

Data Processing Addendum

This Data Processing Addendum (“**DPA**”) forms part of and supplements the existing customer agreement (“**Agreement**”) between ZeroDrift, Inc. (“**ZeroDrift**”), and the counterparty to the Agreement (“**Customer**”). If any conflict arises between this DPA and the Agreement, this DPA prevails over the Terms; the Order Form prevails over both. Each party’s liability arising out of or related to this DPA is subject to the limitation of liability section of the Agreement. Capitalized terms used in this DPA that are not otherwise defined will have the meanings given to them under the Agreement or applicable Data Protection Laws, whichever is more protective of Personal Data.

Customer and ZeroDrift agree as follows:

1. **Definitions.** For purposes of this DPA:

- 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. “**Approved Data Transfer Mechanisms**” means, as applicable, the SCCs, the UK Addendum, or any data transfer mechanism a supervisory authority approves under Data Protection Laws that is incorporated into this DPA.
- c. “**Data Protection Laws**” means all applicable laws, regulations, and other legal or self-regulatory requirements in any jurisdiction relating to privacy, data protection, data security, breach notification, or the Processing of Personal Data, including without limitation, to the extent applicable, the General Data Protection Regulation, Regulation (EU) 2016/679 (“**GDPR**”) (including, for purposes of this DPA, the United Kingdom Data Protection Act of 2018 and as amended by the Data Protection, Privacy and Electronic Communications Act (Amendments etc.) (EU Exit) Regulations 2019), and the Swiss Federal Act on Data Protection (“**FADP**”); and the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* (“**CCPA**”), including its regulations and the amendments made by the California Privacy Rights Act of 2020 (“**CPRA**”), the Virginia Consumer Data Protection Act (“**VCDPA**”), the Colorado Privacy Act and related regulations (“**CPA**”), the Utah Consumer Privacy Act (“**UCPA**”), and the Connecticut Act Concerning Personal Data Privacy and Online Monitoring (“**CTDPA**”) (collectively, beginning with the CCPA, the “**U.S. Privacy Laws**”). For the avoidance of doubt, if a Party’s activities involving Personal Data are not within the scope of a given Data Protection Law, such law is not applicable for purposes of this DPA.
- d. “**Personal Data**” includes “personal data,” “personal information,” “personally identifiable information,” and analogous terms, as defined by Data Protection Laws, that ZeroDrift Processes in relation to the Agreement.
- e. “**Process**” and its cognates “**Processing**,” “**Processed**,” etc. mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- f. “**SCCs**” means Module 2 (Transfer: Controller to Processor) of the standard contractual clauses set out in the European Commission Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries according to GDPR.
- g. “**Security Breach**” means any confirmed unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

- h. **"Services"** means the services that ZeroDrift performs on behalf of Customer pursuant to the Agreement.
- i. **"Sub-processor"** means any third party or ZeroDrift Affiliate that ZeroDrift engages to Process Personal Data.
- j. **"UK Addendum"** means the United Kingdom International Data Transfer Addendum to the SCCs issued by the United Kingdom's Information Commissioner's Office.
- k. The terms **"Business," "Consumer," "Controller," "Data Subject," "Processor,"** and **"Service Provider"** are defined as in Data Protection Laws. "Controller" is deemed to also refer to "Business," and "Processor" is deemed to also refer to "Service Provider." "Data Subject" is deemed to include "Consumer."

2. Roles of the Parties; Scope and Purposes of Processing

- a. Unless otherwise specified, this DPA applies to all Personal Data that ZeroDrift Processes in relation to the Agreement.
- b. To the extent that Customer is the Controller of Personal Data, ZeroDrift is its Processor. To the extent that Customer is a Processor of Personal Data, ZeroDrift is its Sub-processor.
- c. ZeroDrift will Process Personal Data solely: (1) to fulfill its obligations to Customer under the Agreement, including this DPA; (2) on Customer's behalf; and (3) in compliance with Data Protection Laws. ZeroDrift will:
 - i. not retain, use, or disclose Personal Data outside of the direct business relationship between Customer and ZeroDrift, and not use Personal Data to train ZeroDrift's base models (if Customer uses Training Studio, ZeroDrift trains a model adapter for Customer from the policy documents, conversations and examples Customer provides, and that adapter is used only for Customer);
 - ii. not "sell" any Personal Data, as such term is defined in U.S. Privacy Laws (regardless of whether any such laws apply);
 - iii. not "share" any Personal Data, as such term is defined in the CCPA (regardless of whether the CCPA applies);
 - iv. comply with any applicable restrictions under Data Protection Laws on combining Personal Data with personal data that ZeroDrift receives from, or on behalf of, another person or persons, or that ZeroDrift collects from any interaction between it and any individual;
 - v. not attempt to re-identify any pseudonymized or otherwise de-identified Personal Data received from Customer without Customer's express written permission;
 - vi. not otherwise engage in any Processing of Personal Data that is prohibited or not permitted by Processors or Service Providers under Data Protection Laws; and
 - vii. provide the same level of privacy protection for Personal Data subject to the CPRA as the CPRA requires.

3. Personal Data Processing Requirements. ZeroDrift will:

- a. Ensure that the persons it authorizes to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

- b. Assist Customer in the fulfillment of Customer's obligations to respond to verifiable requests by Data Subjects (or their lawful representatives) for exercising their rights under Data Protection Laws (such as rights to access or delete Personal Data).
- c. Promptly notify Customer of any Data Subject requests to exercise their rights under Data Protection Laws with regard to the Personal Data or any government request for access to or information about Customer's Processing of Personal Data on Customer's behalf (collectively, "**Personal Data Request**"), unless prohibited by applicable law from making such notification. Unless otherwise required by applicable law, if ZeroDrift receives a Personal Data Request, ZeroDrift will await written instructions from Customer on how, if at all, to assist in responding. ZeroDrift will provide Customer with reasonable cooperation and assistance in relation to any Personal Data Request.
- d. Solely to the extent that such Processing activities are within ZeroDrift's control and directly relate to the Services, ZeroDrift will provide reasonable assistance to and cooperation with Customer for Customer's (i) performance of a data protection impact assessment of Processing or proposed Processing of Personal Data, when required by Data Protection Laws; and/or (ii) consultation with regulatory authorities in relation to the Processing or proposed Processing of Personal Data, including complying with any applicable obligation upon ZeroDrift to consult with a regulatory authority in relation to ZeroDrift's Processing or proposed Processing of Personal Data.

4. Data Security

ZeroDrift will implement appropriate administrative, technical, physical, and organizational measures to protect Personal Data, as set forth in Annex II. ZeroDrift maintains a SOC 2 Type II report and ISO 27001 certification and will make its current report or certificate available to Customer on request, subject to the confidentiality terms of the Agreement.

5. Security Breach

ZeroDrift will notify Customer of any Security Breach promptly, and in any event within 72 hours after becoming aware of such Security Breach. ZeroDrift will comply with the Security Breach-related obligations directly applicable to it under Data Protection Laws and will assist Customer in Customer's compliance with its Security Breach-related obligations, including without limitation by:

- a. At ZeroDrift's own expense, taking steps to mitigate the effects of the Security Breach and reduce the risk to Data Subjects whose Personal Data was involved; and
- b. Providing Customer with the following information, to the extent known:
 - i. The nature of the Security Breach, including, where possible, how the Security Breach occurred, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;
 - ii. The likely consequences of the Security Breach; and
 - iii. Measures taken or proposed to be taken by ZeroDrift to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects.

6. Sub-processors

- a. Customer acknowledges and agrees that ZeroDrift may use Sub-processors to Process Personal Data in accordance with the provisions within this DPA and Data Protection Laws. Where ZeroDrift sub-contracts any of its rights or obligations concerning Personal Data to a Sub-processor, ZeroDrift will: (i) take steps to select and retain Sub-processors that are capable of maintaining appropriate privacy and security measures to protect Personal Data consistent

with Data Protection Laws; and (ii) enter into a written agreement with each Sub-processor requiring it to comply with obligations at least as restrictive as those imposed on ZeroDrift under this DPA.

- b. ZeroDrift will maintain an up-to-date list of its Sub-processors at <https://trust.zerodrift.ai/subprocessors>. The initial list is provided in Annex III of this DPA, and Customer consents to ZeroDrift's use of the Sub-processors on this list. To the extent required by applicable Data Protection Laws, ZeroDrift will provide Customer notice of any new Sub-processor by email and by updating that page, and will allow Customer thirty (30) days, beginning the day ZeroDrift gives such notice, to object to such appointment. If Customer has legitimate objections to the appointment of a new Sub-processor, ZeroDrift will work with Customer in good faith to resolve the grounds for the objection.

7. Data Transfers

- a. In the event that ZeroDrift Processes Personal Data transferred from the European Union, the European Economic Area and/or its member states, and/or Switzerland (collectively, "EEA") and/or the United Kingdom to countries that do not ensure an adequate level of data protection within the meaning of the Data Protection Laws of those territories, Sections 7(b) and 7(c) of this DPA (and, for Switzerland, Annex IV) apply. ZeroDrift stores Personal Data in the United States. Sub-processors listed in Annex III may process Personal Data in other locations, subject to the Approved Data Transfer Mechanisms.
- b. The SCCs apply to a transfer of Personal Data under this DPA from the EEA between Customer and ZeroDrift. Customer agrees the SCCs are completed and supplemented as follows:
 - i. Customer is the data exporter and ZeroDrift is the data importer;
 - ii. The optional docking clause under Clause 7 of the SCCs will not apply;
 - iii. option 2 under Clause 9 of the SCCs applies and Customer generally authorizes ZeroDrift to engage Sub-processors according to Section 6 of this DPA;
 - iv. the optional redress language under Clause 11(a) of the SCCs will not apply;
 - v. the governing law under Clause 17 of the SCCs will be Ireland;
 - vi. the choice of forum and jurisdiction under Clause 18 of the SCCs will be the courts of Ireland;
 - vii. Annexes I, II and III of the SCCs are deemed to be populated with the information set out in Annexes I, II and III of this DPA; and
 - viii. Annex IV of this DPA supplements the SCCs with additional clauses as described therein.
- c. The UK Addendum applies to a transfer of Personal Data under this DPA from the United Kingdom between Customer and ZeroDrift, Customer agrees the UK Addendum is completed and supplemented as follows:
 - i. Customer is the data exporter and ZeroDrift is the data importer;
 - ii. Table 1 of the UK Addendum is deemed to be populated with the information set out in Annex I of this DPA;

- iii. for the purposes of Table 2 of the UK Addendum, the version of the “Approved EU SCCs” (including the appendix information, modules and selected clauses) appended to the UK Addendum is the SCCs;
 - iv. the optional docking clause under Clause 7 of the SCCs will not apply;
 - v. option 2 under Clause 9 of the SCCs applies and Customer generally authorizes ZeroDrift to engage Sub-processors according to Section 6 of this DPA;
 - vi. the optional redress language under Clause 11(a) of the SCCs will not apply;
 - vii. Annex IV of this DPA supplements the SCCs with additional clauses as described therein;
 - viii. Table 3 of the UK Addendum is deemed to be populated with the information set out in Annexes I, II and III of this DPA;
 - ix. The “importer” and “exporter” option applies for the purposes of Table 4 of the UK Addendum;
 - x. under Part 2, the mandatory clauses of the UK Addendum will apply; and
 - xi. by using the Services to transfer Personal Data to ZeroDrift, Customer will be deemed to have signed the UK Addendum.
- d. The terms applicable to the transfer of Personal Data under this DPA from any other country or region are listed in Annex IV of this DPA and are hereby incorporated into this DPA.

8. Audits

ZeroDrift will provide Customer with all such information as may be reasonably requested by Customer from time to time with regard to ZeroDrift’s compliance with this DPA. Customer may conduct an audit to confirm ZeroDrift’s compliance with this DPA by submitting a data protection questionnaire of reasonable length not more than once annually. ZeroDrift shall promptly complete and return such questionnaire to Customer. To the extent Customer is able to demonstrate that ZeroDrift’s questionnaire responses do not provide sufficient information to demonstrate compliance with this DPA, Customer may conduct follow up interviews with ZeroDrift’s personnel as needed.

9. Return or Destruction of Personal Data

Except to the extent required otherwise by Data Protection Laws, ZeroDrift will, at the choice of Customer, return to Customer and/or securely destroy all Personal Data upon (a) written request of Customer or (b) termination of the Agreement, in each case within 30 days, except for the data that Annex I permits ZeroDrift to keep for longer periods (product audit logs, application and infrastructure logs, backups, and account and billing records), which ZeroDrift will delete at the end of the applicable period and will continue to protect under this DPA until then. Except to the extent prohibited by Data Protection Laws, ZeroDrift will inform Customer if it is not able to return or delete Personal Data.

10. Survival

The provisions of this DPA survive the termination or expiration of the Agreement for so long as ZeroDrift or its Sub-processors Process Personal Data.

* * *

Annex I

APPROVED DATA TRANSFER MECHANISM: DESCRIPTION OF PROCESSING AND TRANSFER

A. LIST OF PARTIES

MODULE TWO: Transfer Controller to Processor

Data exporter(s):

- *Name:* Customer, as identified in the Agreement.
- *Address:* As provided in the Agreement.
- *Contact person's name, position, and contact details:* As provided in the Agreement.
- *Activities relevant to the data transferred under these Clauses:* The data exporter receives the data importer's Services pursuant to their underlying Agreement.
- *Signature and date:* The Parties agree that execution of the Agreement shall constitute execution of these SCCs by both parties.
- *Role:* Controller and/or Processor

Data importer(s):

- *Name:* ZeroDrift, as identified in the Agreement.
- *Address:* As provided in the Agreement.
- *Contact person's name, position, and contact details:* As provided in the Agreement.
- *Activities relevant to the data transferred under these Clauses:* The data importer provides Services to the data exporter pursuant to their underlying Agreement.
- *Signature and date:* The Parties agree that execution of the Agreement shall constitute execution of these SCCs by both parties.
- *Role:* Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer Controller to Processor

- *Categories of data subjects whose personal data is transferred:* The Personal Data transferred concerns the following categories of data subjects:
 - Customer's employees and personnel who use the Services
 - Customer's clients and prospective clients whose information appears in communications submitted for compliance review
 - Third parties whose information appears in communications submitted to the Services for compliance checking
 - End users of Customer's products and AI agents (e.g. candidates, applicants, consumers)

- *Categories of personal data transferred:* The Personal Data transferred concern the following categories of data:
 - Names and contact information of Customer personnel
 - Email addresses, names and other identifiers that Customer includes in message content or the API metadata field; and, for messages submitted through ZeroDrift's email intake feature, the sender, recipients and subject line (read to provide the Services but not stored in ZeroDrift's database) and the sender's email address (recorded in application logs)
 - Content of business communications submitted for compliance checking (email body and subject lines, PDF text)
 - Chat and messaging content (e.g. SMS, WhatsApp, in-app chat)
 - Client identifiers that may appear in communications (such as account numbers and balances)
 - Employee job titles and organizational roles
 - Authentication credentials and account access information
 - Names and email addresses of Customer's users
 - Login records, including IP address, device and approximate location
 - Attachment files received through ZeroDrift's email intake feature
 - Documents synced from sources Customer connects to the Services
 - Data Customer provides for model training or audit
 - Personal data contained in policy documents that Customer provides for Training Studio, if Customer uses that feature
- *Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:* Only where the Order Form permits it, processed only to provide the Services, with need-to-know access. Customer will not submit special categories of personal data or protected health information unless the Order Form expressly permits it and the parties have signed any agreement the law requires for that data, such as a business associate agreement (Section 3.5 of the Agreement's Terms).
- *The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):* Continuous for the duration of the Agreement.
- *Nature of the processing:* Data importer's Processing activities shall be limited to those discussed in the Agreement and the DPA.
- *Purpose(s) of the data transfer and further processing:* Processing customer communications (emails, documents, PDF files) to provide AI-powered compliance checking and advisory suggestions, by checking communications against applicable regulations and Customer's own rules, and training a model adapter used only for Customer.

- *The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:* Except as described below for attachment files, raw message content is not stored by ZeroDrift; it is processed to provide the Services and then discarded, except for temporary upload staging of up to 48 hours. Activity and evidence records (metadata, verdicts, the specific text identified as a potential issue, and suggested rewrites generated by ZeroDrift's own models) are kept according to Customer's retention setting, which includes the option of no storage, or, if Customer makes no selection, for the term of the Agreement plus 30 days. Evidence Pack exports are deleted within 30 days after the Agreement expires or terminates. Product audit logs are kept for the term of the Agreement plus 12 months, for security and dispute resolution. Application and infrastructure logs (including sender email addresses recorded by the email intake feature) are kept for up to 13 months. Backups are overwritten in the ordinary course within 35 days. Account and billing records are kept for 7 years after account closure. Training Studio adapters, and the policy documents used to train them, are deleted within 30 days after the Agreement expires or terminates. Data Customer provides for model training or audit is kept for the term of the Agreement and deleted within 30 days after it ends. Attachment files received through the email intake feature and documents synced from sources Customer connects to the Services are kept for the term of the Agreement plus 30 days. Third-party AI model providers listed in Annex III process message content to provide the Services and may retain it for up to 30 days for abuse monitoring.
- *For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:* Same as above to the extent that Personal Data is provided to Sub-processors for purposes of providing the Services.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer Controller to Processor

To the extent legally permitted, the competent supervisory authority is the Irish Data Protection Commission.

* * *

Annex II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer Controller to Processor

1. SCOPE

- a. **Security Policy.** ZeroDrift will comply with the information security requirements set forth in this Annex II ("**Security Policy**"). The Security Policy applies to ZeroDrift's performance under the Agreement and all access, collection, use, storage, transmission, disclosure, destruction or deletion of, and security incidents regarding all Personal Data. This Security Policy does not limit other obligations of ZeroDrift, including under the Agreement or any laws that apply to ZeroDrift, ZeroDrift's performance under the Agreement, the Personal Data or the Permitted Purpose.
- b. **Permitted Purpose.** ZeroDrift may collect, use, store and retain only the Personal Data that is expressly authorized under the Agreement, and then may only collect, use, store and retain that Personal Data solely as necessary for ZeroDrift to perform the Services in accordance with the Agreement ("**Permitted Purpose**"). In this Annex II, "Customer Data" means Personal Data and any other Customer Content (as defined in the Agreement) that ZeroDrift Processes under the Agreement.

2. REQUIREMENTS

- a. **ZeroDrift Security Policy.** ZeroDrift will implement and enforce a written information and network security policy for employees, subcontractors, agents, and suppliers that meets the requirements of this Annex II.
- b. **Basic Security Requirements.** ZeroDrift will, consistent with current industry standards, maintain physical, administrative and technical safeguards and other security measures (i) to maintain the security and confidentiality of Customer Data accessed, collected, used, stored or transmitted by ZeroDrift, and (ii) to protect that information from known or reasonably anticipated threats or hazards to its security and integrity, accidental loss, alteration, disclosure and all other unlawful forms of processing. Without limitation, ZeroDrift will comply with the following requirements:
 - i. **Firewall.** ZeroDrift will install and maintain a working network firewall or equivalent to protect data accessible via the Internet and will keep all Customer Data protected at all times. The firewall must provide both ingress and egress filtering, and have a default policy of blocking network traffic.
 - ii. **Updates.** ZeroDrift will keep its systems and software up-to-date with the latest upgrades, updates, bug fixes, new versions and other modifications necessary to ensure security of the Customer Data.
 - iii. **Anti-virus.** ZeroDrift will at all times use industry standard anti-virus software on endpoints and scanning technologies for the production environment, and regularly updated signature files, to ensure that all operating systems, software and other systems hosting, storing, processing, or that have access to Customer Data and are known to be susceptible or vulnerable to being infected by or further propagating viruses, spyware and malicious code, are and remain free from such viruses, spyware and malicious code. ZeroDrift will mitigate threats from all viruses, spyware, and other malicious code that are or should reasonably have been detected.
 - iv. **API Security.** ZeroDrift will use TLS 1.2 or higher encryption for all API requests and responses. API authentication will use secure token-based mechanisms with appropriate expiration and rotation policies.

- v. **Data Minimization.** ZeroDrift will only process input content necessary for compliance checking. The API has no sender, recipient or timestamp fields; anything Customer includes in the message body or metadata field is processed as Customer Data. For messages submitted through ZeroDrift's email intake feature, ZeroDrift reads the sender, recipients and subject line to provide the Services but does not store them in its database, records the sender's email address in application logs, and keeps the email's attachment files, each as described in Annex I.
- c. **Testing.** ZeroDrift will regularly test its security systems and processes to ensure they meet the requirements of this Security Policy.
- d. **Access Controls.** ZeroDrift will restrict access to Customer Data to only those people with a "need-to-know" for a Permitted Purpose.
- e. **Encryption.** ZeroDrift will encrypt Customer Data in transit and at rest using industry standard algorithms and methods, including when stored on portable media or portable devices.
- f. **Data Retention and Destruction.**
 - i. **Retention.** ZeroDrift will retain Customer Data only for the purpose of, and as long as is necessary for, the Permitted Purpose.
 - ii. **Return or Deletion.** ZeroDrift will promptly, and in any event within 30 days after Customer's request, return to Customer and permanently and securely delete all Customer Data upon and in accordance with Customer's notice requiring return and/or deletion. Also, ZeroDrift will permanently and securely delete all live (online or network accessible) instances of the Customer Data within 30 days after the earlier of completion of the Permitted Purpose or termination or expiration of the Agreement. These return and deletion obligations do not apply to data that Annex I permits ZeroDrift to keep for longer periods (product audit logs, application and infrastructure logs, backups, and account and billing records), which ZeroDrift will delete at the end of the applicable period.
- g. **Disaster Recovery / Business Continuity.** ZeroDrift will implement appropriate disaster recovery and business continuity plans that will ensure the availability, security, integrity, and (where necessary) restoration of the Customer Data on the occurrence of a business interruption event. ZeroDrift will provide a summary of its disaster recovery and business continuity plans to Customer upon request.
- h. **Security Incidents.** ZeroDrift will inform Customer without undue delay, and in any event, within 72 hours after becoming aware of any Security Breach. ZeroDrift will remedy each Security Breach in a timely manner and provide Customer written details regarding ZeroDrift's internal investigation regarding each Security Breach.

* * *

Annex III

LIST OF SUB-PROCESSORS

The current list of Sub-processors is available at <https://trust.zerodrift.ai/subprocessors>.

Annex IV

SUPPLEMENTAL CLAUSES

SWITZERLAND

The SCCs and as adapted and supplemented as set forth in this section will only apply to a transfer of Personal Data Processed under this DPA from Switzerland to ZeroDrift. Customer agrees that:

1. Any reference to “Member State” will not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland);
2. Any references to “personal data” extend to personal data of legal entities if and to the extent such personal data pertaining to legal entities is within the scope of the Swiss Federal Act on Data Protection (“**FADP**”); and
3. To the extent the transfer of personal data is governed by the FADP, the Swiss Federal Data Protection and Information Commissioner will act as the competent supervisory authority; to the extent the transfer of personal data is governed by the GDPR, the supervisory authority determined in Annex I(C) will act as the competent supervisory authority; any references to the “competent supervisory authority” will be interpreted accordingly.