DATA PROCESSING ADDENDUM

This Data Processing Amendment (this "DPA") to the Corporate Transparency Act Compliance Cloud Platform License Agreement (as amended, the "Agreement") effective as of the date of the Agreement is entered into by and between the Company and Licensee). Unless otherwise defined herein, capitalized terms shall have the meanings assigned to such terms in the Agreement. Capitalized terms not specifically defined in this DPA will have the meanings given to them in the Agreement.

The parties desire to amend the Agreement to address their respective obligations under applicable privacy and data protection laws and to protect personal information processed by the Company in connection with the Agreement. In consideration of the foregoing, the promises and agreements set forth herein, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereby agree as follows:

1. **Definitions**. Capitalized terms not specifically defined in this DPA will have the same meaning as in the Agreement.

1.1. "**Anonymous Data**" means Personal Data that has been processed in such a manner that it can no longer be attributed to an identified or identifiable Data Subject, including as applicable any "deidentified" Personal Data as defined under applicable Data Protection Law.

1.2. "**Authorized Individual**" means an employee of the Company who has a need to know or otherwise access Personal Data to enable the Company to perform its obligations under this DPA or the Agreement or a Sub-Processor.

1.3. "**CCPA**" means the California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 et seq.

1.4. "**Data Protection Laws**" means all privacy or data protection laws applicable to the Processing of Personal Data under the Agreement or this DPA, including, where applicable, EU Data Protection Laws, Singapore Data Protection Laws, Swiss Data Protection Laws, UK Data Protection Laws and the CCPA.

1.5. "**Data Subject**" means the identified or identifiable natural person to whom Personal Data relates.

1.6. "**EEA**" means the European Economic Area.

1.7. "**EU Data Protection Laws**" means the European Union ("**EU**") General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 ("**GDPR**") and EU Member State data protection laws implementing or supplementing the GDPR.

1.8. "**Licensee Data**" means any information, in any form, format or media (including paper, electronic and other records), which Licensee uploads or submits, as applicable, to Company to Process on its behalf as a Processor in performing the Services.

1.9. "**Personal Data**" means Licensee Data relating to an identified or identifiable natural person. Personal Data does not include Anonymous Data.

1.10. "**Processor**" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller, including as applicable.

1.11. "**Security Breach**" means a breach of security of the Services leading to accidental or unlawful destruction, loss, alteration, unauthorized discloser of, or access to Personal Data in the possession or control of Company.

1.12. “**Services**” means the services provided by Company as set forth in the Agreement. Services may include Company’s software-as-a-service offerings which Licensee may purchase as a subscription for a defined term and/or Company’s generally available support services.

1.13. “**Standard Contractual Clauses**” means (i) where the GDPR or Swiss Data Protection Laws applies, the standard contractual clauses for the transfer of Personal Data to third countries approved by the European Commission’s decision 2021/914/EC of June 4, 2021, as currently set out at https://eurlex.europa.eu/eli/dec_impl/2021/914/oj (the “EU SCCs”); (ii) where the UK Data Protection Laws applies, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, as currently set out at https://ico.org.uk/media/fororganisations/documents/4019539/international-data-transfer-addendum.pdf, and as revised under Section 18 of the International Data Transfer Addendum (the “UK Addendum”).

1.14. “**Sub-Processor**” means any third-party Processor engaged by Company or to Process Personal Data.

1.15. “**Singapore Data Protection Laws**” means the Singapore Personal Data Protection (Amendment) Act 2020.

1.16. “**Swiss Data Protection Laws**” means the Swiss Federal Act on Data Protection (1992) or the Swiss Federal Data Protection Act of 25 September 2020 when in full force and effect, as applicable, and its corresponding ordinances.

1.17. “**UK Data Protection Laws**” means the Data Protection Act 2018 of the United Kingdom.

1.18. The terms “**business**,” “**business purposes**,” “**consumer**,” “**controller**,” **“data subject,” “personal data breach,”** “**process**” or “**processing**,” “**processor**,” “**sale**,” “**sensitive data**,” “**sensitive personal information**,” “**service provider**,” “**sharing**,” **“supervisory authority,”** and “**verifiable consumer request**” will have the meanings given to those terms in the applicable Data Protection Laws.

2. **Processing of Data; Relationship of Parties**. This DPA applies where and to the extent that Company or its Sub-Processors Processes Personal Data on behalf of Licensee as a Processor in the course of providing the Services. The subject-matter of the data processing covered by this DPA is the provision of the Services. Schedule 1 of this DPA describes the nature and purpose of the processing, the types of Personal Data Company processes and the categories of data subjects whose Personal Data is processed. As between the parties, Company acts as a Processor and Licensee acts as a Controller of Personal Data. Company will process Personal Data only as a Processor on behalf of Licensee, and with respect to the CCPA, as a “service provider.” To the extent Company processes Personal Data on Licensee’s behalf, Company will comply with all Data Protection Laws applicable to Company as a Processor. The Company shall maintain and use Anonymous Data in a deidentified form and to not attempt to re-identify the Anonymous Data, except solely for the purpose of determining whether its deidentification processes satisfy the requirements of applicable law.

3. **Licensee Instructions**. Company will process Personal Data solely to provide the Services in accordance with the Agreement, or as otherwise required by applicable law and in accordance with Licensee’s documented instructions. Licensee will ensure its processing instructions are lawful and that the processing of Personal Data in accordance with such instructions will not violate Data Protection Laws. For the purposes of this DPA, the following is deemed an instruction by Licensee to process Personal Data (a) to provide and support the Services; and (b) as documented in the Agreement. The parties agree that the Agreement sets out Licensee’s complete and final instructions to Company for the Processing of Personal Data.

4. **Licensee's Processing Obligations**. Licensee agrees that it: (i) will comply with its obligations under Data Protection Laws with respect to its Processing of Personal Data; (ii) will make appropriate use of the Services to ensure a level of security appropriate to the content of the Personal Data; and (iii) has obtained all consents, permissions, and rights necessary under Data Protection Laws for Company to lawfully Process Personal Data in accordance with the Agreement. As between Licensee and Company, Licensee will be responsible for (i) the means by which Licensee acquired Personal Data and (ii) the accuracy, quality, and legality of the Personal Data provided to Company by or on behalf of Licensee.

5. **Authorized Sub-Processors.**

5.1. Authorization. Licensee agrees that Company may use Sub-Processors to Process Personal Data for the purpose of providing the Services to Licensee. Licensee specifically authorizes the engagement of those

Sub-Processors listed at Schedule 3 of this DPA and provides general written authorization to Company to engage Sub-Processors as necessary to perform the Services. Company will enter into a written agreement with the Sub-Processor imposing on the Sub-Processor data protection obligations comparable to those imposed on Company under this DPA with respect to the protection of Personal Data. If a Sub-Processors fails to fulfil its data protection obligations under such written agreement with Company, Company will remain liable to Licensee for the performance of the Sub-Processor's obligations under such agreement.

5.2. Changes to Sub-Processors. Company will notify Licensee of any new Sub-Processors in writing (as Licensee is required to be notified under the Agreement) at least thirty (30) days before such new Sub-

Processor processes Personal Data. Licensee may object to Company's appointment of the new SubProcessor within ten (10) days of Company's notice thereof, provided that such objection is in writing and provides reasonable grounds for such objection. If Licensee can reasonably demonstrate that the new SubProcessor is unable to Process Personal Data in compliance with the terms of this DPA and Company cannot provide an alternative Sub-Processor, or the parties are not otherwise able to achieve resolution, Licensee, as its sole and exclusive remedy, may terminate the Agreement only with respect to those portions of the Services which cannot be provided by Company without the use of the new Sub-Processor by providing written notice to Company, and then (1) Licensee will pay all amounts due for the Services up to the effective date of termination, and/or (2) Licensee will receive a prorated refund of amounts pre-paid to Company for Licensee's use of the Services for the remainder of the subscription term. If Licensee does not object to the engagement of a new Sub-Processor in accordance with this Section within ten (10) days of Company's notice or Company is able to overcome Licensee's objection or find another workaround, such Sub-Processor will be deemed authorized for the purposes of this DPA.

6. **Security**. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Company will implement reasonable technical and organizational safeguards designed to protect Personal Data in its possession or control against unauthorized loss, destruction, alteration, access, or disclosure. The Company shall take commercially reasonable steps to limit access to Personal Data to only Authorized Individuals. The Company shall ensure that all Authorized Individuals are made aware of the confidential nature of Personal Data and have executed confidentiality agreements. More specific security and privacy measures implemented by Workato include, but are not limited to, those set forth in Schedule 2 to this DPA.

7. **Transfer of Personal Data**.

7.1. Transfers Generally. The parties agree that Company may transfer Personal Data processed under this DPA outside the European Economic Area ("EEA"), UK, or Switzerland as necessary to provide the Services. If Company transfers Personal Data protected under this DPA to a jurisdiction that has not been found to provide an adequate or equivalent level of protection under the applicable Data Protection Laws, Company will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws. For purposes of this DPA, Licensee is the "controller", and Company is the "processor" of all Personal Data. Company may engage Sub-Processors pursuant to Section 5 (Authorized Sub- Processors) and Appendix 3 of the Standard Contractual Clauses will refer to Section 5 above.

7.2. Transfer Mechanisms. Regarding any transfers of Personal Data from the EEA to countries that do not provide adequate protection for such data (as determined by the applicable Data Protection Laws), the parties hereby enter into applicable Standard Contractual Clauses in support of such transfer.

7.2.1. *Transfers from the UK*. For transfers of Personal Data from the United Kingdom, the 2010 Standard Contractual Clauses are hereby incorporated by reference when they are available and are a valid transfer mechanism under applicable Data Protection Laws. The Parties further agree to the following provisions with respect to the 2010 Standard Contractual Clauses:

7.2.1.1. *Identity of the Parties:* The data exporter is Licensee, and the data importer is Company.

7.2.1.2. *Conflicts:* In the event of any conflict or inconsistency between this DPA and the 2010 Standard Contractual Clauses, the 2010 Standard Contractual Clauses will prevail.

7.2.1.3. *Appendices:* Responses to the Appendices to the 2010 Standard Contractual Clauses are provided in Schedules 1 and 2, attached hereto.

7.2.1.4. *Liability:* The parties do not incorporate the optional liability clause included in the 2010 Standard
Contractual Clauses.

7.2.2. *Transfers to Third Countries*. For all other transfers of Personal Data under this DPA to Third Countries, to the extent such transfers are subject to Data Protection Laws, the 2021 Standard Contractual Clauses are hereby incorporated by reference when they are available and are a valid transfer mechanism under applicable Data Protection Laws. The parties further agree to the following provisions with respect to the 2021 Standard Contractual Clauses:

7.2.2.1. *Identity of the Parties:* The data exporter is Licensee, and the data importer is Company. Module Two (controller to processor) is the sole module applicable to transfers involving Personal Data.

7.2.2.2. *Conflicts:* In the event of any conflict or inconsistency between this DPA and the 2021 Standard Contractual Clauses, the 2021 Standard Contractual Clauses will prevail.

7.2.2.3. *Appendices:* Responses to the Annexes to the 2021 Standard Contractual Clauses are provided in Schedules 1 and 2, attached hereto.

7.2.2.4. *Specific Provisions:*

7.2.2.4.1. In Clause 7, the parties do not permit docking.

7.2.2.4.2. In Clause 9, the parties select Option 2 and a time period of 30 days.

7.2.2.4.3. In Clause 11, the parties do not select the independent dispute resolution option.

7.2.2.4.4. In Clauses 17 (Option 2) and 18(b), the parties agree that the jurisdiction is the member state in which Controller is established, or if the Controller is not established in a member state, the Republic of Ireland.

7.3. Impact Assessments. Where applicable by virtue of Article 28(3)(f) of the GDPR or UK Data Protection Laws, Company will provide reasonable assistance to the Licensee with any data protection impact assessments which are referred to in Article 35 of the GDPR and with any prior consultations to any Supervisory Authority of the Licensee which are referred to in Article 36 of the GDPR, in each case solely in relation to Processing of GDPR Personal Data and taking into account the nature of the Processing and information available to Company.

8. **Requirements for CCPA.** For the purposes of the CCPA, the parties acknowledge and agree that Company will act as a "service provider" as such term is defined in the CCPA, in its performance of its obligations pursuant to the Agreement. Company will not retain, use, or disclose Personal Data for any purpose other than for the specific purpose of providing the Service, or as otherwise permitted by the CCPA. Company acknowledges and agrees that it will not retain, use, or disclose Personal Data for a commercial purpose other than providing the Services. Processing Personal Data outside the scope of this DPA or the Agreement will require prior written agreement between the Licensee and Company on additional instructions for processing. Company will not sell or share any Licensee Personal Data to another business or third party without the prior written consent of the Licensee. Notwithstanding anything else to the contrary, this Section 10 will only apply to the Processing of Personal Data by Company.

9. **Security Breach**. If Company discovers that a Security Breach has occurred, Company will notify Licensee promptly unless otherwise prohibited by law or otherwise instructed by a law enforcement or supervisory authority. Such notification will provide information about the nature and likely consequences of the Security Breach and how to request additional information if required. In addition to providing such notification, Company will promptly take reasonable steps to remediate the effects of the Security Breach and to stop the Security Breach from continuing to occur.

10. **Audits and Inspections**. Company uses external auditors to verify the adequacy of its security measures, including the security of the physical facilities from which Company provides the Services. This audit: (i) will be performed at least annually; (ii) will be performed according to ISO 27001 and/or SSAE 18 standards or substantially equivalent alternative standards; (iii) will be performed by independent third party security professionals at Company's selection and expense; and (iv) will result in the generation of a SOC 2 audit report ("Au**dit** Report"), which will be Company's Confidential Information. At Licensee's written request, and provided that the parties have applicable confidentiality terms in place, Company will provide Licensee with a copy of the Audit Report so that Licensee can verify Company's compliance with its obligations under this DPA. Licensee agrees that the Audit Report, together with any third-party certification (e.g., ISO 27001) maintained by Company, will be used to satisfy any audit or inspection requests by or on behalf of Licensee and to demonstrate compliance with applicable obligations of Company as set forth in this DPA.

11. **Data Subject Requests**. To the extent legally permitted, Company will promptly notify Licensee if Company receives a request from a Data Subject that identifies Licensee and seeks to exercise the Data Subject's right to access, rectify, erase, transfer, or port Personal Data, or to restrict the Processing of Personal Data ("**Data Subject Request**"). Company shall, at the request of the Licensee, and taking into account the nature of the Processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Licensee in complying with Licensee's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, provided that (i) Licensee is itself unable to respond without Company's assistance and (ii) Company is able to do so in accordance with all applicable laws, rules, and regulations. Licensee shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company. Licensee also understands that the Services provide Licensee with a number of controls that Licensee may use to assist it in responding to a Data Subject Request, and that Company likely does not have access to Licensee Data sufficient to respond to Data Subject Requests.

12. **Term and Termination**. This DPA will become effective upon the Effective Date of the Agreement ("**DPA Effective Date**") and expire on the earlier of: (i) an authorized termination in accordance with this DPA; (ii) the natural expiration or termination of the Agreement; or (iii) the execution of an updated DPA that supersedes this DPA. Either party may immediately terminate this DPA and the Agreement if the other party materially breaches any

provision of this DPA and fails to cure such breach within 30 days from the date of such party's written notice to the other party.

13. **Return or Destruction**. Upon termination or expiration of the Agreement for any reason, (i) Licensee may retrieve or delete all Personal Data, as may be further described in the Agreement, and (ii) Company may delete all Personal Data as described in the Agreement, unless otherwise required by applicable law.

14. **Limitation of Liability. The total liability of each of Licensee and Company (and their respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this DPA, whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the limitation of liability set forth in the Agreement.**

15. **General Terms**. This DPA will inure to the benefit of each party's permitted successors and assigns. Except in connection with a merger, acquisition, or sale of all or substantially all of a party's assets or voting securities, neither party may assign this DPA without the advance written consent of the other party. Any other transfer or assignment of this DPA except as expressly authorized under this Section will be null and void. This DPA and the Agreement is the entire agreement between Company and Licensee and supersedes all previous written and oral communications between the parties with respect to the subject matter hereof. The parties agree that this DPA will replace and supersede any existing data processing DPA that the parties may have previously entered into in connection with the Services. Except as provided by this DPA, the Agreement remains unchanged and in full force and effect. Except as updated by Company for the purpose of addressing changes to the Data Protection Laws, this DPA may only be amended in a writing signed by duly authorized representatives of the parties. If any provision of this DPA is held to be invalid or unenforceable, that provision will be limited to the minimum extent necessary so that this DPA will otherwise remain in effect. Any waiver or failure to enforce any provision of this DPA on one occasion will not be deemed a waiver of any other provision or of such provision on any other occasion. This DPA may be executed in the original or other electronic means. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement. Nothing in this DPA is intended to create an agency relationship between the parties.

16. **Priority of Terms**. To the extent there is a conflict between the Agreement and the terms of this DPA, the terms of this DPA will prevail in connection with the Processing of Personal Data.

SCHEDULE I DETAILS OF PROCESSING

For the purposes of the Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection:

A. PARTIES

Name of Licensee	
Role of Licensee	For purposes of the Agreements and this DPA, Licensee is the sole party that determines the purposes and means of processing Personal Data as the "business" or "controller." To the extent of any cross-border data transfers described in Schedule 1, Section C, Licensee is the data exporter.
Address	
Contact Person's Name, Position, and Contact Details	
Signature	
Date	

Role of Company	For purposes of the Agreements, Company processes Personal Data on behalf of Licensee as a "processor" or "service provider." To the extent of any cross-border data transfers, Company is the data importer.
Address	151 Calle de San Francisco Suite 200 PMB 1392 San Juan, PR 00901
Contact Person's Name, Position, and Contact Details	Daniel Barak (CEO) dan@myboi.com
Signature	/s Daniel Barak
Date	06/08/2024

B. PROCESSING TERMS

Duration of the processing	Company agrees to process Personal Data solely as instructed in the Agreement for the duration of the provision of the Services to Licensee, and the longer of such additional period as: (i) is specified in any provisions of the Agreements regarding data retention; and (ii) is required for compliance with law.
Nature of the processing	Such processing as is necessary to enable Company to comply with its obligations and exercise its rights under the Agreement, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction processing activities.
Purpose of the processing	Company agrees to process Personal Data for limited and specified purposes described in the Agreement, or as otherwise directed by authorized personnel of Licensee in writing (email acceptable).
Consideration in exchange for processing	The parties acknowledge and agree that Company receives no monetary or other valuable consideration in exchange for Personal Data.
Type of personal information processed	Data exporter may submit Personal Data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data: Login information and any other Personal Data Provided by Licensee to Company
Types of sensitive (or special) categories of personal information processed	N/A

Categories of data subjects	Licensee may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects: ● Prospects, Licensees, business partners, customers and vendors of Licensee (who are natural persons) ● Employees or contact persons of Licensee's prospects, Licensees, business partners and vendors ● Employees, agents, advisors, freelancers of Licensee (who are natural persons) Licensee's users authorized by Licensee to use the Service
Obligations and rights of the Parties	As set out in the Agreement.

C. CROSS BORDER DATA TRANSFERS

Description of activities relevant to the Personal Data transferred under the Standard Contractual Clauses	Company will process Personal Data in connection with providing its Services.
Categories of data subjects whose personal information is transferred	Licensee may submit Personal Data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects: ● Prospects, Licensees, business partners and vendors of Licensee (who are natural persons) ● Employees or contact persons of Licensee's prospects, Licensees, business partners and vendors ● Employees, agents, advisors, freelancers of Licensee (who are natural persons) ● Licensee's Users authorized by Licensee to use the Service
Types of personal information that will be transferred	Data exporter may submit Personal Data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:
Types of sensitive (or special) categories of personal information that will be transferred and applicable restrictions or safeguards	N/A
Frequency of the transfer	Continuous
Purpose of the data transfer and further processing	Provision of the Services as set forth in the Agreement.
Sub-processor transfers	Transfers to Sub-processors will occur where necessary for the provision of the Services in accordance with the Agreements solely for the term of the Agreement.
Competent Supervisory Authority	EEA Data Subjects: Republic of Ireland UK Data Subjects: United Kingdom

SCHEDULE 2
TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Company agrees that it:

1. Information Security Program: Implements a management-approved and regularly reviewed information security program that includes secure coding practices, vulnerability assessments, and risk management.

2. Access Control: Restricts Personal Data access to Authorized Individuals based on role and necessity, requiring unique authentication, preferably with multi-factor authentication. Access rights are regularly reviewed and updated upon role change or termination.

3. Physical Security: Ensures secure and monitored physical access to systems handling Personal Data, limited to essential personnel.

4. Data Encryption: Encrypts Personal Data both in transit and at rest using industry-standard protocols and algorithms.

5. Network Segregation and Management: Segregates internal systems processing Personal Data from public networks, employs network security components, and utilizes firewalls to control traffic.

6. Anti-Malware and System Monitoring: Installs anti-malware and monitoring capabilities on systems processing Personal Data, including audit logging and event log recording.

7. Incident Response and Notification: Maintains an incident response plan with specified actions for unauthorized data use or access, and commits to prompt notification in case of a Personal Data Breach.

8. Regular Security Testing: Conducts regular security assessments, including annual third-party penetration tests.

9. Sub-Processor Management: Evaluates and requires all Authorized Sub-Processors to adhere to equivalent security and privacy standards as the company. All Authorized Sub- Processors are required to implement and maintain the same or substantially similar technical and organizational measures and assume the same responsibilities and obligations as those required of Processor under this DPA.

10. Personnel Training: Ensures regular security and privacy training for personnel to maintain awareness of their data protection responsibilities.

11. Patch and Vulnerability Management: Deploys security updates based on risk and maintains a documented patch management process.

12. Business Continuity and Redundancy: Utilizes redundant services, regular backups, and documented business continuity policies to ensure data availability.

13. Data Protection Compliance: Maintains systems and processes for compliance with Data Protection Laws, including limited data retention and handling of Data Subject requests.

14. Defined Terms and Governance: Adheres to definitions of Personal Data, Security Incident, and Data Protection Laws, identifying a named Security Officer and assessing internal and external risks.

15. Remote and Key Access: Manages remote access with encryption and limits access to primary and backup keyholders for software updates and emergency role reassignment.

SCHEDULE 3
SUB-PROCESSORS

1. **Amazon Web Services (AWS)**
2. **FincenFetch (FF)**