

## PREDIBASE, LLC DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is incorporated into and forms part of the Predibase Service Agreement found here: <https://predibase.com/legal/service-agreement.pdf> or other mutually accepted written agreement between Predibase, LLC ("**Predibase**") and the customer entity ("**Customer**") that has executed such an agreement or has signed an order from referencing the Terms of Service (the "**Agreement**") for the use of the Predibase Service described in an order form (the "**Service**").

This DPA reflects the Parties' agreement with respect to the Processing of Customer Personal Data in the provision of the Predibase Service pursuant to the Agreement. In the event of any conflict or inconsistency between the terms of the Agreement and this DPA, the terms of this DPA shall prevail. For clarity, the terms of the SCCs will prevail over any other term in this DPA. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

### 1. DEFINITIONS

1.1. "**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 fifty percent (50%) of the voting interests of the subject entity.

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

1.3. "**Customer Personal Data**" means Customer Data that is Personal Data (defined below) owned or controlled by Customer and which Predibase, a Predibase Affiliate or Subprocessor may Process in the course of providing the Service.

1.4. "**Data Protection Laws**" means all laws and regulations, including laws and regulations of the European Union, the EEA and its member states, Switzerland, the United Kingdom, and the United States, (including without limitation, the U.S. Data Protection Laws) applicable to the Processing of Customer Personal Data under this DPA. For the avoidance of doubt, if Predibase's Processing involving Customer Personal Data is not within the scope of a given Data Protection Law, then such law is not applicable for purposes of this DPA.

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

1.6. "**Personal Data**", "**Personal Information**", and/or "**Personally Identifiable Information**", which shall be referred to individually or collectively in this DPA as "Personal Data", means (i) any information relating to an identified or identifiable natural person; and/or (ii) any information that identifies, relates to, describes, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Unless prohibited or specifically governed by Data Protection Laws, Personal Data shall not include information or data that is anonymized, de-identified and/or compiled on a generic basis and which does not name or identify a specific

person.

1.7. **"Personal Data Breach"** means a breach of Predibase's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.

1.8. **"Processor"** means an entity which is Processing Personal Data on behalf of the Controller.

1.9. **"Process" or "Processing"** means any operation or set of operations which is performed upon Customer Personal Data, whether or not by automatic means, such as 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.

1.10. **"Standard Contractual Clauses" or "SCCs"** means: (i) where the EU GDPR applies, the Standard Contractual Clauses, as described in Article 46 of the EU GDPR and approved by the European Commission decision 2021/914/EC, dated 4 June 2021, found at <https://predibase.com/legal> (ii) where the Swiss Data Protection Act applies, the applicable standard data protection clauses issued, approved or otherwise recognized by the Swiss Federal Data Protection and Information Commissioner ("FDPIC") (the "Swiss SCCs"); and (iii) or any set of clauses later approved by the European Commission which amend, replace or supersede such version.

1.11. **"Subprocessor"** means any party engaged by Predibase or a Predibase Affiliate to Process Customer Personal Data.

1.12. **"Supervisory Authority"** means an independent public authority which is established by an EU Member State or the UK pursuant to the GDPR.

1.13. **"UK"** means the United Kingdom of Great Britain and Northern Ireland.

1.14. **"UK Addendum"** means the template addendum issued by the UK ICO and laid before the UK Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as revised under Section 18, which amends the SCCs and can be found here: <https://predibase.com/legal>.

1.15. **"U.S. Data Protection Laws"** means any applicable United States (U.S.) privacy law or U.S. state privacy law or regulations relating to the protection of Personal Data, whether in existence as of the Effective Date or promulgated thereafter, as amended or superseded, subject to Section 12 (Changes in Law) herein.

**2. ROLES, SCOPE, AND DURATION.** The Parties acknowledge and agree that with respect to the rights and obligations under this DPA, Customer is the Controller and Predibase is the Processor of any Customer Personal Data, except when Customer acts as a Processor of

Personal Data, in which case Predibase is a Subprocessor. The scope and purpose of the Processing shall be to provide the Predibase Service to Customer pursuant to the Agreement. Predibase may Process certain Customer Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Customer Personal Data. Predibase shall not Process Customer Personal Data, except to perform and provide the Predibase Service and business operations relevant thereto, only in accordance with the terms of this DPA, Customer's Instructions (as defined below), and applicable Data Protection Laws. Predibase will Process Customer Personal Data for the Term of the Agreement, unless otherwise agreed to by the Parties in writing or pursuant to a requirement under Data Protection Laws. The categories of Data Subjects, the categories of Customer Personal Data, and the nature and purpose of Processing are set forth in Exhibit 1 of this DPA and Annex I to the SCCs, as applicable. To the extent that Customer is a "covered entity" or a "business associate", as such terms are each defined in the Health Insurance Portability and Accountability Act of 1996, as amended, and the regulations promulgated thereunder (collectively "HIPAA"), and the Customer Personal Data includes "protected health information" as defined under HIPAA, then execution of the Agreement to which this DPA is incorporated includes execution of the HIPAA Business Associate Agreement ("BAA") found on the Predibase Site.

**3. CUSTOMER INSTRUCTIONS** The Parties acknowledge and agree that for the purposes of this DPA, "Customer Instructions" means (i) the obligations and requirements set forth in this DPA and the Agreement; (ii) the applicable Documentation; (iii) Customer's use and configuration of the Predibase Service; and (iv) any additional written instruction Customer provides to Predibase, which Predibase agrees to in writing via an amendment to this DPA, regarding the Processing of any Customer Personal Data. In the event Predibase becomes aware that a Customer Instruction potentially infringes a Data Protection Law to which Predibase is subject, Predibase shall inform Customer of that legal issue before Processing, unless the applicable Data Protection Law prohibits such disclosure, including for reasons such as on the important grounds of public interest. For purposes of clarity, under this DPA, Predibase does not have a duty to investigate any Customer Instruction to determine whether it infringes any Data Protection Law. However, in the event Predibase notifies Customer of any potential infringement of an applicable Data Protection Law, the Parties will work together in good faith to resolve such issue in a timely manner. In no event will either Party be required to perform any activity that violates any applicable Data Protection Law. Customer will be responsible for all liability for all claims and damages arising from any Processing by Predibase in accordance with a Customer Instruction.

**4. PREDIBASE'S OBLIGATIONS.** Predibase shall limit access to Customer Personal Data to only those persons authorized by Predibase to Process Customer Personal Data and who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. When providing or making available Customer Personal Data to Predibase, Customer shall only disclose or transmit Customer Personal Data that is necessary for Predibase to perform the Predibase Service. Predibase will protect the confidentiality of Customer Personal Data through implementing and maintaining the technical and organizational security measures set out in the Data Security Schedule found in Exhibit 2 of this DPA ("Data

Security Schedule”) which take into account the state of the art of technology, the costs of implementation and the nature, scope, context and purposes of Processing, and the risk of varying likelihood and severity for the rights and freedoms of natural persons, and offers a level of security appropriate to the risk of the Processing of Customer Personal Data. The Data Security Schedule shall also serve as the applicable security measures required for an international transfer of Customer Personal Data under the SCCs. Predibase provides additional safeguards to Customer for the Processing of Customer Personal Data by Predibase on behalf of Customer within the scope of the GDPR, and additional redress to the Data Subjects to whom that Personal Data relates, as further described in Annex IV of the SCC’s (“Additional Safeguards”). Predibase shall notify Customer without undue delay, but in no event more than seventy-two (72) hours after becoming aware of any Personal Data Breach, and Predibase will take reasonable steps to: (i) identify the cause of such Personal Data Breach; and (ii) take the steps necessary and reasonable to remediate the cause of such Personal Data Breach to the extent such remediation is within Predibase’s reasonable control. To the extent Predibase has the information, Predibase will provide reasonable assistance to Customer with respect to Customer’s obligations under applicable Data Protection Laws, including without limitation, Article 33(3) of the GDPR.

**5. CUSTOMER’S OBLIGATIONS.** Customer is solely responsible for the accuracy and legality of Customer Personal Data provided to Predibase. Customer represents and warrants that it complies with all applicable Data Protection Laws, including without limitation, possessing all necessary rights to provide the Customer Personal Data to Predibase for the Processing to be performed in relation to the Predibase Service and Customer agrees that it shall be responsible for obtaining all necessary consents and providing all necessary notices to Data Subjects, as required under the relevant Data Protection Law. In addition, Customer is responsible for determining whether the Predibase Service is appropriate for the storage and Processing of Customer Personal Data subject to any specific Data Protection Law or regulation, as well as for the configuration and use of the Predibase Service, including any Customer Instructions, in a manner consistent with Customer’s legal and regulatory obligations.

## **6. AUDITS AND ASSISTANCE.**

6.1 Predibase undertakes to perform regular audits to verify its technical and organizational security measures. Such audits will be conducted: (i) by a qualified independent third party; (ii) at least annually; (iii) in accordance with SOC 2 or ISO 27001 standards or substantially equivalent standards; and (iv) will result in an audit report (“**Report**”). Upon Customer’s written request, and subject to the confidentiality obligations set forth in the Agreement, Predibase agrees to make available the Report and its applicable certifications in order to demonstrate the technical and organizational security measures implemented by Predibase.

6.2 Predibase will provide reasonable assistance to Customer so that Customer may comply with Customer’s obligations to perform a data protection impact assessment (or other assessments required under applicable Data Protection Laws) related to Customer’s use of the Predibase Service, to the extent Customer does not otherwise have access to the relevant information and to the extent such information is available to Predibase. Predibase shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in relation to this DPA, to the extent required by the

GDPR. Further, Predibase will take such steps as are reasonably required to assist Customer with its obligations under Articles 28(3)(h) and 32 to 36 of the GDPR and/or any applicable Data Protection Laws taking into account the nature of the Processing.

**7. DATA RETURN OR ERASURE.** Consistent with the Agreement, Predibase will return or delete all Customer Personal Data following the termination of the Agreement, unless such Customer Personal Data is required to be maintained by Data Protection Laws, in which case it shall be held in accordance with the terms of this DPA.

**8. SUBJECT ACCESS REQUESTS.** Taking into account the nature of the Processing related to the Predibase Service, Predibase will reasonably assist the Customer with Data Subject requests. For the avoidance of doubt Predibase will not respond directly to Data Subjects requests, but to the extent legally permissible, Predibase will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to any such request.

**9. SUBPROCESSORS.** Customer provides a general written authorization for Predibase to engage Subprocessors. Predibase shall maintain a current list of Subprocessors found here: <https://trust.predibase.com/subprocessors>. Predibase shall provide notification to Customer of any new Subprocessor(s) before authorizing such new Subprocessor(s) to Process Customer Personal Data. Customer may object in writing to Predibase's appointment of a new Subprocessor within thirty (30) days of such notice, provided that such objection is based on reasonable grounds relating to data protection. If Customer does not object to the appointment of any new Subprocessors within thirty (30) days after notification of such appointment by Predibase, Customer will be deemed as having provided its consent to the new appointment. If the Parties cannot resolve the objection, Customer may terminate the applicable portion of the Service that cannot be provided without the objected-to new Subprocessor. Such termination right is Customer's sole and exclusive remedy with respect to such objection. Predibase undertakes to enter into a written agreement with any applicable Subprocessors in accordance with the requirements under Data Protection Laws and such obligations will in no event be less protective than this DPA. Predibase will restrict the Subprocessors' access to Customer Personal Data to only that which is necessary to provide or maintain the Predibase Service. Predibase will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Subprocessors.

**10. INTERNATIONAL DATA TRANSFERS.** If the Processing of Customer Personal Data by Predibase involves a transfer of such data outside the EEA, UK, or Switzerland to a country not deemed to provide an adequate level of data protection, the Parties agree that such transfers shall be governed by the Standard Contractual Clauses (SCCs), or other permitted transfer mechanisms as allowed per the GDPR, to the extent agreed between the Parties, which shall be deemed incorporated into this DPA. For the purposes of the SCCs, Customer shall be the "data exporter" and Predibase shall be the "data importer." To the extent that the Standard Contractual Clauses apply pursuant to this DPA to Customer Personal Data transfers from the UK, the Parties agree that the UK Addendum (Attachment I to the SCCs) found at the following URL: <https://predibase.com/legal> which amends the Standard Contractual Clauses, will apply to all such transfers. In case of any transfers of Customer Personal Data from Switzerland to

Predibase in a third country, the following provisions apply: (i) general and specific references in the EU SCCs to the GDPR, or EU or Member State law, shall have the same meaning as the equivalent reference in the Swiss Data Protection Laws; (ii) in respect of data transfers governed by Swiss Data Protection Laws, the EU SCCs also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Protection Laws until such laws are amended to no longer apply to a legal entity; (iii) where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws, the FDPIC shall act as competent Supervisory Authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws; and (iv) for Data Subjects habitually resident in Switzerland, the courts of Switzerland are an alternative place of jurisdiction in respect of disputes.

## **11. SPECIFIC PROCESSING OBLIGATIONS AND CLARIFICATIONS**

**11.1. CCPA/U.S. State Privacy Laws.** To the extent applicable, Predibase will act as a "Service Provider" or "Processor." Predibase will not "sell" or "share" Customer Personal Data (as such terms are defined). Predibase will (i) not retain, use, or disclose Customer Personal Data for any purpose other than for the specific purpose of performing the Service specified in the Agreement, or as otherwise permitted by applicable Data Protection Laws, the Agreement or this DPA, (ii) retain, use, or disclose Customer Personal Data outside of the direct business relationship between Customer and Predibase, or (iii) combine Customer Personal Data with any Personal Data other than Customer Personal Data. Predibase will inform Customer if it can no longer comply with its obligations under this DPA. Upon notice to Predibase, Customer may take reasonable and appropriate steps to remediate Predibase's use of Customer Personal Data in violation of this DPA.

**11.2. Law Enforcement Access.** Predibase will not disclose or provide access to any Customer Personal Data Processed by Predibase under this DPA to a law enforcement agency, unless required by applicable law. If a law enforcement agency contacts Predibase with a demand for Customer Personal Data, Predibase will attempt to redirect the law enforcement agency to request that data directly from Customer. If Predibase is compelled to disclose or provide access to any Customer Personal Data Processed under this DPA to such law enforcement agency, Predibase will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so. Predibase further acknowledges that: (i) it has not purposefully created back doors (non-transparent access capabilities) or similar programming that could be used to enable unauthorized access of any Customer Personal Data or systems at Customer; (ii) it has not purposefully created or changed its business processes in a manner that facilitates unauthorized access to Customer Personal Data or systems at Customer; and (iii) no applicable laws require Predibase to create or maintain any back doors or facilitate unauthorized access to Customer Personal Data or systems at Customer, or for Predibase to be in possession of or hand over any third party encryption keys to decrypt Customer Personal Data.

**12. CHANGES IN LAW.** In the event of (i) any newly enacted Data Protection Law; (ii) any change to an existing Data Protection Law (including generally-accepted interpretations

thereof); (iii) any qualified and informed interpretation of a new or existing Data Protection Law; or (iv) any material new or emerging cybersecurity threat, which individually or collectively requires a change in the manner by which Predibase is delivering the Predibase Service to Customer, the Parties shall agree upon how Predibase's delivery of the Predibase Service will be impacted and shall make equitable adjustments to the terms of the Agreement and the Predibase Service.

## **EXHIBIT 1 TO THE DATA PROCESSING ADDENDUM**

### **Description of Processing of Customer Personal Data**

#### **A. Subject matter and duration of the Processing of Customer Personal Data:**

- **Subject Matter:** The Processing is for Predibase to provide the Service to Customer as set forth in the Agreement. This includes services for fine-tuning datasets and training, deploying, and serving machine learning models.
- **Duration:** The duration of the Processing shall be for the term of the Agreement between Predibase and Customer.

#### **B. The nature and purpose of the Processing of Customer Personal Data:**

- **Nature:** Processing activities include hosting, storing, copying, transmitting, modifying, and creating derivative works of Customer Data as necessary to provide the Service.
- **Purpose:** The purpose of the Processing is to enable Customer to use the Predibase platform to build, train, evaluate, and deploy custom machine learning and AI models, and to provide related support and maintenance services.

#### **C. The categories of Data Subjects to whom the Customer Personal Data relates:**

The categories of Data Subjects are determined and controlled by the Customer in its sole discretion. Depending on Customer's use of the Service, Data Subjects may include, but are not limited to, Customer's employees, contractors, customers, business partners, and end-users.

#### **D. The types of Customer Personal Data to be Processed:**

The types of Customer Personal Data are determined and controlled by the Customer in its sole discretion. Depending on Customer's use of the Service, Customer Personal Data may include, but is not limited to:

- Names
- Email addresses and other contact information
- Financial information
- Images, audio, video, and text data
- Professional and employment-related information
- Any other types of personal data that Customer chooses to include in the Customer Data it provides to the Service for Processing.



## **EXHIBIT 2 TO THE DATA PROCESSING ADDENDUM**

### **Data Security Schedule**

The Parties agree that the Data Security Schedule found at the following URL shall serve as the technical and organizational measures used to protect the confidentiality of the Customer Personal Data being Processed pursuant to this DPA: <https://predibase.com/legal>.