization measures. Whenever practical, Aurascape relies on Single Sign-On to validate the identities of its personnel when deciding whether to grant access. Aurascape deploys firewalls and other relevant security measures to protect its networks from unauthorized access.
3. **Application:** Aurascape incorporates security requirements and guidance into its Software Development Lifecycle to mitigate the risks associated with inappropriate access to or other misuse of Personal Data through the Solutions. Aurascape conducts annual security reviews of the Solutions to identify and help address vulnerabilities.
4. **Data:** Aurascape uses modern encryption techniques to safeguard the transfer and storage of Personal Data wherever practical.
5. **Personnel:** Aurascape screens its personnel in accordance with local laws and regulations, taking into account the business requirements of the role, the classification of the Personal Data the employee will regularly access, and the perceived risks. Aurascape informs its personnel about Aurascape's cybersecurity program and the role they play in it.
6. **Sub-processors:** Aurascape uses third-party cloud infrastructure and software-as-a-service providers for certain aspects of the Solutions. Aurascape reviews these Sub-processors' cybersecurity practices according to its vendor review program to confirm that they provide sufficient safeguards to protect Personal Data.
7. **Agentic AI Data Handling and Retention Controls:** Aurascape includes an agentic artificial intelligence assistant ("Auri") as part of certain Solution capabilities. Where Auri is enabled, the following safeguards apply:
 - **Default Configuration:** Auri is designed to operate with zero data retention. By default, no Personal Data submitted during interactions with Auri is stored or retained by Aurascape.
 - **Optional Model Configuration:** Customers may configure Auri to access large language models ("LLMs") through either (i) an API key provisioned by the Customer, or (ii) an API key provisioned by Aurascape. In either case, the designated LLM provider acts as a Data Processor for purposes of Processing any submitted Personal Data.
 - **Retention Assurance:** Where an Aurascape-provisioned key is used, both Aurascape and the applicable LLM provider enforce a zero-retention policy with respect to such Personal Data, in accordance with their respective roles as Data Processors and consistent with applicable Data Protection Laws.

Schedule 3 – CROSS BORDER TRANSFERS

Part 1 – EEA Transfer

The Parties agree that the terms of the EU SCCs are herein incorporated by reference and shall apply to any EEA Transfer, with the following specifications:

1. Module Two (Controller to Processor) shall apply where the EEA Transfer is effectuated by Customer as the Controller of the Personal Data and Aurascape is the Processor of the Personal Data.
2. Clause 7 (Docking Clause): shall not apply.
3. Clause 9 (Use of sub-processors): Option 2: GENERAL WRITTEN AUTHORISATION shall apply, and the method for appointing and time period for prior notice of Sub-processor changes shall be as set forth in the DPA.
4. Clause 11 (Redress): the optional language will not apply.
5. Clause 17 (Governing law): Option 1 shall apply and the governing law is the law of the Republic of Ireland.
6. Clause 18 (Choice of forum and jurisdiction), lett. (b): the elected forum is the courts of the Republic of Ireland.
7. Annex I.A (List of parties) shall be completed as follows:

Data Exporter: Customer.

Contact details: As detailed in the Agreement.

Data Exporter Role: Controller.

Activities relevant to the data transferred: As detailed in Schedule 1 of the DPA.

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

Data Importer: Aurascape.

Contact details: grc@aurascape.ai.

Data Importer Role: Processor.

Activities relevant to the data transferred: As detailed in Schedule 1 of the DPA.

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

8. Annex I.B (Description of the transfer) shall be completed as follows:

Categories of data subjects whose data is transferred: As detailed in Schedule 1 of the DPA.

Categories of personal data transferred: As detailed in Schedule 1 of the DPA.

Frequency of the transfer: Continuous.

Nature of the processing: As detailed in Schedule 1 of the DPA.

Purpose of the data transfer and further processing: As detailed in Schedule 1 of the DPA.

Period for which the personal data will be retained: As detailed in Schedule 1 of the DPA.

For transfers to Sub-processors, the subject matter, nature, and duration of the processing are as set forth in Schedule 1 of the DPA.

9. Annex I.C (Competent supervisory authority) shall be completed as follows:

The competent supervisory authority in accordance with Clause 13 is the supervisory authority stipulated in Clause 18.

10. Annex II (Technical and organizational measures): As detailed in Schedule 2 of the DPA.
11. To the extent there is any conflict between the EU SCCs and any other terms in this Part 1, the DPA or the Agreement, the provisions of the EU SCCs will prevail.

Part 2 – UK Transfer

The Parties agree that the terms of the UK Addendum are herein incorporated by reference and shall apply to any UK Transfer, with the following specifications:

1. Table 1 shall be completed with the Parties, as stipulated in Section 7 of Part 1 of this Schedule 3.
2. Table 2 shall be completed with the EU SCCs, Modules and Selected Clauses, as stipulated in Part 1 of this Schedule 3.
3. Table 3 shall be completed with the EU SCCs Annexes Information (Appendix Information), as stipulated in Part 1 of this Schedule 3.
4. Table 4 shall state that neither Party may end the UK Addendum in the manner set out in Section 19 of the UK Addendum.
5. The Alternative Part 2 Mandatory Clauses of the UK Addendum shall apply, 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 Transfer

The Parties agree that the EU SCCs as detailed in Part 1 of this Schedule 3 shall be adjusted as set out below where the FADP applies to Swiss Transfers:

1. references to the EU SCCs 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 3;
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; and
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 Transfers are subject to the FADP.

Part 4 – Additional Safeguards

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:

- 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 Processor 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.
- 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 UK GDPR, including under section 702 of the United States Foreign Intelligence Surveillance Act (“FISA”).
- If the Processor becomes aware that any governmental 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 governmental 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 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
 - 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 availability. 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 an event, the Processor shall notify the Controller promptly following the access by the government authority, and provide the Controller with relevant details of the same, unless the Processor is legally prohibited from doing so.

Following the Controller’s written requests, but no more often than once every twelve (12) months, the Processor will inform the Controller of the types of binding legal demands for Personal Data it has received (if any) during the twelve (12)-month period preceding the Controller’s inquiry, including national security orders and directives, which shall encompass any process issued under section 702 of FISA.