Data Processing Agreement

This Data Processing Agreement ("**DPA**"), effective as of the effective date of the relevant statement of work ("**SoW**"), concluded between the UiPath entity as identified in the SoW signature box, including its subsidiaries and affiliates ("**UiPath**") and the Vendor as identified in the SoW signature box ("**Joint Controller**"), individually referred to as "**Party**" and collectively as "**Parties**" or "**Joint Controllers**". The Parties are concluding this DPA in accordance with the legal requirements in the field of personal data protection to establish their responsibilities regarding the protection of personal data processed as a result of the Parties entering into the relevant SoW.

1. Defined Terms. 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 the Applicable Data Protection Law.

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, 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. "**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. "**Processor**" means the subcontractor appointed by one of the Parties to perform the Personal Data Processing on behalf of that Party.

e. "**Services**" means the services and other activities to be supplied to or carried out by the Processor pursuant to the SoW.

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.

2. Object of the DPA

2.1. The Parties agree that, in accordance with the Applicable Data Protection Law, they qualify as joint controllers and together establish the means and purposes for the Processing of Personal Data. Personal Data shall be processed according to this DPA for the purpose(s) mentioned in Annex 1.

2.2. The Joint Controller will immediately notify UiPath at privacy@uipath.com if it makes a determination that it can no longer meet its obligation under this DPA and, when such a determination is made, the Joint Controller will immediately cease any data Processing or take other reasonable and appropriate steps to remediate the nonconformity.

3. The responsibilities of the Joint Controllers in relation to the Data Subjects

3.1. The Parties will not use the Personal Data for other purposes than those provided in Annex 1.

3.2. Each of the Joint Controllers hereby undertakes to ensure that the Data Subjects are informed regarding the Processing of Personal Data according to the GDPR requirements by providing them at the time of the collection of Personal Data, at least as stated in Art. 13 of the GDPR, if the Personal Data are obtained directly from the Data Subjects, respectively, in compliance with the provisions of Art. 14 par. (3) of the GDPR, if the Personal Data were not obtained from the Data Subjects, an information note, or a privacy policy, as appropriate. The Parties will ensure that the data subjects are informed that the Parties act as Joint Controllers with respect to the Personal Data Processing.

3.3. In those situations in which the legal basis of Processing is the consent of the Data Subjects, the Party that collects the Personal Data from the Data Subjects undertakes to ensure that the Data Subjects have been informed and have provided valid consent to the Processing.

3.4. Each Party will promptly inform the other Party about the receipt of any Data Subject access request. The Party who receives the request will be the Party responsible for answering within the timeframe required by the Applicable Data Protection Law. The Parties will collaborate in answering to such requests.

3.5. The Parties will delete the Personal Data on the completion of the Services detailed in the SoW with the exception of the Personal Data that the Joint Controllers have a legal obligation to Process.

3.6. Each Party shall comply with its obligation to report a Personal Data Breach to the appropriate Supervisory Authority and (where applicable) notify Data Subjects under Applicable Data Protection Law. The Party who identifies the Personal Data Breach will notify the other Party without undue delay regarding the occurrence of the Personal Data Breach prior to reporting the Personal Data Breach to the Supervisory Authority and to notifying the Data Subjects. The notification will include the categories of Personal Data affected and the measures taken and at least the

information mentioned in art. 33 (2) of the GDPR. The Party who has the obligation to notify will allow the other Party to review the notification and shall have proper consideration to any reasonable comments or amendments proposed by the other Party in so far as the comments or amendments are provided within the timeframe indicated by the notifying Party. UiPath shall be notified at security.breach@uipath.com. The Joint Controller shall be notified as per the relevant SoW.

4. Maintaining Data Confidentiality

4.1. The Parties will preserve the confidentiality of the Processing of Personal Data and will make sure that their staff and any other third party to whom data is disclosed will respect the confidentiality and protection of the Personal Data.

4.2. Each Party will make sure that they have contractual obligations in place with their Processors in order to ensure the protection of Personal Data, according to at least the obligations set out under article 28 of the GDPR.

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 Parties will implement technical and organizational measures to ensure a level of security appropriate to the risk for the Personal Data Processing that they carry out while taking into account, at the same time, the nature of the Processing and the information available to each Party. Further obligations may be imposed on the Party receiving the Personal Data from the other Party in the SoW.

5.2. To assess the appropriate level of protection, the Parties will in particular take into account the risks associated with the Processing, such as destruction, loss, modification, unauthorized disclosure or unauthorized access to Personal Data unintentionally or unlawfully.

5.3. The Joint Controllers may take one or more of the following measures, without being limited to such measures, to ensure the security of the Data Processing:

a) Pseudonymization and encryption of Personal Data.
b) Ensure the capabilities, confidentiality, availability and capabilities of systems and services.
c) Ensure ability to quickly restore availability and access to Personal Data.
d) Implement a process of periodic verification and evaluation of the effectiveness of technical and organizational measures to guarantee the security of Processing.

6. Joint Controllers' right to be informed

6.1. Upon request of one Party, the other Party shall provide without undue delay all necessary information in order to update the internal registries of Processing activities or to monitor compliance with the obligations set forth in this DPA.

6.2. Each Party shall inform the other Party, whether it identifies errors or irregularities when verifying if the Processing of Personal Data is done in accordance with this DPA or the Applicable Data Protection Law.

7. Cooperation with the Supervisory Authorities

7.1. Each Party shall notify the other Party without undue delay if a Supervisory Authority contacts it directly with respect to the Processing activities subject to this DPA.

8. Cross Border Transfers of Personal Data

8.1. Each Party will transfer Personal Data to Third Countries if the following conditions are met:

a) 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
b) In the absence of a European Commission decision as per the above paragraph, the Party transferring Personal Data to a third Country has provided and assured that there are adequate guarantees, opposable rights and effective remedies available to the Data Subjects. In this situation, the respective Party 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 that Party for example binding corporate rules or codes of conduct, in the sense of art. 40 and 47 of GDPR or certifications. Each Party shall provide the other Party with the relevant information and documents in order to obtain its consent before doing the transfer to a Third Country.

9. Liability and Legal Remedies

9.1. Each Party shall be liable to the other Party for the full and timely execution of all obligations under this DPA, the Applicable Data Protection Law, or any other instrument agreed by the Parties or applicable to the Personal Data Processing covered by this DPA, including obligations regarding the confidentiality and security of Personal Data and the fulfillment of obligations towards the Data Subjects.

9.2. Each Party shall indemnify the other Party in full against any material, direct damage, including court fees and lawyers' fees, or sanctions imposed by any competent authority as a result of negligence, non-execution or non-compliance or late fulfillment of any obligations in or derived from this DPA.

9.3. Each of the Parties will be liable to the Data Subjects for any material or moral damage caused by its Personal Data Processing operations as a result of breaches of the Applicable Data Protection Law or the provisions of this DPA.

9.4. The Parties are aware that, in accordance with Art. 82 par. (4) of GDPR, if Joint Controllers were involved in the same Personal Data Processing operation that caused harm to the Data Subject, each of them will have to provide compensation to the Data Subject for all damage suffered as a result of non-compliance with the Applicable Data Protection Law if the Data Subject decides to file a claim for damages and to base its claims against only one of the Joint Controllers.

9.5. The Parties agree that the Party who fully paid the damage in accordance with art. 9.4 is entitled to claim from the other Party the amount of damages corresponding to its liability as a result from its breach of its obligations under the Applicable Data Protection Law or the provisions of this DPA. For the avoidance of any doubt, in case of a Personal Data Breach, the Party who suffered the Personal Data Breach will be fully liable for damages resulting from such Personal Data Breach.

10. Duration and Termination of the DPA

10.1. This DPA is concluded for the duration of the SoW concluded between the Parties as of the SoW effective date.

11. Miscellaneous

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

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

11.3. If any provision of this DPA is declared invalid or unenforceable by a court, arbitral tribunal or any other competent authority, the other contractual provisions, that is, the rights and obligations of the Parties provided for therein, remain in force. The provision which is null and void will be removed from the DPA and the Parties will take all care to ensure that it is replaced by a valid and applicable provision that has, as far as possible, the same economic effects.

Annex 1 to the DPA– Details of the Processing

Contact person(s) of UiPath	privacy@uipath.com
Contact person(s) of the Joint Controller	As per SoW concluded between the Parties.
Purpose (reason) of Processing	Provision of recruiting/headhunting services.
Type of Processing	Electronically.
Nature of Processing (e.g.: collecting, recording, structuring, combining data)	As necessary for the performance of the SoW concluded between the Parties.
Processing duration	For the duration of the relevant SoW.
Categories of processed Personal Data (e.g.: name, address, e-mail, location data, image, voice)	Name, email address, phone number, job position information, job performance information, right to work status, citizenship.
Special categories of Personal Data/ sensitive data (if any) (e.g. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic, biometric or health data)	N/A
Data Subjects (ex: employees, customers)	Candidates.