DataRobot Data Processing Addendum
Incorporating EU Standard Contractual Clauses

This Data Processing Addendum ("**DPA**") is an exhibit to the Master Subscription Agreement and any other written agreements ("**Agreement**") between DataRobot, Inc. and Customer and sets forth the obligations of the parties with regard to the Processing of Personal Data pursuant to such Agreement.

1. Definitions

Unless otherwise defined below, all capitalized terms have the meaning given to them in the Master Subscription Agreement.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Customer Data" means data that is input into the Service or supplied to DataRobot by the Customer.

"Data Protection Laws" means (1) EC Regulation 2016/679 ("GDPR") on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and the EU e-Privacy Directive (Directive 2002/58/EC) (the "e-Privacy Directive") (collectively, "EU Data Protection Law"); and (2) the California Consumer Privacy Act of 2018 ("CCPA"); in each case, all of the foregoing as amended, replaced or supplemented from time to time, and all subordinate legislation made under them, together with any codes of practice, regulations or other guidance issued by the governments, agencies, data protection regulators, or other authorities in the relevant countries or jurisdictions.

"Data Subject" means the individual to whom Personal Data relates.

"Personal Data" means any Customer Data relating to an identified or identifiable natural person or household.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Processor" means the entity which processes Personal Data on behalf of the Controller.

"Standard Contractual Clauses (SCCs)" means the Standard Contractual Clauses which are the standard data protection clauses for the transfer of personal data to processors established in third countries as described in Art. 46 of the GDPR as from time to time varied, amended or substituted by the European Commission.

"Subprocessor" means a third party entity engaged by DataRobot or Affiliate as a Data Processor under this DPA.

"Supervisory Authority" means an independent public authority which is established by an EU Member State pursuant to the GDPR or by the applicable Data Protection Laws and Regulations in the EEA, Switzerland, and the UK.

"User" means an individual who is granted access to the Solution pursuant to the Agreement between Customer and DataRobot.

2. Processing of Personal Data

2.1 Scope and Role of the Parties. This DPA applies to the Processing of Personal Data by DataRobot in its role as a Processor to provide the Solution pursuant to the Agreement. For the purposes of this DPA, DataRobot and its Affiliates are the Processor and Customer is the Controller.

2.2 Instructions for Processing. DataRobot shall Process Personal Data in accordance with Customer's documented instructions. Customer instructs DataRobot to Process Personal Data to provide the Solution pursuant to the Agreement and this DPA.

2.3 Compliance with Laws. DataRobot shall comply with all Data Protection Laws applicable to DataRobot in its role as a Processor Processing Personal Data. Customer shall comply with all Data Protection Laws applicable to Customer as a Data Controller.

3. Subprocessors

3.1 Use of Subprocessors. Customer hereby agrees and provides a general prior authorization that DataRobot and DataRobot Affiliates may engage Subprocessors. DataRobot or its Affiliate engaging a Subprocessor shall ensure that such Subprocessor has entered into a written agreement that is no less protective than this DPA with respect to the protection of Personal Data, to the extent applicable to the nature of the services provided by such Subprocessor ("**Relevant Terms**"). DataRobot shall be liable to the Customer for the breach of any Subprocessors to the Relevant Terms that causes the Customer material injury.

3.2 Notification of New Subprocessors. A current list of Subprocessors for the Solution is available at www.datarobot.com/privacy/subprocessors ("**Subprocessor List**"). Customers may receive notice of any changes to the Subprocessor List by subscribing to updates at that webpage.

3.3 Subprocessor Objection Right. This Section shall apply only where and to the extent that Customer is established within the European Economic Area, the United Kingdom or Switzerland. Customer may object to DataRobot's use of a new Subprocessor by notifying DataRobot in writing within ten (10) business days after notice of an updated Subprocessor List. In that event, DataRobot will use commercially reasonable efforts to make available to Customer a change in the Solution or recommend a commercially reasonable change to Customer's use of the Solution to avoid Processing of Personal Data by the objected-to new Subprocessor without unreasonably burdening the Customer. If DataRobot is unable to make available such change within a reasonable period of time and cannot come to a reasonable, mutually agreed upon solution, Customer may terminate

only to those services which cannot be provided by DataRobot without the use of the objected-to new Subprocessor, by providing written notice to DataRobot. DataRobot will refund to Customer any prepaid fees for the terminated portion of the Solution.

4. Data Subject Rights

4.1 Assistance with Data Subject Requests. DataRobot will, in a manner consistent with the functionality of the Solution and DataRobot's role as a Processor, provide reasonable support to Customer to enable Customer to respond to Data Subject requests to exercise their rights under the Data Protection Laws ("**Data Subject Requests**").

4.2 Handling of Data Subject Requests. DataRobot will, to the extent legally permitted, promptly notify Customer via email if DataRobot receives a Data Subject Request from a Data Subject who is a User.

5. DataRobot Personnel

DataRobot will require DataRobot personnel (i) to process Personal Data in accordance with Customer's instructions as set forth in this DPA, (ii) to receive appropriate training on their responsibilities regarding the handling and safeguarding of Personal Data; and (iii) to be subject to confidentiality obligations which shall survive the termination of employment.

6. Personal Data Breach

DataRobot maintains security incident management policies and procedures and shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data ("**Breach**"). DataRobot shall make reasonable efforts to identify the cause of such Breach and take steps that DataRobot deems necessary and reasonable in order to remediate the cause of the Breach, to the extent the remediation is within DataRobot's control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Users.

7. Security Program

DataRobot shall implement appropriate technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data as set forth in **Appendix 2.**

8. Audits and Certifications

The Customer may exercise its right of audit under Data Protection Laws by requesting, on an annual basis, that DataRobot provide: (i) DataRobot's then current SOC 2 Type II audit report and DataRobot's ISO 27001 certification, or comparable industry standard reports and (ii) response to Customer's written questionnaires regarding security and privacy practices. In the event a Supervisory Authority requests or requires additional information in relation to DataRobot's Processing of Personal Data under this DPA, DataRobot will reasonably cooperate with the Customer and Supervisory Authority.

9. Return and Deletion of Personal Data

Within 30 days of termination of the Service, DataRobot will return or delete all Customer Personal Data that is not required to be retained pursuant to our legal and information security obligations. Customer Personal Data that is retained will be managed and deleted according to our Retention Policy.

10. Standard Contractual Clauses

10.1 **Incorporation.** The SCCs shall be deemed incorporated into this DPE by reference and shall apply between Customers established within the European Economic Area, the United Kingdom and Switzerland (as a "data exporter") and DataRobot, Inc. (as "data importer") subject to the requirements of Section 11.

10.2 **Appendices.** Appendices 1 and 2 to this DPA shall be deemed automatically incorporated into Appendices 1 and 2 of the SCCs.

10.3 **Audits.** For the purposes of Clause 5(f) of the SCCs, audits will be performed in accordance with Section 8 of this DPA.

10.4 **Subprocessors.** For purposes of Clause 11 of the SCCs, Customer consents to DataRobot appointing Subprocessors in accordance with Section 3 of this DPA.

10.5 **Return and Deletion of Personal Data.** For purposes of Clause 12(1) of the SCCs, DataRobot shall return and delete Customer's data in accordance with Section 9 of this DPA.

10.6 **Conflict.** For the avoidance of doubt, the parties agree that the terms of this section are not intended to amend or modify the SCCs. These provisions provide clarity in terms of DataRobot's business processes for complying with the SCCs. In the event of any conflict between the terms of this DPE and the provisions of the SCCs, the SCCs shall prevail.

10.7 **Subject Matter, Nature, Purpose and Duration of Data Processing.** DataRobot will Process Personal Data to provide the Solution. The duration of Processing Personal Data will be for the term of the Agreement.

11. General Provisions

11.1 **Applicability.** Customer shall not provide to DataRobot any Personal Data other than that specified in Appendix 1, in relation to DataRobot's role as a data Processor. In its consumption of the Solution, Customer shall not upload any model data that contains Personal Data.

11.2 **Notice.** All notices and communications related to this DPA shall be sent to the following email address: privacy@datarobot.com

11.3 **Customer Affiliates.** Customer is responsible for coordinating all communication with DataRobot on behalf of its Affiliates with regard to this DPA. Customer represents that it is authorized to

issue instructions as well as make and receive any communications or notifications in relation to this DPA on behalf of its Affiliates.

11.4 **Termination.** The term of this DPA will end simultaneously and automatically at the later of (i) the termination of the Agreement, or (ii) when all Personal Data is deleted from DataRobot systems.

11.5 **Conflict.** This DPA is subject to the non-conflicting terms of the Agreement. With regard to the subject matter in this DPA, in the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA shall prevail with regard to the parties' data protection obligations.

11.6 **Remedies.** Customer's remedies with respect to any breach by DataRobot or its Affiliates shall be subject to the limitation of liability contained in the Agreement.

Appendix 1
Description of Data Processing Activities

Data Exporter:

A DataRobot customer receiving the Solution as contemplated in the Agreement.

Data Importer:

DataRobot, Inc.

Data Subjects:

The personal data transferred concerns Customer's employees, agents, and contractors authorized to use the Solution.

Categories of Data:

The personal data transferred concerns the following categories of data:

- Name
- Email
- Company
- Connection information, including IP address, localization data and browser information

The personal data transferred does not include any special categories of data.

Appendix 2
Information Security Controls

Access Control
Users interact with the external interfaces of the DataRobot application via a web-based user interface or by programming against the DataRobot APIs using DataRobot client libraries or RESTful APIs; components required for these options communicate internally within the cluster with no external exposure. Additionally, and preferably, users can generate predictions using the DataRobot Prediction Server API, described below. Any required internet- based communications use TLS 1.2 to protect the confidentiality of the authentication process as well as the data in-flight.

WEB-BASED AUTHENTICATION
To log into the application website, users can choose to authenticate by providing a username and password or they can delegate authentication to Google. The authentication process is handled over HTTPS using TLS 1.2 to the application server. After the user sets their password, it is hashed and uniquely salted using SHA-512 and further protected with Password-Based Key Derivation Function 2 (BPKDF2). The original password is discarded.

When creating passwords, only printable ASCII characters may be used. Passwords must contain at least one capital letter and one number, and be between 8 and 512 characters. The username and password cannot be the same. A user has five attempts to authenticate successfully before DataRobot locks the account, and an administrator is needed to unlock it.

DataRobot also provides enhancements to password-based authentication, including support for multifactor authentication (MFA) with software tokens generated using Time-based One-time Password (TOTP).

API AUTHENTICATION
There are two different APIs used for communicating with the DataRobot platform. All API communications use TLS 1.2 to protect the confidentiality of authentication materials.

- DataRobot API. When interacting with the DataRobot API, authentication is performed using a bearer token contained in the HTTP Authorization header.
- Prediction Server API. When interacting with prediction servers via the API, authentication is performed using HTTP Basic Authentication with a username and an assigned API token for the password. An additional HTTP Header named “datarobot-key” is required to further limit access to the prediction servers.

Authorization
The Managed AI Cloud service is a multi-tenant solution, but data is partitioned at the project level. That is, DataRobot stores all file data under project ID locations and manages access control on a per-project basis. Data access is initially granted at the project level by the project creator (the owner), who can then assign specific roles and invite others to participate. Each role has a set of pre-defined capabilities, allowing careful control of who can see, modify, and delete projects. The DataRobot administrator can control user accounts, but has no access to user projects unless invited to participate by the owner.

Data Confidentiality
Data is secured at-rest using encryption. The Managed AI Cloud service uses the AWS S3 file system, which is secured with Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3). On top of file system encryption, all data transferred to and from AWS S3 is encrypted in transit using TLS 1.2 for metadata stores, along with password enablement. When using the DataRobot managed cloud environment, data sent to be trained or scored is transmitted encrypted with TLS 1.2 over the public internet. If your data submitted to DataRobot is subject to regulatory compliance (for example, HIPAA or PII) or has a classification that requires specific security controls, you may want to consider an On-Premise AI Cluster deployment, which can be further configured to meet your compliance needs. A separate instance of DataRobot Managed AI Cloud is hosted in the AWS EU (Ireland) region to support the unique data protection requirements of EU customers. DataRobot is Privacy Shield certified, which allows EU and Swiss personal business data to be processed in the US. However, personal data should not be uploaded into the Managed Cloud service.

Data Removal
DataRobot provides two options for deleting projects. Owners can delete projects so that they are removed from active project management listings. Completely removing the project, including the data used to build it, requires an administrator. Managed AI Cloud users wanting to permanently remove data would ask their primary DataRobot contact to file a ticket with DataRobot Support and request the data be removed. Additionally, for those projects mistakenly deleted from the active list, DataRobot Support has the capability to easily restore them.

Code and Component Security
DataRobot releases new code to the Managed AI Cloud almost every week. Each release is thoroughly vetted by a formal change management process, and robust validation, testing, and enterprise-grade quality assurance programs. For example, all code commits are subjected to more than 20,000 unique tests to compare known inputs to saved expected outputs. Results are analyzed by data scientists, data engineers, and software developers with significant data science expertise. If any change causes a deviation of more than six decimal points, the code will not be accepted.

In addition to the rigorous testing for each release, DataRobot blueprints (the logic that drives the thousands of tasks that go into a machine learning project) are automatically tested every night using a series of datasets that are carefully curated to utilize every major feature, and simulate the wide variety of use cases and dataset types that DataRobot would routinely encounter in a production environment. Any regressions in key metrics are carefully reviewed by our data science team.

Source code and binary artifacts for all third-party and internal modeling libraries are stored in an internal artifact repository. New and upgraded libraries are subjected to open source license review, build compatibility testing, and extensive performance and compatibility tests. Open source components are regularly scanned for known vulnerabilities and license compliance issues, and upgraded in accordance with our validation framework to deliver consistent and reliable results, with enterprise-grade security and regulatory compliance.

Physical Security
DataRobot is hosted on AWS, and Amazon's data centers are ISO 27001 certified, and have PCI/DSS Service Provider Level 1 and other certifications. Please refer to AWS Services in Scope for details of these certifications. AWS installs robust surveillance and detection in and around their data centers with

robust perimeter security, Closed Circuit Television (CCTV) cameras, multifactor authentication mechanisms, and intrusion detection.

Security Monitoring and Alerting
DataRobot uses many security tools to continuously monitor the production AWS/SaaS environment, including AWS GuardDuty at the network level and Sophos Endpoint Security at the instance level.

Disaster Recovery
Disaster recovery plans are reviewed on an annual basis, with accountability and responsibility led by our Chief Operating Officer. In the case of a business continuity event, DataRobot notifies customers through proper escalation channels.

Corporate Security
DataRobot requires card/badge system-controlled access to all DataRobot office areas and HR background checks for all employees. DataRobot ’s Managed AI Cloud service is SOC 2 Type II certified, ISO 27001 certified, and is working towards FedRAMP compliance.