

# MongoDB Data Processing Agreement

Last updated: December 5, 2023. To see what has changed in this Agreement, [click here](#).

This Data Processing Agreement (“DPA”) is incorporated into and forms a part of the Cloud Subscription Agreement, Cloud Terms of Service, or other applicable service or subscription agreement between you and MongoDB with respect to your use of the Cloud Services (“MongoDB Agreement”). This DPA sets out data protection requirements with respect to the processing of Customer Personal Data (as defined below) that is collected, stored, or otherwise processed by MongoDB for the purpose of providing the Cloud Services. This DPA is effective on the effective date of the MongoDB Agreement, unless this DPA is separately executed in which case it is effective on the date of the last signature.

## 1. Definitions.

The following terms have the following meanings when used in this DPA. Any capitalized terms that are not defined in this DPA have the meaning provided in your MongoDB Agreement.

“Customer,” “you” and “your” means the organization that agrees to an Order Form, or uses the Cloud Services subject to the relevant MongoDB Agreement.

**“Customer Personal Data”** means any personal data that Customer uploads into the Cloud Services that is processed by MongoDB.

**“Data Protection Law”** means, to the extent applicable, (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (**“EU GDPR”**); (ii) the Data Protection Act 2018 and EU GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (**“UK GDPR”**); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); (iv) the Swiss Federal Act on Data Protection (**“FADP”**); (v) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (Cal. Civ. Code §§ 1798.100 to 1798.199.100), together with the CCPA Regulations (Cal. Code Regs. tit. 11, §§ 7000 to 7102) which may be amended from time to time (**“CCPA”**); and (vi) any other data protection legislation applicable to the respective party in its role in the processing of Customer Personal Data under the MongoDB Agreement.

**“Data Subject Request”** has the meaning given to it in Section 5.1.

**“EEA”** means the European Economic Area.

**“Subprocessor”** means any third-party data processor engaged by MongoDB to process Customer Personal Data.

**“Technical and Organizational Security Measures”** has the meaning given to it in Section 3.2.

The terms **“controller,” “data subject,” “personal data,” “personal data breach,” “processor,” “processing”** and **“supervisory authority”** have the meanings set forth in the EU GDPR.

## 2. Data Processing.

**2.1. Scope and Roles.** This DPA applies when MongoDB processes Customer Personal Data in the course of providing the Cloud Services. In this context, MongoDB is a “processor” to Customer, who may act as either a “controller” or “processor” with respect to Customer Personal Data.

## **2.2. Details of the Processing.**

**2.2.1. Subject Matter.** The subject matter of the data processing under this DPA is Customer Personal Data.

**2.2.2. Duration.** The duration of the data processing under this DPA is until the expiration or termination of the MongoDB Agreement in accordance with its terms.

**2.2.3. Nature and Purpose.** The purpose of the data processing under this DPA is the provision of the Cloud Services to Customer in accordance with the MongoDB Agreement.

**2.2.4. Types of Customer Personal Data.** The types of Customer Personal Data processed under this DPA include any Customer Personal Data uploaded to the Cloud Services by Customer.

**2.2.5. Categories of Data Subjects.** The data subjects may include Customer’s customers, employees, suppliers, and end users, or any other individual whose personal data Customer uploads to the Cloud Services.

**2.3. Compliance with Laws.** Each party will comply with all applicable Data Protection Law, including the EU GDPR, in relation to the processing of Customer Personal Data.

**2.4. MongoDB’s Processing.** MongoDB will process Customer Personal Data only for the purposes of: (i) provisioning the Cloud Services, (ii) processing initiated by Customer in its use of the Cloud Services, and (iii) processing in accordance with your MongoDB Agreement, this DPA, and your other

reasonable documented instructions that are consistent with the terms of your MongoDB Agreement. Any other processing will require prior written agreement between the parties.

**2.5. Customer Obligations.** Customer acknowledges that it controls the nature and contents of the Customer Personal Data. Customer will ensure that it has obtained all necessary and appropriate consents from and provided notices to data subjects where required by Data Protection Law to enable the lawful transfer of any Customer Personal Data to MongoDB for the duration and purposes of this DPA and the MongoDB Agreement.

### **3. Security.**

**3.1. Confidentiality of Personnel.** MongoDB will ensure that any of our personnel and any subcontractors who have access to Customer Personal Data are under an appropriate obligation of confidentiality.

**3.2. Security Measures.** We will implement appropriate technical and organizational security measures to ensure a level of security appropriate to the risks that are presented by the processing of Customer Personal Data. The current technical and organizational security measures are described at <https://www.mongodb.com/technical-and-organizational-security-measures> (“Technical and Organizational Security Measures”).

**3.3. Optional Security Controls.** MongoDB makes available a number of security controls, features, and functionalities that Customer may elect to use, as described in the Technical and Organizational Security Measures and our Documentation. Customer is responsible for implementing those measures to ensure a level of security appropriate to the Customer Personal Data.

**3.4. Breach Notification.** We will notify you without undue delay if we become aware of a personal data breach affecting Customer Personal Data.

## 4. Subprocessors.

**4.1. Authorized Subprocessors.** You acknowledge and agree that we may retain our affiliates and other third parties to further process Customer Personal Data on your behalf as Subprocessors in connection with the provision of the Cloud Services. We maintain a current list of our Subprocessors at: <https://www.mongodb.com/cloud/trust/compliance/subprocessors> which we will update at least 30 days before the addition or replacement of any Subprocessor. You may also register to receive email notifications of any change to our list of Subprocessors.

**4.2. Objections to Subprocessors.** In the event you have a reasonable objection to any new Subprocessor, either (A) we will instruct such Subprocessor not to process Customer Personal Data on your behalf and, if possible, continue to provide the Cloud Services in accordance with the terms of the MongoDB Agreement and any applicable Order Form, or (B) if we cannot provide the Cloud Services without the use of such Subprocessor, you may, as your sole and exclusive remedy, terminate this Agreement and any applicable Order Form and receive a refund of any prepaid fees for unused Subscriptions.

**4.3 Subprocessor Obligations.** MongoDB will impose on each Subprocessor the same data protection obligations as are imposed on us under this DPA. We will be liable to you for the performance of the Subprocessors' obligations to the extent required by Data Protection Law.

## 5. Data Subject Requests.

**5.1.** To assist with your obligations to respond to requests from data subjects, the Cloud Services provide Customer with the ability to retrieve, correct, or delete Customer Personal Data. Customer may use these controls to assist it in connection with its obligations under Data Protection Law, including its obligations related to any request from a data subject to exercise their rights under Data Protection Law (each, a “Data Subject Request”).

5.2. If a data subject contacts MongoDB with a Data Subject Request that identifies Customer, to the extent legally permitted, we will promptly notify Customer. Solely to the extent that Customer is unable to access Customer Personal Data itself, and MongoDB is legally permitted to do so, we will provide commercially reasonable assistance to Customer in responding to the Data Subject Request. To the extent legally permitted, Customer will be responsible for any costs arising from MongoDB's provision of such assistance, including any fees associated with the provision of additional functionality.

## **6. Requests for Customer Personal Data.**

6.1. If we receive a valid and binding legal order (“Request”) from any governmental body (“Requesting Party”) for disclosure of Customer Personal Data, we will use commercially reasonable efforts to redirect the Requesting Party to seek that Customer Personal Data directly from Customer.

6.2. If, despite our efforts, we are compelled to disclose Customer Personal Data to a Requesting Party, we will:

(a) if legally permitted, promptly notify Customer of the Request to allow Customer to seek a protective order or other appropriate remedy. If we are prohibited from notifying Customer, we will use commercially reasonable efforts to obtain a waiver of that prohibition;

(b) challenge any over-broad or inappropriate Request (including Requests that conflict with the law of the European Union); and

(c) disclose only the minimum amount of Customer Personal Data necessary to satisfy the Request.

**7. Cooperation.** Taking into account the nature of the processing and the information available to us, at your request and cost, MongoDB will provide reasonable assistance to ensure compliance with the

obligations under applicable Data Protection Law with respect to implementing appropriate security measures, personal data breach notifications, impact assessments and consultations with supervisory authorities or regulators, in each case solely related to processing of Customer Personal Data by MongoDB.

## **8. Customer Audit Rights.**

8.1. Upon Customer's request, and subject to the confidentiality obligations set forth in your MongoDB Agreement, MongoDB will make available to Customer (or Customer's independent, third-party auditor) information regarding MongoDB's compliance with the security obligations set forth in this DPA in the form of third-party certifications and audits.

8.2. If that information is not sufficient to demonstrate our compliance with the security obligations in the DPA, you may contact MongoDB in accordance with the notice provision of your MongoDB Agreement to request an on-site audit of MongoDB's procedures relevant to the protection of Customer Personal Data, but only to the extent required under applicable Data Protection Law. Customer will reimburse MongoDB for its reasonable costs associated with any such on-site audit. Before the commencement of any such on-site audit, Customer and MongoDB will mutually agree upon the scope, timing, and duration of the audit.

8.3. Customer will promptly notify MongoDB with information regarding any non-compliance discovered during the course of an audit, and MongoDB will use commercially reasonable efforts to address any confirmed non-compliance.

## **9. Data Transfers.**

9.1. **Data Deployment Locations.** Customer Personal Data will only be hosted in the region(s) that Customer chooses to deploy its database clusters in its configuration of the Cloud Services (the

“**Deployment Region**”). Customer is solely responsible for any transfer of Customer Personal Data caused by Customer’s subsequent designation of other Deployment Regions. When required by Data Protection Law, such transfers by Customer will be governed by the transfer mechanisms described in Section 9.3 below.

**9.2. Other Processing Locations.** You may choose to use certain optional features of the Cloud Services that require transfers of Customer Personal Data outside of the EEA, Switzerland or the United Kingdom. When required by Data Protection Law, such transfers will be governed by the provisions of Section 9.3 below.

**9.3. Transfer Mechanism.** MongoDB participates in and certifies compliance with the EU-US Data Privacy Framework, the UK Extension to the EU-US Data Privacy Framework, and the Swiss-US Data Privacy Framework (together, the “**DPF**”). As required by the DPF, MongoDB will (i) provide at least the same level of privacy protection to Customer Personal Data as is required by the DPF Principles, (ii) notify Customer if MongoDB makes a determination it can no longer meet its obligation to provide the same level of protection as is required by the DPF Principles, and (iii) upon notice, take reasonable and appropriate steps to remediate unauthorized processing of Customer Personal Data. Where the transfer of Customer Personal Data is from the EEA, Switzerland or the United Kingdom to a territory which has not been recognized by the relevant authorities as providing an adequate level of protection for personal data according to Data Protection Law, MongoDB agrees to process that Customer Personal Data in compliance with the provisions set out in Schedule 1 below, which forms an integral part of this DPA.

**10. Return or Deletion of Data.** Customer may retrieve or delete all Customer Personal Data upon expiration or termination of the MongoDB Agreement. Upon termination of your MongoDB Agreement or upon your request, MongoDB will delete any Customer Personal Data not deleted by Customer, unless we are legally required to store the Customer Personal Data.

**11. CCPA Obligations.** For purposes of this Section 11, Customer Personal Data shall include “personal information” (as that term is defined under CCPA) that Customer uploads into the Cloud Services that is processed by MongoDB. MongoDB is a “service provider” as defined in CCPA.

11.1. MongoDB will not:

11.1.1. retain, use, or disclose Customer Personal Data for any purpose other than providing the Cloud Services;

11.1.2. retain, use, or disclose Customer Personal Data outside of the direct business relationship between MongoDB and Customer;

11.1.3. sell or share Customer Personal Data (as the terms “sell” and “share” are defined in CCPA);  
or

11.1.4. combine Customer Personal Data with personal information that MongoDB has received from another MongoDB customer, except as permitted under CCPA.

11.2. We will notify you if we determine that we can no longer comply with our obligations as a service provider under CCPA.

11.3. You have the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information that is protected under CCPA.

## SCHEDULE 1 STANDARD CONTRACTUAL CLAUSES

1. For purposes of this Schedule 1, “Standard Contractual Clauses” means, as the circumstances may require, the applicable module(s) of the Standard Contractual Clauses approved by the European

Commission in decision 2021/914, or any subsequent versions of the Standard Contractual Clauses which may be adopted by the European Commission from time to time. Upon the effective date of adoption for any revised Standard Contractual Clauses by the European Commission, all references in this DPA to the “Standard Contractual Clauses” shall refer to that latest version thereof.

2. Pursuant to Section 9.3 of the DPA, where the transfer of Customer Personal Data is from the EEA, Switzerland or the United Kingdom to a territory which has not been recognized by the relevant authorities as providing an adequate level of protection for personal data according to Data Protection Law, then the Standard Contractual Clauses shall apply in accordance with this Schedule 1.

### **3. Incorporation of the Standard Contractual Clauses.**

3.1. When the Standard Contractual Clauses are the applicable transfer mechanism in accordance with Section 2 above, the parties agree that:

3.1.1 Clause 7 will not apply.

3.1.2 in Clause 9(a), Option 2 will apply, and the time period for prior notice of Subprocessor changes will be as set forth in Section 4.1 of the DPA.

3.1.3 in Clause 11(a), the optional language will not apply.

3.1.4 in Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by the law of the Republic of Ireland.

3.1.5 in Clause 18(b), disputes will be resolved before the courts of the Republic of Ireland.

3.2. For purposes of Annex I, Part A of the Standard Contractual Clauses (List of Parties):

### 3.2.1 Data Exporter: Customer.

- Contact Details: Customer's account owner email address, or to the email address(es) for which Customer elects to receive legal communications.
- Data Exporter Role: Data Exporter's role is outlined in Section 2 of the DPA.
- Signature & Date: By entering into the MongoDB Agreement, Data Exporter is deemed to have signed the Standard Contractual Clauses, including their Annexes and configured according to Section 3 of this Schedule I to the DPA, as of the effective date of the MongoDB Agreement.

### 3.2.2 Data Importer: MongoDB, Inc., on its own behalf and on behalf of its non-EEA Affiliates.

- Contact Details: MongoDB's DPO at [privacy@mongodb.com](mailto:privacy@mongodb.com).
- Data Importer Role: Data Importer's role is outlined in Section 2 of the DPA.
- Signature & Date: By entering into the MongoDB Agreement, Data Importer is deemed to have signed the Standard Contractual Clauses, including their Annexes and configured according to Section 3 of this Schedule 1 to the DPA, as of the effective date of the MongoDB Agreement.

## 3.3. For purposes of Annex I, Part B of the Standard Contractual Clauses (Description of Transfer):

### 3.3.1 The categories of data subjects are described in Section 2.2.5 of the DPA.

3.3.2 The forms of Customer Personal Data transferred are described in Section 2.2.4 of the DPA.

3.3.3 The frequency of the transfer is on a continuous basis for the duration of the MongoDB Agreement.

3.3.4 The nature and purpose of the processing is described in Section 2.2.3 of the DPA.

3.3.5 The period of retention of Customer Personal Data in relation to the processing will end upon termination of the MongoDB Agreement.

3.3.6 For transfers to Subprocessors, the subject matter and nature of the processing is described at: <https://www.mongodb.com/cloud/trust/compliance/subprocessors>. The duration of processing by Subprocessors is the same as by Data Importer.

3.4. For purposes of Annex I, Part C of the Standard Contractual Clauses (Competent Supervisory Authority), the competent supervisory authority/ies shall be determined in accordance with EU GDPR and Clause 13 of the Standard Contractual Clauses.

3.5. Sections 3 and 4.3 of the DPA contain the information required under Annex II of the Standard Contractual Clauses (Technical and Organizational Measures).

3.6. In addition to the above stipulations, each of the following forms part of the Standard Contractual Clauses and sets out the parties' understanding of their respective obligations under the Standard Contractual Clauses:

3.6.1 Clause 8.9 of the Standard Contractual Clauses: Audit. Data Exporter acknowledges and agrees that it exercises its audit right(s) under Clause 8.9 by instructing Data Importer to comply with the audit measures described in Section 8 (Customer Audit Rights) of the DPA.

3.6.2 Clause 9(c) of the Standard Contractual Clauses: Disclosure of Subprocessor agreements. The parties acknowledge that, pursuant to subprocessor confidentiality

restrictions, Data Importer may be restricted from disclosing onward subprocessor agreements to Data Exporter. Even where Data Importer cannot disclose a subprocessor agreement to Data Exporter, the parties agree that, upon the request of Data Exporter, Data Importer shall (on a confidential basis) provide all information it reasonably can in connection with such subprocessing agreement to Data Exporter.

3.6.3 Clause 12 of the Standard Contractual Clauses: Liability. To the greatest extent permitted under Data Protection Law, any claims brought under the Standard Contractual Clauses will be subject to any aggregate limitations on liability set out in the MongoDB Agreement.

#### **4. Transfers of Customer Personal Data Protected by FADP.**

4.1. With respect to transfers of Customer Personal Data protected by FADP, the Standard Contractual Clauses will apply in accordance with Sections 2 and 3 above, with the following modifications:

4.1.1 any references in the Standard Contractual Clauses to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to FADP;

4.1.2 references to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be; and

4.1.3 references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner and competent courts in Switzerland.

#### **5. Transfers of Customer Personal Data Protected by UK GDPR.**

5.1. With respect to transfers of Customer Personal Data protected by UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued under S119A(1) Data Protection Act 2018 (“UK Addendum”), shall apply and be incorporated by reference into this DPA, with Part 1: Tables completed in accordance with the applicable stipulations in Section 3 of this Schedule 1. Either data exporter or data importer may terminate the UK Addendum pursuant to Section 19 of the UK Addendum if, after a good faith effort by the parties to amend the DPA to account for the approved changes and any reasonable clarifications to the UK Addendum, the parties are unable to come to agreement. To the extent of any conflict between Section 3 of this Schedule 1 and any mandatory clauses of the UK Addendum, the UK Addendum shall govern to the extent UK GDPR applies to the transfer.