

HIVEMQ DATA PROCESSING AGREEMENT

This Data Processing Addendum (“DPA”) is entered into as of the last date signed below, between the Customer listed in the signature box (“Customer”) and HiveMQ GmbH (EMEA Customer) or HiveMQ Inc. (non-EMEA Customer) (“Provider”) and forms part of the Enterprise Subscription Agreement (the “Agreement”) executed by the parties, provided that this DPA only applies to Customer’s purchase of Provider’s Cloud Service. This DPA does not apply to the Provider’s Self-Managed Service. Capitalized terms not defined herein shall have the meaning set forth in the Agreement.

DEFINITIONS

The terms “Data Breach”, “Data Controller”, “Data Processor”, “Data Subject”, “Personal Data/Personal Information”, “Process/Processing” and “Supervisory Authority” shall have the meaning set out under Data Protection Laws, or where not specifically defined under Data Protection Laws, the same meaning as analogous terms in those Data Protection Laws. For example: (i) where the EU GDPR or UK GDPR is applicable, “Data Controller” means the person or entity that determines the purposes and means of processing Personal Data, and where the CCPA is applicable includes any “business” as that term is defined by the CCPA, and (ii) where the EU GDPR or UK GDPR is applicable, “Data Processor” means an entity that processes Personal Data on behalf of a Data Controller, and where the CCPA is applicable includes any “service provider” or “contractor” as those terms are defined by the CCPA.

“**CCPA**” means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act, Cal. Civ. Code § 1798.100 et seq, and its implementing regulations.

“**Data Protection Laws**” means all US Privacy Laws and European applicable laws, regulations, or other legally binding obligations (including any and all legislative and/or regulatory amendments or successors thereto), including but not limited to, as applicable, EU Data Protection Laws, UK Data Protection Laws, and any other specifically stated jurisdictional law, that apply to the Processing of Personal Data in connection with the services provided by Provider under the Agreement.

“**EEA**” means European Economic Area.

“**GDPR**” means the General Data Protection 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.

“**Personal Data**” shall have the meaning set forth under Data Protection Laws but at minimum means data that can be used to directly or indirectly identify a Data Subject or household.

“**SCCs**” means the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and available on the official website of the European Union [here](#).

“**Subprocessor**” means any third-party entity engaged by Provider to Process Personal Data on Provider’s behalf in connection with the Provider Service.

“US Privacy Laws” means all laws relating to data protection, the processing of Personal Data, privacy and/or electronic communications in force from time to time in the United States at the federal or state level that apply to the Processing of Personal Data in connection with the services provided by Provider under the Agreement, including without limitation the CCPA; Colorado Privacy Act, Col. Rev. Stat. § 6-1-1301 et seq.; Connecticut Data Privacy Act, S.B. 6; Virginia Consumer Data Protection Act, S.B. 1392 § 59.1 et seq.; and Utah Consumer Privacy Act, S.B. 227.

“UK Data Transfer Addendum” means the international data transfer addendum to the EU SCCs issued by the UK Information Commissioner in accordance with section 119A of the UK Data Protection Act 2018, as amended or replaced from time to time by a competent authority under applicable DP Law.

All other defined terms used in this DPA will have the meanings set out in the Agreement between the parties.

PROCESSING OF PERSONAL DATA

IN GENERAL

Roles of the Parties. For the purposes of this DPA, Provider is a Data Processor of Customer’s Personal Data regardless of whether Customer is the Data Controller of such data or itself a Data Processor of such data on behalf of an Affiliate. With respect to CCPA, Provider is Customer’s “Service Provider.”

Details of Processing. The subject-matter and scope of the Processing is stated in Attachment 1 (Details of Processing) to this DPA and is incorporated herein.

USE & RESTRICTIONS

Business Purpose. Provider may Process Personal Data for the following business purposes: (i) performing services on behalf of Customer as more fully set forth in the Agreement; (ii) helping to ensure the security and integrity of the services; (iii) debugging the Services; (iv) maintaining the quality and safety of the services; (v) to the extent permitted by this DPA, to retain and employ other service providers as Sub-processors; and (vi) to detect data security incidents and protect against fraudulent or illegal activity.

Restrictions on Use of Personal Data. Provider shall not retain, use, disclose, or otherwise process Personal Data for any purpose other than the business purpose of providing the services or such other purpose permitted or required by Data Protection Laws, and Provider shall Process the Personal Data in accordance with this DPA, applicable Data Protection Laws, and the Agreement. Without limiting the foregoing, Provider shall not (i) combine the Personal Data received from or on behalf of Customer with the Personal Data Processed on behalf of Provider’s other customers; and (ii) otherwise Process Personal Data outside of the direct business relationship between Customer and Provider.

Additional Restrictions. In addition to the foregoing above, Provider shall not process California Personal Data in a manner that would constitute a Sale or a Share as such terms are defined under CCPA, or combine any California Personal Data with Personal Data that it receives from or on behalf of any other third party or its interactions with Consumers (as the term “Consumers” is defined under the CCPA), provided that Provider may do so for a Business Purpose (as that term is defined under the CCPA) if directed to do so by Customer or as otherwise expressly permitted by the CCPA. Nothing in the Agreement shall be construed as providing for the sale or transfer for valuable consideration of Personal Data to Provider.

De-Identified Data. Provider shall not attempt to re-identify any de-identified Personal Data and publicly commit to not doing so if requested by Customer.

Customer Responsibilities. Customer will comply with its obligations under Data Protection Laws, including providing any required notice to Data Subjects. Customer will not transmit Personal Data outside the scope of Attachment 1.

SECURITY AND RETENTION

DATA SECURITY

Security. Provider shall implement and maintain a written information security program that includes appropriate technical and organisational measures to safeguard Personal Data and ensure a level of security appropriate to the risk of processing personal data, taking into account the nature, scope, context and purposes of processing, in accordance with Data Protection Laws (“Information Security Program.”) Provider’s security terms and requirements are outlined in the Technical and Organizational Measures Addendum described in Attachment 2.

Training. Provider shall ensure that all authorized Provider personnel with access to Personal Data are subject to a duty of confidentiality (whether statutory or contractual) and provide such personnel with the appropriate privacy and security training to ensure that Provider maintains the requisite safeguarding and protection of Personal Data.

RETENTION

Duty to Delete, Destroy or Return. At the expiry or termination of the Agreement, or upon Customer’s request, Provider will safely delete, destroy or return all Personal Data set out in Attachment 1 to Customer, except where it is required to retain copies under Data Protection Laws.

Retention upon Termination. If Provider is required to retain Personal Data upon expiration or termination of the Agreement, Provider will only retain and Process such Personal Data as strictly necessary to comply with applicable laws, continue to remain subject to its obligations under this DPA, and securely delete the retained Personal Data once the retention is no longer necessary to comply with applicable laws.

USE OF SUBPROCESSORS

SUBPROCESSORS

Generally. Provider may retain Subprocessor to Process Personal Data to provide the services and fulfill its contractual obligations under the Agreement, provided (i) Provider will enter into a written contract with each Subprocessor that imposes terms as protective as those set out in applicable Data Protection Laws, this DPA, and the Agreement; and (ii) Provider remains liable for each Subprocessor’s acts and omissions to the same extent Provider would itself be liable under this DPA. A list of Provider’s current Subprocessors is available as Attachment 3.

New Sub-processors. Before any new Subprocessor processes Personal Data, Provider will notify Customer if they opt into receiving updates on the Provider’s Trust Center. If Customer reasonably objects to a new Subprocessor within 15 days of receiving notice, and if Provider cannot provide the Service without the Subprocessor, Customer may immediately terminate the Agreement and receive a prorated refund.

COMPLIANCE

COOPERATION

Data Subject Requests. Provider shall promptly notify Customer (and in no event later than forty-eight (48) hours) of receiving a request from a Data Subject and Provider will provide reasonable assistance to help Customer facilitate Data Subject requests it receives, including but not limited to a request concerning a Data Subject's rights to, as applicable: (i) delete, (ii) opt-out, (iii) correct, (iv) access and receive a copy of, and (v) limit the use of Personal Data. Provider will not respond to a Data Subject request directly, except to inform them of the nature of the relationship with Customer and redirect such requests, unless otherwise required by law or Customer provided prior written consent.

Compliance Assistance. Provider will cooperate and comply with all reasonable Customer instructions and requests in order for Customer to comply with its obligations under Data Protection Laws with respect to Data Subject Requests, data protection impact assessments, or supervisory authorities' inquiries.

Notification of Privacy Inquiries. If a competent judicial, government or other supervisory authority requires Provider to disclose Personal Data, Provider shall notify Customer in writing immediately but in no event later than forty-eight (48) hours of receipt of such request, so that Customer may seek to retain the confidentiality of the Personal Data. Provider shall cooperate with Customer to redirect the appropriate authority to request the Personal Data directly from Customer.

Audits. Upon request, Provider will provide Customer with a copy of its most recent third-party reports and additional relevant information. If such reports and information are not sufficient for Customer to meet its obligations under Data Protection Laws, Provider and Customer will mutually agree upon the scope, timing, and duration of an on-site inspection, which will be conducted at Customer's expense. Information arising from an on-site audit is Provider's Confidential Information.

PERSONAL DATA BREACHES AND PROCEDURE

Response Plan. In accordance with Data Protection Laws and industry standards, Provider shall implement a security incident response plan that includes procedures to be followed in the event of an actual or suspected Personal Data Breach. ("**Personal Data Breach**") means security threats that may lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

Breach Response and Remediation. In the event of a Personal Data Breach related to Customer Personal Data, Provider will notify Customer without undue delay (and in no event later than 48 hours) after becoming aware of a Personal Data Breach. The notification shall include: (i) a description of the nature of the Personal Data Breach; (ii) contact details for Provider's security and privacy representatives; and (iii) measures taken or proposed to be taken to mitigate the potential adverse effects. Provider shall investigate and analyze the cause and extent of such Personal Data Breach and develop plans to contain and remediate the Personal Data Breach and prevent its reoccurrence. Provider will provide assistance as required for Customer to comply with its obligations under Data Protection Laws and cooperate with Customer in any post-breach investigation, remediation, and communication efforts.

INTERNATIONAL TRANSFERS

Scope. In the event that Personal Data Processed by Provider is subject to restrictions under Data Protection Laws concerning international transfers of Personal Data, the Parties agree to take all necessary steps to provide the Personal Data with an adequate level of data protection during and after any such international data transfers in accordance with the requirements of the Data Protection Laws.

Transfers of Personal Data from the EEA. Personal Data transfers from the EEA to a non-adequate country will be Processed in accordance with the SCCs and the following (“**Transfer Clauses**”) shall apply

- i. Where Customer is the Controller and Provider is the Processors, Module 2 (Controller to Processor) shall apply.
- ii. where Customer is the Processors (acting on behalf of an Affiliate) and Provider is the Processors, Module 3 (Processor to Processor) shall apply.
- iii. The optional Clause 7 (Docking clause) does not apply.
- iv. Option 2 of Clause 9 (General Written Authorization) applies, and notice will be provided at least 15 days in advance.
- v. The optional provision under Clause 11(a) (Redress) does not apply.
- vi. Option 1 for Clause 17 (Governing law) shall be the law of the Republic of Ireland.
- vii. The Courts under Clause 18 (Choice of forum and jurisdiction) shall be the Courts of Germany.
- viii. The contents of Attachment 1 form Annex I—A. (List of Parties), B. (Description of Transfer) and C. (Competent Supervisory Authority)—to the SCCs.
- ix. The contents of Attachment 2 form Annex II — (Description of Technical and Organisational Measures)—to the SCCs.

Transfers of Personal Data from the United Kingdom (UK). Personal Data transfers from the UK to a non-adequate country, will be Processed in accordance with the Transfer Clauses, as amended in the “UK Addendum” attached hereto as Exhibit 1.

Transfers of Personal Data from Switzerland. Personal Data transfers from Switzerland to a non-adequate country, will be Processed in accordance with the Transfer Clauses, as amended in the “Swiss Addendum” attached hereto as Exhibit 2.

MISCELLANEOUS

Changes to Data Protection Laws. The parties will cooperate in good faith, in the event an applicable Data Protection Law becomes invalidated or replaced, the relevant Supervisory Authority establishes new transfer safeguards, or Data Protection Laws require any further steps to be taken to permit international transfers of Personal Data as contemplated under this DPA. Customer may suspend or require Provider to suspend any international transfers or Processing of Customer Personal Data that do not comply or that cease to comply with the provisions of this International Transfer Section and its related Attachments.

Order of Precedence. To the extent of any conflict between the Agreement and this DPA, this DPA will prevail. To the extent of any conflict between this DPA and the SCCs or the UK Addendum, the SCCs or UK Addendum will prevail.

Limitation of Liability. The parties' aggregate liability arising out of this DPA will be subject to the same limitations and exclusions of liability as apply under the Agreement, whether liability arises under the Agreement or this DPA.

Governing Law. Unless stated otherwise, this DPA will be construed in accordance with the governing law provision in the Agreement.

ATTACHMENT 1
ANNEX I
DESCRIPTION OF THE PROCESSING

A. LIST OF PARTIES

Data exporter(s):

Name:

Address:

Contact person's name, position, and contact details: Customer listed on Order Form

Activities relevant to the data transferred under these Clauses: Determining the subject-matter of the Processing and performing Processing operations as required to receive and use the Service pursuant to the Agreement.

Role: Controller

Signature and date: Accepted via online Order

Data importer(s):

Name: HiveMQ GmbH / HiveMQ Inc.

Address: c/o Mindspace Friedrichstr. 68 10117 Berlin, Germany or
600 N Broad Street, Suite 5, 553 Middletown DE 19709, USA

Contact person's name, position and contact details: privacy@HiveMQ.com

Activities relevant to the data transferred under these Clauses: Processing operations as required to provide the Service to the data exporter pursuant to the Agreement.

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects Whose Personal Data is Transferred:

The Categories of Data Subjects are individuals about whom Personal Data is provided to Provider by or at the direction of Customer as part of the Enterprise SaaS (Cloud Service), including employee, contractors and authorized users of Customer.

Categories of Personal Data Transferred:

The Categories of Personal Data provided to the Provider by or at the direction of Customer as part of the services including First name, Last Name, IP Address, and Work Email

Sensitive Data Transferred:

None

Frequency of the Transfer:

Continuous, depending on the Customer's use of the Services

Nature of the Processing:

The nature of the Processing is the provision of the Service pursuant to the Agreement

Purpose of the Data Transfer and Further Processing:

Provider will Process Personal Data as necessary to provide the Service pursuant to the Agreement

Duration of the Processing:

Provider will Process Personal Data for the duration of the Agreement.

Transfers to Subprocessors:

Transfers to Subprocessors is governed by Subprocessors Clause of this DPA. The subject-matter, nature, and duration of Processing by Subprocessors is as required for the data importer to provide Service.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority/ies in accordance with Clause 13

ATTACHMENT 2

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES

Measures of pseudonymisation and encryption of personal data

Provider pseudonymizes Personal Data where feasible and encrypts Personal Data at rest using AES-256 (or better) and in transit using TLS 1.2 (or better), supported by documented cryptographic key management procedures.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Provider ensures the ongoing confidentiality, integrity, availability, and resilience of the systems and services that Process Personal Data through role-based, need-to-know access controls, network segmentation, continuous monitoring and logging, regular data backups, and highly available, redundant infrastructure hosted across multiple certified cloud service providers (Microsoft Azure, Google Cloud Platform, and AWS).

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Provider maintains a security incident response policy, business continuity plan, and disaster recovery plan, supported by automated restorability tooling and continuous monitoring and reporting. Incident recovery plans are tested on a regular basis.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Provider's comprehensive security program, including its technical and organisational measures, is reviewed and updated at least annually to address changes to Provider's business and products, applicable laws, and the threat landscape. Provider continuously monitors its networks and systems for threats, including by regularly scanning for vulnerabilities, applying critical security patches through a formal patch management process, conducting internal penetration tests, and employing an intrusion detection system to detect malicious activity. Provider also maintains an internal audit program covering regular system, process, IT security, and data protection audits.

Measures for user identification and authorization

Authentication and authorization in the Enterprise SaaS (Cloud Service) are enforced through Customer-configured role-based access controls and single sign-on integrations. Provider employees are governed by "separation of duties" and "least privilege" principles, with use restrictions based on unique custom roles, centralized authorization and single sign-on (with hardware security key multi-factor authentication for privileged access), and automated detection and blocking of brute-force login attempts. Access permissions are reviewed at least quarterly, and user permissions are promptly revoked upon termination through a formal offboarding process.

Measures for the protection of data during transmission

Personal Data is encrypted in transit between Provider and Customer's systems over public networks using HTTPS/TLS 1.2 or better. Access to data in transit is authenticated and logged, and transmission activity is monitored to help ensure Personal Data reaches only its intended recipients.

Measures for the protection of data during storage

Customer Data at rest is encrypted using AES-256 or better, with encryption keys managed under Provider’s cryptographic key management procedures.

Measures for ensuring physical security of locations at which personal data are processed

Provider delivers its Cloud Service using certified cloud infrastructure providers (Microsoft Azure, Google Cloud Platform, and AWS), which maintain independently audited physical security controls at their data centers. Physical access to Provider’s own offices is controlled at all entry points, and visitors are logged and always accompanied in accordance with Provider’s Physical Access Control Policy.

Measures for ensuring events logging

Provider collects and monitors log data using industry-standard tools, with access to logs restricted on a need-to-know basis. Logging covers the entry, modification, and deletion of data at the system level, and such activity is traceable to specific, uniquely identified user accounts under an authorization concept governing rights to enter, alter, and delete data.

Measures for ensuring system configuration, including default configuration

All changes to the production environment are made through a centralized configuration management system, maintained as Infrastructure-as-Code, logged, and subject to security review, vulnerability scanning, code review, and other testing before deployment. Production and test environments are logically separated, and for Cloud Services, each customer’s environment is isolated (or, where applications are multi-tenant, protected by multi-tenancy access controls). Application security is assessed against the OWASP Top 10 as part of Provider’s secure development lifecycle.

Measures for internal IT and IT security governance and management

Provider maintains a comprehensive security program designed to comply with Data Protection Laws, prevent and recover from security incidents, and maintain the confidentiality, integrity, and availability of Personal Data. The program is overseen legal and security and the risk management process is governed by a suite of information security policies (including Access Management, Information Security Roles and Responsibilities, Risk Management and Procedures, Acceptable Use Policy, and Operations Management policies), and is reinforced through mandatory employee security and data protection awareness training performed at least annually.

Measures for certification/assurance of processes and products

Independent third-party SOC 2 Type II audits and/or ISO 27001 certifications and penetration tests are performed at least annually.

Measures for ensuring data minimization

Provider collects and uses only the Personal Data necessary to provide the SaaS (Cloud Service) and services to Customer, consistent with the privacy-by-design and privacy-by-default principles embedded in Provider’s Data Protection Policy and secure development lifecycle.

Measures for ensuring data quality

Customer can update and correct its users’ Personal Data in the Provider SaaS (Cloud Service).

Measures for ensuring limited data retention

Customer can manage retention of its users’ Personal Data in the Provider SaaS (Cloud Service), and all Personal Data is deleted upon request or termination.

Measures for ensuring accountability

Provider implements data protection and security policies in accordance with Data Protection Law, maintains documentation of processing activities, operates a formalized process for responding to data subject requests, and undergoes independent third-party audits (SOC 2 Type II and/or ISO 27001) to ensure accountability.

Measures for allowing data portability and ensuring erasure

Customer can delete or request its Personal Data associated with the Cloud Service by emailing privacy@hivemq.com.

For transfers to sub-processors, also describe the specific technical and organisational measures to be taken by the sub-processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Provider conducts due diligence before onboarding new Sub-processors, including prior examination of the Sub-processor's security measures and documentation through a self-assessment questionnaire, certificate or audit reviews, through Provider's Vendor Onboarding process, and selects Sub-processors based on their data protection and security posture. Provider contractually obligates Sub-processors to maintain confidentiality (including through confidentiality/non-disclosure agreements) and to implement the technical and organisational measures necessary to satisfy Provider's commitments to Customer, and monitors Sub-processors for compliance on an ongoing basis, including evaluation of contractually agreed-upon reports (e.g., security events/incidents, availability statistics). Provider ensures Sub-processors erase Personal Data following termination of their engagement and reviews the security posture of Sub-processors engaged in prolonged collaborations on a regular basis.

ATTACHMENT 3
ANNEX III
SUB-PROCESSORS

Provider's current list of Subprocessors may be found on Provider's TRUST CENTER webpage, available here:
<https://www.hivemq.com/solutions/technology/hivemq-security/>

EXHIBIT 1

UK ADDENDUM

This UK Addendum shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that it fulfils the intention for it to provide the appropriate safeguards as required by Article 46 UK GDPR

This UK Addendum incorporates the Transfer Clauses, which are deemed to be amended to the extent necessary, so they operate (1) for transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that transfer; and (2) to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR.

The Parties agree to amend the following provisions of the Transfer Clauses:

- (1) Clause 17 and/or 18 to shall refer to the laws and/or courts of England/Wales; and.
- (2) The parties may amend this UK Addendum provided it maintains the appropriate safeguards required by Art. 46 UK GDPR for the relevant transfer.

Additionally, the following provisions shall apply so that the Transfer Clauses are suitable for providing an adequate level of protection for such transfer under UK Data Protection Laws:

- (a) Part 2: 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 28 January 2022, as it is revised under Section 18 of those Mandatory Clauses;
- (b) With respect to Section 19 of the Approved Addendum, in the event the Approved Addendum changes, both the data importer and the data exporter may end this addendum in accordance with the terms of the UK Data Transfer Addendum; and
- (c) Any references to "Mandatory Clauses" or "SCCs" shall be deemed to refer to the Module 2 and Module 3, with the parties selections, set out in Transfers of Personal Data from the EEA.

EXHIBIT 2

SWISS ADDENDUM

The parties agree to comply with the terms of the Transfer Clauses and the following additional provisions shall also apply in order for the Transfer Clauses to be suitable for ensuring an adequate level of protection for such transfer in accordance with the Federal Act on Data Protection of 19 June 1992 (SR 235.1) (“FADP”) Article 6 paragraph 2(a):

- (a) “FDPIC” means the Swiss Federal Data Protection and Information Commissioner.
 - (b) “Revised FADP” means the revised version of the FADP of 25 September 2020, which came into force on 1 September 2023.
 - (c) The term “EU Member State” must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility for using their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).
 - (d) The FDPIC shall act as the “competent supervisory authority” insofar as the relevant data transfer is governed by the FADP.
2. To the extent that the provision of the Services involves the transfer of Personal Data that is subject to European Data Protection Laws and the FADP and where (i) such Personal Data is transferred either directly or via onward transfer to countries that do not ensure an adequate level of protection within the meaning of European Data Protection Laws, and (ii) the parties have agreed to comply with the terms of the Transfer Clauses, the following additional provisions shall also apply in order for the Transfer Clauses to be suitable for ensuring an adequate level of protection for such transfer in accordance with the Federal Act on Data Protection of 19 June 1992 (SR 235.1) (“FADP”) Article 6 paragraph 2(a):
- (a) “FDPIC” means the Swiss Federal Data Protection and Information Commissioner.
 - (b) “Revised FADP” means the revised version of the FADP of 25 September 2020, which came into force on 1 September 2023.

The term “EU Member State” must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility for using their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c).

The FDPIC shall act as the “competent supervisory authority” insofar as the relevant data transfer is governed by the FADP