Data Processing Agreement

This data processing agreement ("**DPA**") is entered into by and between UiPath and the Company (as identified below, each a "**Party**" and collectively, the "**Parties**") as of the date (i) the last Party signs this DPA or (ii) the effective date of the Principal Agreement or relevant SOW ("**Effective Date**"). By signing or otherwise accepting this DPA, each Party represents it has reviewed this DPA and agrees to the terms set forth herein and the individuals signing this DPA below certify they are authorized to bind each Party to the terms of this DPA.

1. **Defined Terms.** Terms used with capital letter shall have the meaning assigned to them below or in the body of the Agreement:

a. "**Affiliate**" means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with a Party, where "Control" means the direct or indirect control of greater than 50% of the voting rights or equity interests of a Party or the power to direct or cause the direction of the management and/or business strategy of that Party.

b. "**Applicable Data Protection Legislation**" means any and all applicable data protection and privacy laws including, where applicable, Regulation (EU) 2016/679 regarding the Personal Data Protection ("GDPR"), any other applicable law which governs the agreements between the Parties in the field of data protection, including acts of secondary character, the rules of interpretation, recommendations and any other normative acts issued by the European Commission, the European Data Protection Board or the competent Supervisory Authorities as may be amended at different time intervals.

c. "**controller**", "**processor**", "**data subject**", "**personal data**", "**processing**", "**process**" shall have the meaning given in the GDPR.

d. "**Controller**" or "**UiPath**" means the UiPath entity entering into this DPA on behalf of itself and its Affiliates, a list of which is available at https://www.uipath.com/assets/downloads/uipath-group-entities (or successor website).

e. "**Personal Data**" means personal data held by UiPath as a controller or processor and entrusted by virtue herein to the Company, as processor.

f. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

g. "**Principal Agreement**" means the agreement executed for the purpose of the procurement of Services by UiPath from the Company and, in lack thereof, the Procurement Terms & Conditions available at https://www.uipath.com/assets/downloads/procurement-terms-and-conditions (or successor website), together with any statements or work or order forms concluded in relation thereto ("**SOW**").

h. "**Processor**" or "**Company**" means the Services provider entity detailed in the signatures block below or in the Principal Agreement or relevant SOW, entering into this DPA on behalf of itself and its Affiliates.

i. "**SCC**" 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 of the Council approved by the Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as available here (or successor website): https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914, the details of which are prescribed in Exhibit A (*SCC Details*) hereto.

j. "**Services**" means any products, goods, or services provided by Processor to UiPath, as detailed in the Principal Agreement which may include, but are not limited to, configuration, implementation, customization, consulting, and training. Any reference in the Principal Agreement to, as applicable, Deliverable, Goods, or Software, will be deemed a reference to "Services" herein.

k. "**Sub-processor**" means, if any, the subcontractor appointed by the Processor to perform the Personal Data processing on its behalf, as detailed in the Principal Agreement).

l. "**Supervisory Authority**" shall have the meaning given to the authority having as object of activity the supervision in the field of personal data protection, in the Applicable Data Protection Legislation.

m. "**Third Country**" means the third country, the territory or one or more specified sectors from that third country or the international organization which is not a member of the European Union or of the European Economic Area.

n. "**Transfer Safeguards**" means a solution, other than SCC, that enables the lawful transfer of Personal Data to a Third Country in accordance with the GDPR, including, by way of example and without limitation, adequacy decisions, biding corporate rules, etc.

2. Governance

2.1. Company provides certain Services to UiPath and, during the provision of Services, may have access to Personal Data. This DPA establishes the Parties' responsibilities regarding the protection of Personal Data and applies to the extent the Company processes Personal Data on behalf of UiPath, subject to the Principal Agreement.

3. Object of the DPA

3.1. **Controller to Processor**. The Parties agree that, in accordance with the Applicable Data Protection Legislation, UiPath is a controller of Personal Data who entrusts the processing of Personal Data to the Company, which acts as a processor. The Personal Data processing shall be performed under and within the Controller's written instructions.

3.2. **Scope.** The general rights and obligations of the Parties are set forth in this DPA, and the specific information and details regarding individual data processing (e.g., purpose, duration, nature and purpose of each processing, type of Personal Data and data subjects) are defined and specified in the Principal Agreement. Any amendment to the processing details described in the applicable Principal Agreement may only be made on the basis of a written instruction from the Controller. The Processor will process the Personal Data only within the limit and in such a manner as is necessary to fulfil the purpose of the processing as determined by the Controller and will not process the Personal Data for other purposes or in another manner which is not reflected in the Controller's instructions, is contrary to the DPA or to the Applicable Data Protection Legislation.

4. Processing only in accordance with Controller's Instructions

4.1. **Controller's Instructions**. The Processor is required to process Personal Data only at, and within the limits set forth in, the written instructions from the Controller, including with respect to the transfer of Personal Data to a Third Country or an international organization. In addition to the instructions provided in this DPA, the Controller reserves the right to issue any other instructions regarding the type, purpose, and procedures for processing Personal Data, which will be transmitted in writing to the Processor. The Processor will notify the Controller without delay, in accordance with the Legal Notices section herein, if it considers that a Controller's instruction or any implementation of an instruction submitted by the Controller breaches or has the potential to breach the Applicable Data Protection Legislation or this DPA.

4.2. **Records of Processing**. The Processor will keep a detailed, clear, and up-to-date record of the processing of Personal Data carried out on behalf of the Controller under this DPA, in the form, with the content and reflecting at least the information provided by art. 30 par. (2) GDPR.

5. Confidentiality and Security

5.1. **Confidentiality.** The Processor will preserve the confidentiality of the Personal Data and the processing activities. The Processor shall ensure that any person charged with the processing of Personal Data by the Processor, either an employee, a contractor, or a Sub-processor, undertakes to maintain the confidentiality of Personal Data. The obligations to preserve the confidentiality of Personal Data will continue to be binding on the Processor, its employees, contractors, and Sub-processors after termination of processing under this DPA, termination of the provision of Services by the Processor, or termination of the Principal Agreement.

5.2. **Security**. Taking into account the current state of technology and the varying degrees of risks and severity for the rights and freedoms of individuals, the Processor will implement, as a minimum, the technical and organizational measures described in the Controller's Cybersecurity Requirements available at https://www.uipath.com/assets/downloads/cybersecurity-requirements (or successor website) to ensure a level of security appropriate to the risk for the Personal Data processing that it carries out, in line with Applicable Data Protection Legislation and ISO 27001 or similar industry information security standards. Processor shall guarantee compliance with these provisions by its staff and its relevant Sub-processors. The Processor shall keep Personal Data logically segregated from Processor's own data and the data of other customers or suppliers of the Processor.

6. Obligations for the Processor

6.1. Access to Personal Data. Subject to, and within the limits provided under the Applicable Data Protection Legislation (including, by means of example and without limitation, Article 12 para. 5 or the GDPR), the Processor undertakes the obligations listed below in respect to the access to Personal Data.

(i) The Processor shall promptly inform the Controller of requests received by the Processor from data subjects exercising their rights under the Applicable Data Protection Legislation.

(ii) The Processor shall assist the Controller with extracting, deleting, or performing any other operations on, the Personal Data, or, where possible, provide the Controller the ability to perform any of the aforementioned actions on the Personal Data.

(iii) The Processor shall provide commercially reasonable and timely assistance to Controller, in accordance with the technical capabilities of each Service, to enable Controller to respond to: (i) any request from a data subject exercising its rights under the Applicable Data Protection Legislation; and (ii) any other enquiry or complaint received from a data subject or a Supervisory Authority in connection with the processing of the Personal Data.

6.2. Personal Data Breach. Upon any known potential or actual breach of the DPA or any obligations or duties owed by the Processor to the Controller relating to the confidentiality, integrity or availability of Personal Data, or upon the occurrence of a Personal Data Breach, the Processor will in the most expedient time possible under the circumstances and at its expense investigate the event to identify, prevent and mitigate the effects and to carry out any recovery or other remediation actions necessary. The Processor will notify the Controller, without undue delay (but no later than 48 hours) from becoming aware that a Personal Data Breach has occurred, and shall provide reasonable information and cooperation to Controller, so that Controller can fulfil any Personal Data Breach reporting obligations it has under the Applicable Data Protection Legislation, and will follow-up in writing with any additional details, including the cause of the Personal Data Breach, remedial action taken and the potential consequences thereof. The notice, and any follow-ups, shall be sent in writing to UiPath, in accordance with the Legal Notices section herein. The Controller acknowledges that it is responsible for complying with its own legal obligations regarding Personal Data Breach notifications.

6.3. Assistance. Upon written request from the Controller, the Processor shall give reasonable assistance to the Controller in carrying out any assessment of the consequences or impact of processing of Personal Data and in any consultation with the Supervisory Authority. The Processor will notify the Controller without delay if a Supervision Authority contacts the Processor directly with respect to the processing activities that fall within the subject matter of this DPA.

7. Controller’s Rights

7.1. Audit. The Processor will allow the Controller, either directly or via third-party consultants, to audit the Processor’s compliance with this DPA, on-site or remote, at any time upon prior written notice of at least 10 (ten) working days, but not more than once a year. In case the Controller, in its own discretion, reasonably suspects that a breach of this DPA occurred, the Controller shall always have the right to audit by giving a 24 (twenty-four) hours prior written notice.

7.2. Conditions of the Audit. The audit will include but will not be limited to the following:

(i) Processor must grant Controller access to any facilities relevant for the audit during normal business hours, particularly to its information systems and documentations related to the processing activities and shall reasonably make available personnel who are responsible and qualified to support the Controller for those audits.

(ii) The Processor shall, without undue delay, provide the Controller with all the data and information necessary to monitor compliance with the obligations set forth in this DPA.

(iii) If the Controller so requests, the Processor shall, without undue delay, provide the Controller with the register describing the processing activities.

(iv) The Controller will inform the Processor if it identifies errors or irregularities when inspecting the processing of Personal Data. The Processor shall remediate the errors or irregularities in reasonable time and depending on their severity shall provide a roadmap of remediation.

(v) Each Party shall bear its own audit costs, and the Processor will give reasonable cooperation and assistance to the Controller. If irregularities are identified, the Controller's audit costs will be borne by the Processor.

7.3. **Cooperation with Authorities.** The Processor will notify the Controller without delay if, by way of a court order or by law, by pledge, or any other measures imposed, or events produced by third parties, including the Supervisory Authority, the Processor is legally required to give details with respect to the processing activities that fall within the subject matter of this DPA, or access to the Personal Data is otherwise required. Furthermore, if required by the Controller, the Processor will permit the Controller to handle such request directly and will promptly provide, at no additional cost, assistance reasonably required by the Controller to comply with the request. Processor will notify Controller immediately upon receipt of such request, to allow Controller time to object and move for a protective order or similar protection. Processor will limit any disclosure of the Personal Data to the greatest extent permitted by the applicable law, and where disclosure is required by law, court order, or administrative body decision binding on the Processor, the Processor will file any Personal Data under seal or request that the court or administrative body seal the Personal Data prior to Processor's disclosure.

8. Sub-processors

8.1. **Authorization.** Controller hereby authorizes the Processor to engage and use the Services of the Sub-processors listed in the Principal Agreement.

8.2. **Change of Sub-processors.** The Processor shall notify the Controller, in accordance with the Legal Notices section herein, of any intended change to the list of Sub-processors. The Controller will have a period of 30 (thirty) days from receipt of the notification sent by the Processor to object to any change to the list of Sub-processors. In this case, the Processor shall work with the Controller in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of the proposed Sub-processor(s) contested by the Controller. Where such a change cannot be made, the Controller, at its discretion, may, by written notice to the Processor, terminate the DPA and/or the Principal Agreement with immediate effect. Upon such termination, Processor will immediately refund to Controller any and all unused and pre-paid fees under the Principal Agreement.

8.3. **Compliance by the Sub-processors**. The Processor will flow down all the confidentiality and security obligations provided to it under this DPA, in the applicable agreements executed with its Sub-processors, and shall remain liable for each Sub-processor's compliance with the obligations set out for the Processor in this DPA. Upon written request from the Controller, and subject to any confidentiality obligations binding on the Processor, the Processor shall provide Controller all relevant information it reasonably can in connection with its applicable Sub-processor agreements, where required to satisfy Controller's obligations

9. Cross-border Transfers of Personal Data

9.1. **Transfer Safeguards**. Processor may process Personal Data, including by using Sub-processors, outside the country in which the Controller or its Affiliates using the Services are located, in accordance with this DPA and as permitted under the Applicable Data Protection Legislation, and solely by offering Transfer Safeguards and ensuring that all transfers are made in accordance with Transfer Safeguards.

9.2. **SCC**. To the extent Transfer Safeguards, as regulated by the Applicable Data Protection Legislation, cannot be provided, and where the Processor is located in a Third Country, the SCC are hereby incorporated into this DPA. By executing the DPA, the Parties hereby agree to the execution of the SCC by and between the Processor as "the data importer", and the Controller as "the data exporter" and the SCC will be deemed incorporated into, and considered part and parcel of, this DPA. The details required by the SCC, and by Annexes I and II thereto, are specified in Exhibit A below.

9.3. **Amendments to the SCC and Other Measures.** Unless the Controller notifies the Processor otherwise, if the European Commission amends the SCC after the Effective Date, the amended SCC will supersede and replace the SCC executed between the Parties by virtue of this section. In addition, if and to the extent a court of competent jurisdiction or Supervisory Authority orders (for whatever reason) that the measures described in this DPA cannot be relied on for the purpose of lawfully transferring Personal Data to Third Countries, the Controller agrees that the Processor may implement any additional measures or safeguards that may be reasonably required to enable a lawful transfer.

10. Liability and Legal Remedies

10.1. **Liability.** Each Party will be liable for its own actions and/or omissions under this DPA. The Processor will remain fully liable to the Controller for the performance of the obligations that its appointed Sub-processors fail to comply with.

10.2. **Indemnity**. Notwithstanding anything to the contrary set forth herein, the Processor shall defend, indemnify, and hold harmless the Controller against any claims, proceedings, material or moral damages, and losses, whether direct or indirect, including court fees and lawyers' fees or sanctions imposed by any competent authority, arising out of a breach of Processor's (or its Sub-processors') obligations, as set forth in, or derived from, this DPA. The Company will not enter into any settlement with any third-party that admits liability on behalf of UiPath or imposes any obligations on UiPath and will take all reasonable measures to mitigate the damages.

10.3. **LIMITATION OF LIABILITY**. UNLESS OTHERWISE PROHIBITED BY APPLICABLE LAWS BINDING ON THE PARTIES, AND EXCEPT FOR THE INDEMNIFICATION OBLIGATIONS IN THIS DPA, THE LIMITATIONS OF LIABILITY SET OUT IN THE PRINCIPAL AGREEMENT APPLY TO ANY LIABILITY UNDER THIS DPA AND THE MAXIMUM AGGREGATE LIABILITY OF EACH PARTY AND/OR THEIR AFFILIATES, FOR ANY AND ALL BREACHES AND CLAIMS (INDIVIDUALLY AND TOGETHER) UNDER OR RELATING TO THIS DPA, AND FOR ALL DATA PROCESSING ACTIVITIES CONTEMPLATED BY THIS DPA, WILL NOT EXCEED THE LIABILITY CAP OR LIMITATION SET OUT IN THE PRINCIPAL AGREEMENT. THIS LIMITATION APPLIES WHETHER THE CLAIM ARISES FROM CONTRACT, NON-CONFORMITY OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY.

10.4. **DAMAGES EXCLUSION**. UNLESS OTHERWISE PROHIBITED BY APPLICABLE LAWS BINDING ON THE PARTIES, NEITHER PARTY WILL BE LIABLE TO THE OTHER FOR ANY SPECIAL, INDIRECT, MORAL, CONSEQUENTIAL, INCIDENTAL, PUNITIVE, OR EXEMPLARY DAMAGES, LOSS OF PROFITS, REPUTATION, USE, OR REVENUE, OR INTERRUPTION OF BUSINESS, IRRESPECTIVE OF WHETHER THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. PROCESSOR WILL NOT BE LIABLE FOR ANY DAMAGE CAUSED BY FAILURE OF CONTROLLER TO COMPLY WITH THE DPA OR ANY APPLICABLE PRIVACY POLICIES, LAWS OR REGULATIONS.

10.5. **Proportionality**. If both the Controller and the Processor are liable for material or moral loss or damage caused by processing activities that are not in compliance with the Applicable Data Protection Legislation, each of the Parties shall be held liable proportionally for such loss or damage, in accordance with the aspects which are under the responsibility of that Party under the Applicable Data Protection Legislation and this DPA.

11. Term and Termination

11.1. **Term.** This DPA is effective as of the Effective Date and will continue for the entire duration of the Principal Agreement, and as long as the Processor continues to process Personal Data as a Processor or Sub-processor on behalf of UiPath.

11.2. **Termination.** This DPA may be terminated by the Controller upon written notice with immediate effect, in case of Processor's material breach of the DPA and/or for legitimate cause. This Agreement will terminate immediately upon termination of the Principal Agreement, however Company's obligations of confidentiality, availability and security of Personal Data will continue to be in effect in accordance with the Applicable Data Protection Legislation and the Consequences of Termination section below.

11.3. **Consequences of Termination.** Unless otherwise agreed between the Parties in, or in accordance with, the Principal Agreement, termination of this DPA will not cause the immediate termination of the Principal Agreement. Following termination of this DPA, Company will cooperate with UiPath to return, or delete the Personal Data records, and will continue to comply with the obligations of confidentiality, availability, and security in respect of Personal Data as set out below.

11.3.1. **Deletion of Personal Data.** Within maximum 30 (thirty) days after the termination or expiration of this DPA, the Processor shall delete or return to the Controller, at the Controller's choice and free of charge, all Personal Data, results, and records of the processing of the Personal Data. If the Controller opts for the deletion of the Personal Data, the Processor shall ensure that the Personal Data is removed from all devices, including those belonging to Sub-processors. Within maximum 10 (ten) days of request from the Controller, the Processor shall provide written evidence of the deletion or destruction of Personal Data.

11.3.2. **Records.** If the Processor is bound by the Applicable Data Protection Legislation, to continue to retain Personal Data results or records, it will notify the Controller in writing prior to the commencement of the processing, or at the latest within 5 (five) business days after becoming aware of the existence of this obligation. Processor will retain all documents or registers serving as proof of the lawful processing of Personal Data as per Controller's instructions, in accordance with the legal periods of retention, including after the processing operations cease, and will provide copies of such records to the Controller, within maximum 30 (thirty) days from Controller's request.

12. Miscellaneous

12.1. **Legal Notices.** Unless otherwise provided herein, legal notices under this DPA must be sent by e-mail, with a suggestive subject and will be effective on the next business day after being sent. Legal notices to the Company will be sent to the business account contact, and, in lack of a valid e-mail address, to any e-mail address publicly available, or any e-mail addresses previously used in communication with UiPath. Notices to UiPath will be sent to the addresses listed below (or otherwise notified in writing by UiPath).

Notices to UiPath		Notices to Company
For general matters and changes in Sub-processors:	privacy@uipath.com	As per signature box or Principal Agreement.
For Personal Data breaches:	security.breach@uipath.com	

12.2. **Principal Agreement.** This DPA with all references herein is the entire understanding between UiPath and Company with respect to the subject matter of this DPA and supersedes any prior written or oral agreement between the Parties with respect to such subject matter. This DPA is without prejudice to the rights and obligations of the Parties under the Principal Agreement which will continue to have full force and effect. This DPA is incorporated into and made a part of the Principal Agreement by this reference. The Processor undertakes not to assign the rights and obligations arising from this DPA, or the Principal Agreement without the prior written consent of the Controller. This DPA will supersede and take precedence over any conflicting provisions governing the protection, confidentiality, and security of Personal Data in the Principal Agreement.

12.3. **Amendments.** Unless otherwise expressly stated in this DPA, all amendments and additions, as well as the termination of this DPA and/or any Exhibit(s), shall be valid only if made in writing and signed by authorized representatives of both Parties.

12.4. **Severability.** If any provision of this DPA is declared invalid or unenforceable by a court, arbitral tribunal or any other competent authority, no other contractual provisions or rights and obligations of the Parties provided by this DPA will be affected. The provision which is null or void will be deemed removed from the DPA and the Parties will ensure that it is replaced by a valid and applicable provision that has, as far as possible, the same economic effects.

12.5. **Applicable Language.** This DPA is made in the English language, which will be controlling in all respects, and all versions hereof in any other language will not be binding on the Parties hereto. All communications and notices to be made or given pursuant to this DPA and any dispute resolution (including, but not limited to, any court proceeding, legal notices, motions, discovery, etc.) will be in the English language only.

Exhibit A - SCC Details

Selection of Module	
SCC	Module Two (transfer controller to processor) is selected as the applicable module for the entirety of the SCC.
Selection of Options	
Clause 7	Clause 7 Docking clause is optional, and the parties wish to adopt it.
Clause 9(a)	Option 2 is selected (general written authorization), with the specified time period of 30 days.
Clause 11(a)	The second paragraph of Clause 11(a) is optional, and the parties do not wish to adopt it.
Clause 17	Option 1 is selected, with the specified Member State of Romania.
Clause 18(b)	The specified Member State is Romania.

Annex I		
List of Parties		
Data exporter(s)	*Identity:*	UiPath SRL (or one of its affiliates based in a Third Country) and its Sub-processors
	Contact person's name:	privacy@uipath.com
	Activities relevant to data transferred under these SCC:	As per Principal Agreement.
	Role:	Controller
Data importer(s)	*Identity:*	Company and its affiliates
	Contact person's name:	As per Principal Agreement
	Activities relevant to data transferred *under these* SCC*:*	As per Principal Agreement
	Role:	Processor
Description of Transfer	As per Principal Agreement	
Categories of Data Subjects whose Personal Data is transferred	As per Principal Agreement	
Categories of Personal Data transferred	As per Principal Agreement	
Sensitive data transferred	As per Principal Agreement	
Frequency of the transfer	As per Principal Agreement	
Nature of the processing	As per Principal Agreement	

Purpose(s) of the data transfer and further processing	As per Principal Agreement
The period for which the Personal Data will be retained	As per Principal Agreement
Transfers to Sub-processors	As per Principal Agreement
Competent Supervisory Authority	
Supervisory Authority with responsibility for ensuring compliance by the data exporter	The applicable Supervisory Authority is the authority in the EU Member State where the data exporter is established, or other supervisory authority with the right by operation of law to supervise compliance.
Description of the technical and organizational measures implemented by the data importer(s)	The Processor will maintain at least the technical and organizational security measures set out in the DPA.

Annex II Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of Personal Data	
Description of the technical and organizational measures implemented by the data importer(s)	The Processor will maintain at least the technical and organizational security measures set out in the DPA.

Transfers from the United Kingdom	
EU SCC, completed with the details set forth under Section 1 above apply for transfers from the United Kingdom, subject to the following:	
Applicable law	any references to “Directive 95/46/EC” or “Regulation (EU) 2016/679 shall be understood as references to the UK GDPR
	any references to the “EU”, “Union” and “Member State law” shall be understood as references to English law
Competent authorities	any references to the “competent supervisory authority” and “competent courts” shall be understood as references to the relevant data protection authority and courts in England, unless the EU SCCs as implemented above cannot be used to lawfully Transfer such Data in compliance with the UK GDPR, in which event the UK SCCs will instead be incorporated by reference and form an integral part of this DPA and will apply to such Transfers. Where this is the case, the relevant Annexes or Appendices of the UK SCCs will be populated using the information contained in Section 1 above of this DPA (as applicable).

Transfers from Switzerland	
EU SCC, completed with the details set forth under Section 1 above apply for transfers from Switzerland, subject to the following:	
Applicable law	any references to “Directive 95/46/EC” or “Regulation (EU) 2016/679 shall be understood as references to FADP
Competent authorities	any references to the “competent supervisory authority” shall be understood as reference to “Swiss Federal Data Protection and Information Commissioner (the “FDPIC”)
	any references to the competent courts or to any provisions related to contractual claims may be understood as references to the Member State, as set forth under Section 1 subject to data subjects in Switzerland having the possibility to file claims for their rights in Switzerland.