DATA PROCESSING AGREEMENT
("**DPA**")

Concluded between:
1. Customer, hereinafter referred to as the "**Controller**"; and

2. UiPath, hereinafter referred to as the "**Processor**"

each as described in the signature box and each referred to as the "Party" and collectively the "Parties".

Preamble

The Controller and the Processor have concluded this DPA in accordance with the legal requirements in the field of personal data protection and in order to establish their responsibilities regarding the protection of personal data which may be processed as a result of the Parties entering into the UiPath License Agreement (the **"Agreement").** This DPA is tailored to UiPath's RPA Cloud Platform architecture and to the functionalities of UiPath's cloud activities, which do not require the processing of personal data. The Customer, which in this case is the Controller, has full control over the data sent for processing. This Agreement does not apply to the data processed as a result of using third party cloud integrations, such as OCR tools, which are subject to their own terms and conditions and privacy policies. The Controller is responsible for complying with its applicable data protection laws and for assessing whether the use of the UiPath Services meets its compliance and contractual obligations.

1. Interpretation and terminology
In this DPA, the following terms shall have the following meanings:

a. "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**", "**Processing**" (and "**Process**"), "**Supervisory Authority**" shall have the meaning given in GDPR;

b. "**Applicable Data Protection Law**" 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;

c. "**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;

d. "**Services**" means the online services and other activities to be supplied to or carried out by the Processor pursuant to the License Agreement which involve the transfer of personal data to the Processor through electronic or physical means of communication;

e. "**Sub-processor**" means the subcontractor appointed by the Processor to perform the Personal Data Processing on behalf of the Processor;

f. "**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;

g. "**Transfer Safeguards**" means a solution, other than the EU Standard Contractual Clauses, that enables the lawful transfer of personal data to a Third Country in accordance with the GDPR.

h. "**UiPath License Agreement**" – means the license agreement concluded between the Controller and the Processor.

2. Object of the DPA
2.1.   The Parties agree that, in accordance with the Applicable Data Protection Law, the Customer is the Controller of Personal Data who entrusts the Processing of the Personal Data to the Processor, to the extent Personal Data is provided when using the UiPath Services. No Personal Data is required for the performance of the Agreement, but taking into account the particularities of each Service, UiPath acknowledges that it may receive personal data. This DPA governs these types

of situations. The Personal Data Processing shall be performed under and within the Controller's instructions. The personal data processed in connection to the provision of **Professional Services and Support services are not subject to this DPA.**

2.2. The general rights and obligations of the Parties are set forth in this DPA, and the specific information and details regarding individual data processing (i.e. purpose, duration, nature and purpose of each processing, type of Personal Data and Data Subjects) are defined and specified in Exhibit 1 of this DPA. Any amendment to the processing details described in Annex 1 may only be made on the basis of a written instruction from the Controller.

3. Processing only in accordance with the Controller's Instructions and Purposes

3.1. The Processor is required to process the Personal Data only at and within the limits set forth in the instructions sent in writing by the Controller, including regarding the transfer of Personal Data to a Third Country or an international organization.

3.2. The Processor will notify the Controller without delay 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 Law.

3.3. UiPath shall maintain all records required by Article 30(2) of the GDPR and, to the extent applicable to the processing of Personal Data on behalf of Controller, make them available to Controller upon request.

4. Maintaining Data Confidentiality

4.1. The Processor will preserve the confidentiality of the Processing activities and the Personal Data processed.

4.2. 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.

5. Security of Processing

5.1. 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 reasonable technical and organizational measures to ensure an adequate level of security for the Personal Data Processing that it carries out. This does not limit the Controller's responsibility to safeguard its credential information and any components it has control over as well as to assess whether it's privacy and security obligations are met when using the UiPath Services. Please find here a description of the Processor's security practices. The Processor shall maintain security measures which comply with ISO 27001 or similar industry information security standards. The Processor reserves the right to modify or update its security measures or practices as long as the updates or modifications do not translate into a lower level of security for the processing activities.

6. Obligations to Provide Support

6.1. The Processor shall promptly inform the Controller of any request received by the Processor from Data Subjects exercising their rights in connection to their Personal Data. The Processor shall provide the Controller the ability to extract, delete or perform any other operations on its data, to the extent technically possible. The actions mentioned in this paragraph are subject to the provisions set out in article 12, para. 5 of the GDPR. If necessary, the Processor shall provide commercially reasonable and timely assistance to Controller, in accordance with the technical capabilities of each UiPath cloud Service in order to enable Controller to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law; and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data. The Processor shall notify the Controller promptly of any request received from a data subject and shall provide all reasonable assistance to enable the Controller to respond within the legally required timeframe of 30 days from receiving such a request.

6.2. In the event of a Personal Data Breach, the Processor shall notify the Controller by email within 48 hours of becoming aware of the occurrence of the breach and shall provide reasonable information and cooperation to Controller so that Controller can fulfil any data breach reporting obligations it may have under Applicable Data Protection Law. The Controller is responsible for providing appropriate and updated contact information and for complying with its legal obligations regarding Personal Data Breach notifications. Notifying a personal data breach does not translate in an acknowledgement by the Processor of the responsibility or liability for the breach. In the event the Controller suspects that a potential incident occurred, the Controller shall with undue delay notify the Processor at privacy@uipath.com.

6.3. The Processor will reasonably support the Controller in carrying out any assessment of the consequences or impact of Processing of Personal Data and in any consultation with the Supervision Authority.

7. Cooperation with the Supervision Authorities

7.1. 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.

8. Controller's Right to be Informed and to Carry out Inspections

8.1. If the Controller reasonably believes that an on-site audit is necessary for compliance with data protection obligations set forth in this DPA, the Controller may request that a third party conducts an audit, if the following conditions are met:

a) an audit plan must be agreed by both parties eight (8) weeks in advance of the proposed audit date together with the third party auditor performing the audit; the audit plan will describe the scope, duration, third party auditor and start date of the audit and shall take into consideration the Processor's confidentiality and security obligations towards its customers and employees

b) audits may be performed at most once per year and must be conducted during regular business hours, according to Processor's policies so as not to interfere with Processor's business activities

c) audits may be performed only if a confidentiality agreement is concluded with the auditor and the audit results will remain confidential and will not be shared with third parties unless agreed by the Processor

d) the Controller must provide UiPath with any audit report generated in connection with any audit at no charge, unless otherwise stated in the applicable laws

e) if the audit scope described in the audit plan is addressed in an ISO, SOC or similar audit report performed by a qualified third party auditor within twelve months of the Controller's audit request, the Controller agrees to accept these reports instead of performing the audit if the Processor confirms that there were no material changes in the data protection/security measures audited

f) audits are performed at Controller's expense and Processor will cooperate and assist in the performance of the audit plan.

9. Sub-processors

9.1. If the Processor intends to use the services of subcontractors ("**Sub-processors**") to carry out the Personal Data Processing activities on its behalf, the Processor will update the list of such Sub-processors on its official website at this address: https://www.uipath.com/hubfs/legalspot/Uipath%20Sub-processors%2024.05.pdf (or its successor website). The Processor shall notify the Controller of any change to the Sub-processors list, if the Controller makes a reasonable request at privacy@uipath.com in this respect and provides an e-mail address for this purpose. The Processor has the right to reasonably object to any new third party Sub-processor by providing a notice at privacy@uipath.com within 30 days of being notified regarding the engagement of such Sub-processor. If the Processor cannot replace or not use the new Sub-processor in providing the services to the Controller as it is not commercially reasonable, the Processor can rescind the main Agreement.

9.2. The Processor will make sure that any Sub-processor is subject to the same data confidentiality obligations and provides the same adequate guarantees for the security of the Personal Data such as those envisioned in this DPA for the Processor.

10. Cross-border Transfers of Personal Data

10.1. The Processor and its Sub-Processors are entitled to process Personal Data outside the country where the Controller is located, as permitted by Applicable Data Protection laws and only by offering Transfer Safeguards and ensuring that all transfers are made in accordance with such Transfer Safeguards. In case the Processor is established in a Third Country and cannot offer any Transfer Safeguards, by entering into this DPA, the Processor is entering into Standard Contractual Clauses with the Controller.

10.2. If the Processor and its Sub-processors cannot offer Transfer Safeguards as specified by Applicable Data Protection laws, by entering into this DPA, the Processor is entering into Standard Contractual Clauses with the Controller, in the latest form adopted by the European Commission. For this purpose of entering into the Standard Contractual Clauses, the Processor is considered the Data Importer, the Controller is considered the Data Exporter and Annex 1 is applicable for the processing activities. The Standard Contractual Clauses agreement is attached to this DPA as Exhibit 2.

10.3. The Processor and Sub-processors may transfer Personal Data to Third Countries if the following conditions are met:

1. The European Commission has decided that the Third Country in question provides an adequate level of protection to ensure the rights of the Data Subjects; or

2. In the absence of a European Commission decision as per the above paragraph, the Processor has provided and assured that there are adequate guarantees, opposable rights and effective remedies available to the Data Subjects. In this situation, the Processor shall ensure that those guarantees equate at least to the application of the Standard Contractual Clauses in the latest form adopted by the European Commission or other mechanisms imposed by the Controller for example binding corporate rules or codes of conduct, in the sense of art. 40 and 47 of the Applicable Data Protection Law or certifications. The Processor shall provide the Controller with the relevant information and documents in order to obtain its consent before performing the transfer to that Third Country.

11. Duration and Termination of the DPA

11.1. This DPA is concluded for the duration of the Agreement concluded between the Parties with effect from the date of its signature by both Parties.

12. Consequences of Termination

12.1. Based on the Service functionalities, the Processor can provide the functionality to export and/or delete all Customer Data or the Processor shall delete or return Customer Data to the Controller, at the Controller's choice and express request, after the termination or expiration of the Master Service Agreement governing this DPA. This requirement shall not apply to the extent that the Processor is required by applicable law to retain some or all of the Data, or the Data has been archived on back-up systems due to Service functionalities, which Processor shall securely protect. Deletion of Customer Data includes the deletion of the associated metadata.

12.2. Liability. Each party's liability for one or more breaches of this DPA shall be subject to the limitation cap specified in the License Agreement for all aggregated claims incurred under this DPA and to the limitations and exclusions of liability set out in the License Agreement. Neither Party shall be held liable for any indirect, consequential, incidental, special or punitive damages. The liability limitations and exclusions are applicable to all of the Party's affiliates and claims, taken together in the aggregate and for all data processing activities between the Controller and the Processor.

13. Miscellaneous

13.1. This DPA is without prejudice to the rights and obligations of the parties under the Agreement which will continue to have full force and effect. This DPA is incorporated into and made a part of the Agreement by this reference.

13.2. This DPA shall be interpreted and construed in accordance with the governing laws and jurisdictions specified in the main agreement between the parties, unless otherwise provisioned in the applicable data protection laws.

13.3. All amendments and additions, as well as the termination of this DPA and its Annexes, shall be valid only if made in writing.

Signatures		
UiPath Inc.	**UiPath SRL**	_____ **(Customer)**
Address: [Inc Address]	Address: [SRL Address]	Address: [Address]
By: [Inc Signer]	By: [SRL Signer]	By: [Signer]
Title: [Inc Signer Title]	Title: [SRL Signer Title]	Title: [Signer Title]
Authorized Signature: [Inc Signature]	Authorized Signature: [SRL Signature]	Authorized Signature: [Signature]
Date: [Inc Signature Date]	Date: [SRL Signature Date]	Date: [Signature Date]

Exhibit A – DETAILS OF THE PROCESSING

The Processor shall process the Personal Data in the following manner:

Contact person(s) of the Processor	privacy@uipath.com
Purpose (reason) of Processing	Performing the License Agreement concluded between the Parties.
Type of Processing	Electronically
Processing duration	For the duration of the License Agreement
Categories of processed Personal Data	Identification data such as name, e-mail address, location data, data about an identified or identifiable individual
Data Subjects (ex: employees, customers)	Employees, Vendors, Suppliers, Partners, Customer's of Customer, Individuals
Data storage/ server location	Ireland, Netherlands

Exhibit B – STANDARD CONTRACTUAL CLAUSE

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Controller (as defined in the Agreement)

………………………………………………………………

(the data **exporter**)

And

Processor (as defined in the Agreement)

…………………………………UiPath………………………………

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

(a)   *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b)   '*the data exporter'* means the controller who transfers the personal data;

(c)   *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d)   *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e)   '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f)   *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-party beneficiary clause

1.   The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2.   The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.   The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and

obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5
Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6
Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Subprocessing

1.   The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2.   The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.   The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4.   The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12
Obligation after the termination of personal data processing services

1.   The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2.   The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

ANNEX 1 TO EXHIBIT B - STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is UiPath and, if applicable, other data controllers that are affiliated entities of UiPath located in the European Union or the European Economic Area.

Data importer
The data importer is a vendor of UiPath that is providing services to UiPath or UiPath's affiliated entities and that, by providing those services, is processing Personal Data controlled by the data exporters.

Data subjects
The personal data transferred concern the categories of data subjects set out in Annex 1 of this Agreement.

Categories of data
The personal data transferred concern the categories of data set out in Annex 1 of this Agreement.

Special categories of data (if appropriate)
The personal data transferred concern the special categories of data set out in Annex 1 of this Agreement.

Processing operations
The personal data transferred will be subject to processing activities set out in Annex 1 of this Agreement.

ANNEX 2 TO EXHIBIT B - STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):
The technical and organizational measures are at least the measures set out here and in this DPA.