# Technische und organisatorische Maßnahmen (TOMs)
# Maddox AI GmbH

Version: 3.1

Stand: 25.03.2024

# I. Allgemeine Hinweise

## 1. Rechtlicher Hintergrund

Die EU-Datenschutzgrundverordnung (**DSGVO**) schreibt vor, dass jeder Verantwortliche sowie Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen muss, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Als Teil der Erfüllung unserer Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO dokumentieren wir im vorliegenden Dokument die von uns gem. Art. 25 und 32 DSGVO getroffenen technischen und organisatorischen Maßnahmen.

## 2. Inhalt und Stand des Dokumentes

Dieses Dokument wurde zuletzt am 25.03.2024 aktualisiert.

Unter Ziff. II werden die technischen und organisatorischen Maßnahmen aufgeführt, die die Maddox AI GmbH (nachfolgend **„Maddox AI**“) in Ihrem eigenen Kontrollbereich unmittelbar selbst umsetzt.

Hiervon abzugrenzen sind technische und organisatorischen Maßnahmen, die die von Maddox AI eingesetzten Dienstleister ihrerseits ergreifen, um für die von ihnen übernommenen Datenverarbeitungen ein angemessenes Schutzniveau zu gewährleisten.

Als innovatives Start-Up im Bereich der KI-basierten Qualitätssicherung bedient sich Maddox AI in verschiedenen Bereichen spezialisierter IT-Dienstleister, auch weil spezialisierte Anbieter erfahrungsgemäß besonders hohe Sicherheitsstandards gewährleisten können. Der Einsatz von spezialisierten IT-Dienstleistern mit besonders hohen Sicherheitsstandards ist insofern ein wichtiger Baustein im IT-Sicherheits- und Datenschutzkonzept von Maddox AI.

Die umfangreichen technischen und organisatorischen Maßnahmen der eingesetzten Dienstleister erhöhen das Schutzniveau der unter Verantwortung von Maddox AI verarbeiteten Daten weiter und werden unter Ziff. III. aufgeführt.

## 3. Änderungsnachweise

| Hinweis zur Vergabe von Versionsnummern | |
|---|---|
| 0.1 – 0.9 | Das Dokument befindet sich im Entwurfsstadium |
| 1.0 | Bezeichnet die erste freigegebene Version |
| Inhaltliche Änderungen | Bei inhaltlichen Änderungen sollte die erste Ziffer erhöht werden (z.B. Version 2.0 nach grundlegender Überarbeitung der Version 1.6) |
| Kleinere Korrekturen | Bei Berichtigung von Fehlern (z.B. Rechtschreibung) ohne Auswirkung auf den Inhalt oder minimalen inhaltlichen Änderungen sollte dagegen nur die zweite Ziffer erhöht werden (z.B. Version 1.7 nach kleineren Korrekturen der Version 1.6) |

| | | | |
|---|---|---|---|
| Version | Datum | Autor | Kurzbeschreibung der Änderung / Änderungsgrund |
| 3.0 | 22.03.2024 | Cornelius Widmaier | Erstellung Version 3 der TOMs |
| 3.1 | 25.03.2024 | Julian Schneider | Anpassung und Übersetzung |

# II. Technische und organisatorische Maßnahmen - Maddox AI GmbH

## 1. Vertraulichkeit (Art. 32 Abs.1 lit. b DSGVO, Art 5 Abs. 1 lit. f DSGVO)

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten gewährleistet. Das Unternehmen hat geeignete technische und organisatorische Maßnahmen getroffen für den Schutz personenbezogener Daten

- vor unbefugter oder unrechtmäßiger Verarbeitung,
- vor unbeabsichtigtem Verlust,
- vor unbeabsichtigter Zerstörung und
- vor unbeabsichtigter Schädigung.

### a. Zutrittskontrolle

Geeignete Maßnahmen der Zutrittskontrolle **verwehren unbefugten Personen physisch den Zutritt** zu Datenverarbeitungsanlagen. Sie stellen sicher, dass nur autorisierte Personen Zutritt zu den Datenverarbeitungsanlagen erhalten.

Wirksame Zutrittskontrollmaßnahmen minimieren insbesondere folgende Risiken:

- Verlust/Zerstörung/Beschädigung von Datenverarbeitungsanlagen
- unrechtmäßige oder unbefugte Verarbeitung wie z.B. Einsichtnahme

Maddox AI ergreift unter anderem die folgenden Maßnahmen, um den unbefugten Zutritt zu Datenverarbeitungsanlagen (insbes. Notebooks; Festplatten, IT-Server) zu verhindern:

*(1) Technische Maßnahmen*

Zutrittssicherung Serverraum

Manuelles Schließsystem (z.B. Türschlösser)

Automatisch zufallende und schließende Türen

Sicherheitsschlösser

Verschließen nach außen öffnender Türen

Zutrittssicherung Gebäudetechnik (z.B. Verteilerräume für Netzwerk oder elektrische Verteiler)

*(2) Organisatorische Maßnahmen*

Schlüsselregelung und -dokumentation für Geschäftsräume

Schließordnung (Regelung betreffend Öffnen und Verschließen von Gebäuden und Räumen)

Führen einer zentralen Besucherliste

Besucher nur in Begleitung von Mitarbeitern

Richtlinie/Anweisungen für Zutritt Externer

Richtlinie/Anweisungen für Umgang mit Besuch

## b. Zugangs- und Benutzerkontrolle

Die Zugangskontrolle soll die **unbefugte Nutzung von Datenverarbeitungssystemen verhindern**, so dass nur autorisierte Personen Zugang zu Datenverarbeitungssystemen erhalten und diese Systeme nutzen können. Wirksame Zutrittskontrollmaßnahmen minimieren insbesondere folgende Risiken:

- Verlust/Zerstörung/Beschädigung von Datenverarbeitungsanlagen
- unrechtmäßige oder unbefugte Verarbeitung wie z.B. Einsichtnahme

Maddox AI ergreift diesbezüglich unter anderem folgende Maßnahmen:

*(1) Technische Maßnahmen*

Benutzer-Authentifikation (Name und Passwort)

Zugangssicherung Netzwerk (Kabelverbindung)

Sachkundiger Einsatz von Anti-Viren-Software

Automatische Desktopsperre (nach 5 Minuten)

Zugangssicherung des WLAN

Zugangssicherung des firmeninternen Kabelnetzwerks (auch bei Herstellung eines Kabelanschlusses erhalten nur registrierte Geräte Zugang zum Netzwerk)

Intrusion Prevention System

Einrichtung einer Zwei-Faktor Authentifizierung

Automatische Aktualisierung der Betriebssysteme von Endgeräten durch regelmäßige Updates/Patches

Verschlüsselung von Datenträgern in Laptops/Notebooks und Mobiltelefonen

Verschlüsselung von sonstigen Datenträgern (z.B. USB-Sticks, externen Festplatten)

*(2) Organisatorische Maßnahmen*

Passwortvergabe/Passwortregeln (die Vergabe der Passwörter basiert auf einer gültigen Passwortrichtlinie)

Regelmäßige Änderung von Passwörtern

Unmittelbare Änderung der Standardkennwörter auf allen Geräten

Unmittelbare Sperrung und Löschung des Zugangs nach Ausscheiden des Mitarbeiters

Registrierung aller ausgegebenen Endgeräte, um die Ausgabe nachzuvollziehen und Geräte im Bedarfsfall von den Mitarbeitern zurückfordern zu können

Unmittelbare Rücknahme von ausgegebenen Endgeräten nach Ausscheiden eines Mitarbeiters

Sorgfältige Verwaltung der Benutzerberechtigungen

Richtlinie für den Arbeitsplatz

Richtlinie zur Löschung/Vernichtung von Dokumenten mit personenbezogenen Daten

Prokollierung des Zugriffs auf Datenverarbeitungssysteme

Clear Desktop Policy

Richtlinie für den Umgang mit Smartphones

Richtlinie für den Umgang mit Laptops/Tablets

Richtlinie für Homeoffice

## c. Zugriffs-, Daten und Speicherkontrolle

Zugriffskontrollmaßnahmen sollen gewährleisten, dass ein Benutzer des Datenverarbeitungssystems ausschließlich auf solche personenbezogenen Daten **Zugriff** erhält, zu deren Verarbeitung eine **Berechtigung** vorliegt. Eine wirksame Zugriffskontrolle minimiert folgende Risiken:

- unbefugte Einsichtnahme bei Verarbeitung und Nutzung,
- unbefugtes Kopieren,
- unbefugte Veränderung und
- unbefugte Löschung.

Maddox AI ergreift unter anderem die folgenden Maßnahmen, um ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Daten innerhalb des Systems zu verhindern:

### *(1) Technische Maßnahmen*

Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

Änderungen an Dateien sind individuellen Benutzern zugeordnet

Datenschutzkonforme Vernichtung von Endgeräten und Speichermedien durch eine Spezialfirma

Physische Zerstörung von Datenträgern

Abschließbare Dokumentenschränke

*(2) Organisatorische Maßnahmen*

Sorgfältige Vergabe von Zugriffsberechtigungen auf Basis eines Berechtigungskonzeptes

Berechtigungskonzept basiert auf dem Need-to-know-Prinzip

Zugriffsberechtigungen sind auf den minimal erforderlichen Personenkreis beschränkt

Übereinstimmung von Zugriffsberechtigungen „digital und analog“

Formaler Prozess für Erteilung von Zugriffsberechtigungen

Anzahl der Administratoren ist auf ein Mindestmaß reduziert

Anweisung Entsorgung von Papierdokumenten, Datenträgern und Endgeräten

Clear Screen Clear Desk Policy

Vertraulichkeitsverpflichtung von Mitarbeitern

Passwortvergabe/Passwortregeln (die Vergabe der Passwörter basiert auf einer gültigen Passwortrichtlinie)

Regelmäßige Änderung von Passwörtern

## d. Trennungskontrolle (Sicherstellung der Trennung zu unterschiedlichen Zwecken erhobener Daten)

Maßnahmen der Trennungskontrolle sollen gewährleisten, dass personenbezogene Daten, die zu unterschiedlichen Verarbeitungszwecken erhoben wurden, **zweckgebunden und getrennt** verarbeitet werden. Außerdem gewährleistet die Trennungskontrolle die Mandantenfähigkeit der Verarbeitungsvorgänge, insoweit dies erforderlich ist (z.B. bei Nutzerkonten einer Online-Plattform). Eine wirksame Trennungskontrolle minimiert folgende Risiken:

- unbefugte Einsichtnahme personenbezogener Daten,
- Verarbeitung von personenbezogenen Daten in einer nicht mit den Verarbeitungszwecken zu vereinbarenden Weise.

Maddox AI ergreift unter anderem die folgenden Maßnahmen, um eine getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, sicherzustellen:

*(1) Technische Maßnahmen*

Physikalische Trennung von Datenbanken/Datenträgern

Wirksame, softwarebasierte Trennung unterschiedlicher Datenpools

Trennung von Produktiv- und Testsystem

*(2) Organisatorische Maßnahmen*

Verwaltung von Benutzerberechtigungen für Datenbanken/Anwendungen

Verzeichnis von Verarbeitungstätigkeiten

Anweisung zur Trennung privater und betrieblicher Daten

## 2. Integrität (Art. 32 Abs. 1 lit. b DSGVO, Art 5 Abs. 1 lit. f DSGVO)

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die **eine angemessene Sicherheit** gewährleistet. Maddox AI hat geeignete technische und organisatorische Maßnahmen getroffen für den Schutz personenbezogener Daten

- vor unbefugter oder unrechtmäßiger Verarbeitung,
- vor unbeabsichtigtem Verlust,
- vor unbeabsichtigter Zerstörung und
- vor unbeabsichtigter Schädigung.

### a. Weitergabekontrolle

Die Weitergabekontrolle verhindert, dass personenbezogene Daten bei der elektronischen **Übertragung** oder während ihres Transports oder ihrer Speicherung auf Datenträgern **unbefugt gelesen, kopiert, verändert oder entfernt** werden.

Außerdem wird im Rahmen der Weitergabekontrolle überprüfbar dokumentiert, welche Empfänger personenbezogene Daten erhalten dürfen.

Maddox AI ergreift unter anderem die folgenden Maßnahmen, um ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Daten bei elektronischer Übertragung oder Transport zu verhindern:

*(1) Technische Maßnahmen*

Verschlüsselte E-Mail-Kommunikation (z.B. S-MIME)

Verschlüsselte Datenübertragung im Internet unter Nutzung aktueller Verschlüsselungsprotokolle (z.B. TLS 1.3, HTTPS, SFTP, etc.)

Sicherer Transport von Datenträgern (sicherer Transportbehälter)

Einsatz digitaler Signaturverfahren für Dokumente (z.B. digitale Unterschrift auf PDF)

*(2) Organisatorische Maßnahmen*

Richtlinie für den Umgang mit Smartphones

Richtlinie für den Umgang mit Laptops/Tablets

Richtlinie für Homeoffice

Sorgfältige Auswahl von Dienstleistern

Physische Datenweitergabe nur gegen Beleg

Anweisung Entsorgung von Papierdokumenten, Datenträgern und Endgeräten

Anweisung zur Prüfung des Adressaten

Übersicht elektronischer/automatischer Datenübermittlungen

Protokollierung der Abruf- und Übermittlungsvorgänge

Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. Löschfristen

## b. Eingabekontrolle

Maßnahmen der **Eingabekontrolle** sollen gewährleisten, dass **nachträglich überprüft** und festgestellt werden kann, ob und wie personenbezogene Daten eingegeben, verändert oder entfernt worden sind, um die **Richtigkeit** und Integrität der personenbezogenen Daten sicherstellen zu können.

Maddox AI ergreift unter anderem die folgenden Maßnahmen, um festzustellen, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

*(1) Technische Maßnahmen*

Automatisches Protokollieren von Änderungen und Eingaben der Nutzer mit Zeitstempel

Protokollieren von Löschvorgängen

Kollisionsprüfung bei Datenbanken

*(2) Organisatorische Maßnahmen*

Zuständigkeit für Löschung definiert

Sorgfältige Vergabe von Eingabe-, Änderungs- und Löschrechten auf Basis des Berechtigungskonzeptes (s. zum Berechtigungskonzept auch unter Zugriffs-, Daten und Speicherkontrolle)

## 3. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO)

Durch die in Art. 32 Abs. 1 lit. a DSGVO vorgesehene **Pseudonymisierung** werden die Möglichkeiten reduziert, vorhandene Daten einzelnen natürlichen Personen zuzuordnen. Darin liegt eine **wichtige Sicherheitsmaßnahme** zum Schutz personenbezogener Daten.

Maddox AI ergreift zum Zwecke der Pseudonymisierung u.a. folgende Maßnahmen:

Datensätze werden, wenn eine Anonymisierung nicht möglich ist, möglichst in pseudonymisierter Form weitergegeben

## 4. Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO)

Art. 32 Abs. 1 lit. a DSGVO zeigt die **Verschlüsselung** von personenbezogenen Daten als **wichtige Maßnahme** zum Schutz der Sicherheit personenbezogener Daten auf.

Maddox AI ergreift u.a. folgende Verschlüsselungsmaßnahmen:

### a. Technische Maßnahmen

Verschlüsselung von Datenträgern in Laptops/Notebooks und Mobiltelefonen

Verschlüsselung von sonstigen Datenträgern (z.B. USB-Sticks, externen Festplatten)

Verschlüsselte E-Mail-Kommunikation (z.B. S-MIME)

Verschlüsselte Datenübertragung im Internet unter Nutzung aktueller Verschlüsselungsprotokolle (z.B. TLS 1.3, HTTPS, SFTP, etc.)

Verschlüsselung von Back-Ups

### b. Organisatorische Maßnahmen

Richtlinie zum Umgang mit Verschlüsselungsmöglichkeiten

Regelmäßige Überprüfung der Wirksamkeit ergriffener Verschlüsselungsmaßnahmen

## 5. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Es wird gewährleistet, dass **personenbezogene Daten gegen Zerstörung, oder Verlust geschützt** sind. Eine wirksame Verfügbarkeitskontrolle stellt sicher, dass personenbezogene Daten zu den erforderlichen Zeiten auch tatsächlich verfügbar sind.

Maddox AI ergreift unter anderem die folgenden Maßnahmen zum Schutz der Daten gegen zufällige Zerstörung bzw. Verlust:

### a. Technische Maßnahmen

Brandschutzmaßnahmen

Feuerlöschgeräte in Geschäftsräumen

Überspannungsschutz des Gebäudes gegen Blitzeinschlag

Digitalisieren von Dokumenten in Papierform

Unterbrechungsfreie Stromversorgung

Automatisches Benachrichtigungssystem bei Erreichung der maximalen Auslastung

bevorzugte Verwendung von Endgeräten mit Akku zur Überbrückung von Stromausfällen

### b. Organisatorische Maßnahmen

Auslagerung der Datenserver an spezialisierte Anbieter mit hohem Sicherheitsstandard, redundanten Systemen und automatisierten Datensicherungen

Durchgeführte Risiko- und Schwachstellenanalyse

Planung von Kapazität und Betriebsmitteln

Notfallhandbuch für IT-Vorfälle vorhanden

Notfallplan für IT-Vorfälle vorhanden

## 6. Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Es wird sichergestellt, dass Daten nach Zwischenfällen **rasch wiederherstellbar** sind.

Maddox AI ergreift unter anderem die folgenden Maßnahmen, um eine Wiederherstellung von Daten zu ermöglichen:

### a. Technische Maßnahmen

automatisierte zyklische Durchführung einer Backup-Routine

Externe Back-Ups (z.B. Dienstleister)

### b. Organisatorische Maßnahmen

Backup- und Recovery-Konzept vorhanden

Anweisung zur regelmäßigen Sicherung lokal gespeicherter Daten

Regelmäßige Überprüfung der Wiederherstellbarkeit

## 7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d, Art. 25 DSGVO)

Es wurden insbesondere folgende Verfahren zur regelmäßigen **Überprüfung, Bewertung und Evaluierung der Wirksamkeit** der technischen und organisatorischen Maßnahmen eingerichtet.

### a. Datenschutz-Management (Datenschutzgerechte Betriebsorganisation)

Maddox AI ergreift unter anderem die folgenden Maßnahmen, um die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird:

*(1) Technische Maßnahmen*

Einsatz von Monitoring-Anwendungen

Einsatz von Datenschutz-Management-Software

Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz (Mitarbeiterwiki/ Intranet)

Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen (z.B. Widerspruchs-Links auf Websites oder in Newsletter-E-Mails

*(2) Organisatorische Maßnahmen*

Regelmäßige Überprüfung Zutrittskontrollmaßnahmen

Jährliche Schulung der MitarbeiterInnen im Datenschutz

Verpflichtungen von MitarbeiterInnen auf die Vertraulichkeit

Regelmäßige Sensibilisierung der Beschäftigen bzgl. Datenschutz, insbes. zur Vermeidung von Cyberangriffen mittels Social-Engineerings

Bestellung eines/einer Datenschutzbeauftragten

Bestellung eines/einer IT-Sicherheitsbeauftragten

Jährliche Überprüfung technischer und organisatorischer Maßnahmen

Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklung berücksichtigt (Art. 25 Abs. 2 DSGVO)

Definierter Prozess zur Meldung von Datenschutzvorfällen

Definierter Prozess zur Erfüllung von Betroffenenrechten

Löschkonzept ist vorhanden

Eingesetzte Software ermöglicht die Löschung von Daten

Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind

Datenschutzfreundliche Voreinstellungen bei verwendeter Software

Soweit möglich und sinnvoll werden für die Datenverarbeitung spezialisierte IT-Dienstleister mit hohen Sicherheitsstandards eingesetzt

Regelmäßige Überprüfung, ob für alle Endgeräte die erforderlichen Updates und Patches der Betriebssysteme installiert wurden

Regelmäßige Überprüfung, ob die Betriebssysteme von Geräten der unternehmensinternen IT-Infrastruktur (z.B. eigene Server, Router) auf dem neusten Stand sind

## b. Auftragskontrolle

Maddox AI ergreift unter anderem die folgenden Maßnahmen, um die **weisungsgemäße** Verarbeitung von Daten im Auftrag sicherzustellen:

Sorgfältige Auswahl von Auftragsverarbeitern

Vorherige Prüfung der TOM jedes (weiteren) Auftragsverarbeiters

Mit eingesetzten Auftragsverarbeitern wurden Vereinbarungen zur Auftragsverarbeitung (AVV) abgeschlossen

Eine eindeutige Vertragsgestaltung zwischen Auftraggebern und Auftragnehmern zur Datenverarbeitung personenbezogener Daten ist erfolgt

Regelungen zum Einsatz neuer Subunternehmer sind vorhanden

Daten werden nach Beendigung des Auftrags beim Auftragsverarbeiter datenschutzkonform gelöscht

# III. Technische und organisatorische Maßnahmen der eingesetzten Dienstleister

## 1. Microsoft Azure

| Domain | Practices |
|---|---|
| Organization of Information Security | **Security Ownership**. Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.<br><br>**Security Roles and Responsibilities**. Microsoft personnel with access to Customer Data or Professional Services Data are subject to confidentiality obligations.<br><br>**Risk Management Program**. Microsoft performed a risk assessment before processing the Customer Data or launching the Online Services service and before processing Professional Service Data or launching the Professional Services.<br><br>Microsoft retains its security documents pursuant to its retention requirements after they are no longer in effect. |
| Asset Management | **Asset Inventory**. Microsoft maintains an inventory of all media on which Customer Data or Professional Services Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access.<br><br>**Asset Handling**<br><br>- Microsoft classifies Customer Data and Professional Services Data to help identify it and to allow for access to it to be appropriately restricted.<br><br>- Microsoft imposes restrictions on printing Customer Data and Professional Services Data and has procedures for disposing of printed materials that contain such data.<br><br>- Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data or Professional Services Data on portable devices, remotely accessing such data, or processing such data outside Microsoft's facilities. |
| Human Resources Security | **Security Training**. Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures. Microsoft will only use anonymous data in training. |
| Physical and Environmental Security | **Physical Access to Facilities**. Microsoft limits access to facilities where information systems that process Customer Data or Professional Services Data are located to identified authorized individuals.<br><br>**Physical Access to Components**. Microsoft maintains records of the incoming and outgoing media containing Customer Data or Professional Services Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of such data they contain.<br><br>**Protection from Disruptions**. Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.<br><br>**Component Disposal**. Microsoft uses industry standard processes to delete Customer Data and Professional Services Data when it is no longer needed. |
| Communications and Operations Management | **Operational Policy**. Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data or Professional Services Data.<br><br>**Data Recovery Procedures**<br><br>- On an ongoing basis, but in no case less frequently than once a week (unless no updates have occurred during that period), Microsoft maintains multiple copies of Customer Data and Professional Services Data from which such data can be recovered.<br><br>- Microsoft stores copies of Customer Data and Professional Services Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data and Professional Services Data are located.<br><br>- Microsoft has specific procedures in place governing access to copies of Customer Data and Professional Services Data.<br><br>- Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Professional Services and for Azure Government Services, which are reviewed every twelve months.<br><br>- Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.<br><br>**Malicious Software**. Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data and Professional Services Data, including malicious software originating from public networks.<br><br>**Data Beyond Boundaries**<br><br>- Microsoft encrypts, or enables Customer to encrypt, Customer Data and Professional Services Data that is transmitted over public networks.<br><br>- Microsoft restricts access to Customer Data and Professional Services Data in media leaving its facilities. |

| Domain | Practices |
|---|---|
| | **Event Logging**. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data or Professional Services Data, registering the access ID, time, authorization granted or denied, and relevant activity. |
| Access Control | **Access Policy**. Microsoft maintains a record of security privileges of individuals having access to Customer Data or Professional Services Data.<br>**Access Authorization**<br>- Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data or Professional Services Data.<br>- Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months.<br>- Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources.<br>- Microsoft ensures that where more than one individual has access to systems containing Customer Data or Professional Services Data, the individuals have separate identifiers/log-ins.<br>**Least Privilege**<br>- Technical support personnel are only permitted to have access to Customer Data and Professional Services Data when needed.<br>- Microsoft restricts access to Customer Data and Professional Services Data to only those individuals who require such access to perform their job function.<br>**Integrity and Confidentiality**<br>- Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended.<br>- Microsoft stores passwords in a way that makes them unintelligible while they are in force.<br>**Authentication**<br>- Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems.<br>- Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly.<br>- Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long.<br>- Microsoft ensures that de-activated or expired identifiers are not granted to other individuals.<br>- Microsoft monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password.<br>- Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.<br>- Microsoft uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.<br>**Network Design**. Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data or Professional Services Data they are not authorized to access. |
| Information Security Incident Management | **Incident Response Process**<br>- Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.<br>- For each security breach that is a Security Incident, notification by Microsoft (as described in the “Security Incident Notification” section above) will be made without undue delay and, in any event, within 72 hours.<br>- Microsoft tracks, or enables Customer to track, disclosures of Customer Data and Professional Services Data, including what data has been disclosed, to whom, and at what time.<br>**Service Monitoring**. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary. |
| Business Continuity Management | - Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Customer Data or Professional Services Data are located.<br>- Microsoft’s redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data and Professional Services Data in its original or last-replicated state from before the time it was lost or destroyed. |

# 2. MongoDB Atlas

# 1. Definitions

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

1.1. "Cloud Provider" means Amazon Web Services (AWS), Microsoft Azure (Azure), or Google Cloud Platform (GCP), as selected by Customer.

1.2. "Customer Data" means any data you or your end users upload into MongoDB Atlas.

1.3. "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.

1.4. "Information Security Program" means MongoDB’s written security program, policies, and procedures that set forth the administrative, technical, and physical safeguards designed to protect Customer Data.

1.5. "MongoDB Atlas Cluster" means each replica set or sharded cluster of data-bearing nodes running the MongoDB database software that is managed by MongoDB Atlas, subject to your selected configurations.

1.6. "MongoDB Atlas Project" means one or more associated MongoDB Atlas Clusters with a shared set of authorization and network configurations.

1.7. "MongoDB Systems" means MongoDB’s internal infrastructure, including development, testing, and production environments, for MongoDB Atlas.

1.8. "Privileged User" means a select MongoDB employee or third-party contractor who has been granted unique authority to access Customer Data or MongoDB Systems as required to perform their job function.

1.9. "Security Incident Response Plan" means MongoDB’s documented protocols for evaluating suspected security threats and responding to confirmed Data Breaches and other security incidents.

# 2. Information Security Program Overview.

2.1. General. MongoDB maintains a comprehensive written Information Security Program to establish effective administrative, technical, and physical safeguards for Customer Data, and to identify, detect, protect against, respond

to, and recover from security incidents. MongoDB's Information Security Program complies with applicable Data Protection Law and is aligned with the NIST Cyber Security Framework (NIST). Additionally, MongoDB Atlas is certified against ISO 27001:2013, ISO 27017:2015, ISO 27018:2019, SOC 2 Type II, Payment Card Industry Data Security Standard v.4, and Cloud Security Alliance (CSA) Security, Trust, Assurance, and Risk (STAR) Level 2. MongoDB Atlas has also undergone a HIPAA examination validated by a qualified third-party assessor and can be configured to build HIPAA compliant applications.

2.2. Maintenance and Compliance. MongoDB's Information Security Program is maintained by a dedicated security team, led by our Chief Information Security Officer. MongoDB monitors compliance with its Information Security Program, and conducts ongoing education and training of personnel to ensure compliance. The Information Security Program is reviewed and updated at least annually to reflect changes to our organization, business practices, technology, services, and applicable laws and regulations. We will not alter or modify the Information Security Program in a way that materially weakens or compromises the effectiveness of its security controls.

2.3. MongoDB Personnel Controls.

2.3.1. Background Checks. MongoDB performs industry standard background checks on all MongoDB employees as well as any third-party contractor with access to Customer Data or MongoDB Systems.

2.3.2. Personnel Obligations. Any Privileged User authorized to access Customer Data is required to commit in writing to information security and confidentiality obligations that survive termination and change of employment. MongoDB maintains a formal disciplinary procedure for violations by MongoDB personnel of its security policies and procedures.

2.3.3. Training. Upon hire and subsequently at least once per year, Privileged Users authorized to access Customer Data undergo required training on specific security topics, including phishing, secure coding, insider threats, and the secure handling of Customer Data and personally identifiable information. Further, MongoDB implements mandatory, role-specific training for Privileged Users who are authorized to access Customer Data. MongoDB maintains records of training occurrence and content. In addition to these mandatory

trainings, MongoDB offers employees additional training resources, such as internal security awareness and education groups and hackathons.

2.4. Third Parties. MongoDB maintains and adheres to a documented process for the evaluation and approval of third-party service providers prior to onboarding, which includes appropriate due diligence regarding each third party's security processes and controls. We require third parties to contractually commit to confidentiality, security responsibilities, security controls, and data reporting obligations, and we perform ongoing targeted due diligence on a quarterly basis.

2.5. Security Contact. If you have security concerns or questions, you may contact us via your normal Support channels, via support.mongodb.com, or by emailing security@mongodb.com.

3. MongoDB Atlas Security Controls.

3.1. Data Centers and Physical Storage. MongoDB Atlas runs on AWS, Azure, and GCP, and you control which Cloud Provider to use for deploying your MongoDB Atlas Clusters. Each Cloud Provider is responsible for the security of its data centers, which are compliant with a number of physical security and information security standards detailed at the Cloud Provider's respective websites:

- https://aws.amazon.com/security/
- https://www.microsoft.com/en-us/trustcenter/security/azure-security
- https://cloud.google.com/security/

At least twice per year, each of our Cloud Providers is subject to due diligence performed by MongoDB or third-party auditors, which includes obtaining and reviewing security compliance certifications.

In addition to selecting which Cloud Provider to use, you also control the region where your MongoDB Atlas Clusters are deployed. This gives you the flexibility to decide where your Customer Data is physically stored, and you may choose to deploy your Customer Data in a specific geographic region (for example, only within the European Union or only within the United States).

3.2. Encryption.

3.2.1. Encryption in Transit. All MongoDB Atlas network traffic is protected by Transport Layer Security (TLS), which is enabled by default and cannot be disabled. Customer Data that you transmit to MongoDB Atlas, as well as Customer Data transmitted between nodes of your MongoDB Atlas Cluster, is encrypted in transit using TLS. You can select which TLS version to use for your MongoDB Atlas Clusters, with TLS 1.2 being the recommended default and a minimum key length of 128 bits.

> 3.2.1.1. Key Management Procedures for Encryption in Transit. All encryption in transit is supported by the use of OpenSSL FIPS Object Module. We maintain documented cryptography and key management guidelines for the secure transmission of Customer Data, and we configure our TLS encryption key protocols and parameters accordingly. MongoDB's key management procedures include: (i) generation of keys with approved key length; (ii) secure distribution, activation and storage, recovery and replacement, and update of keys; (iii) recovery of keys that are lost, corrupted, or expired; (iv) backup/archive of keys; (v) maintenance of key history; (vi) allocation of defined key activation and deactivation dates; (vii) restriction of key access to authorized individuals; and (viii) compliance with legal and regulatory requirements. When a key is compromised, it is revoked, retired, and replaced to prevent further use (except for limited use of that compromised key to remove or verify protections). Keys are protected in storage by encryption and are stored separately from encrypted data. TLS certificates are obtained from a major, widely trusted third-party public certificate authority. In the course of standard TLS key negotiation for active sessions, ephemeral session keys are generated which are never persisted to disk, as per the design of the TLS protocol.

3.2.2. Encryption at Rest. Upon creation of a MongoDB Atlas Cluster, by default, Customer Data is encrypted at rest using AES-256 to secure all volume (disk) data. That process is automated by the transparent disk encryption of your selected Cloud Provider, and the Cloud Provider fully manages the encryption keys. You may also choose to enable database-level encryption via the WiredTiger Encrypted Storage Engine

(using AES-256), as well as to bring your own encryption key with AWS Key Management Service (KMS), GCP KMS, or Azure Key Vault (KV).

3.2.3. Encryption in Use. MongoDB Atlas also supports automatic encryption of individual data fields of Customer Data before they are sent to MongoDB Atlas. If you enable this client-side field level encryption feature for a selected data field, an application-side component built into the MongoDB drivers encrypts that field of Customer Data before leaving the driver to be sent to MongoDB Atlas, and only decrypts it upon return to the application once inside the driver. With respect to the Customer Data for which you enable client-side field level encryption, MongoDB Atlas never sees your unencrypted Customer Data and you control the encryption keys, which you can secure using any KMIP-compliant key management service.

3.3. Network Connectivity Options.

3.3.1. Network Isolation. You may choose to deploy your MongoDB Atlas Clusters in a dedicated virtual environment or a shared multi-tenant system. Dedicated MongoDB Atlas Clusters are deployed in a VPC (for AWS and GCP) or VNet (for Azure) that fully isolates your Customer Data and is configured to prevent inbound network access from the internet. Each such MongoDB Atlas VPC or VNet utilizes security groups that act as a virtual firewall for your dedicated MongoDB Atlas Clusters.

3.3.2. Atlas IP Access List. In order to allow inbound network access to your MongoDB Atlas VPC or VNet, you must configure an Atlas IP Access List to enable specific networks to connect to the MongoDB Atlas Clusters within your MongoDB Atlas Project. Unless the Atlas IP Access List for a MongoDB Atlas Project includes a specific network’s IP addresses, network traffic is prevented from accessing your MongoDB Atlas Clusters in that MongoDB Atlas Project.

3.3.3. Virtual Private Cloud Peering. You may enable peering between your MongoDB Atlas VPC or VNet to your own dedicated application tier virtual private network with the Cloud Provider of your choice (VPC or VNet). Peering permits you to route encrypted traffic between your MongoDB Atlas VPC or VNet and your own application tier VPC or VNet privately, rather than traversing the public internet. Subject to the capabilities of your selected Cloud Provider, you may also choose to

peer your MongoDB Atlas VPC or VNet to your application tier VPC or VNet across regions.

3.3.4. Private Endpoints. MongoDB Atlas also supports private endpoints on AWS using the AWS PrivateLink feature and on Azure using the Azure Private Link feature. If you enable this feature for any MongoDB Atlas Cluster, that MongoDB Atlas Cluster will only allow a one-way connection from your AWS VPC or Azure VNet to the MongoDB Atlas Cluster and that MongoDB Atlas Cluster cannot initiate connections back to your AWS VPC or Azure VNet. Private endpoints also enable you to reach your MongoDB Atlas Cluster transitively over the network from other application tier AWS VPCs and Azure VNets that you have peered with the private endpoint, or through your own self-managed virtual private network including via AWS DirectConnect and Azure ExpressRoute.

3.4. Configuration Management. The MongoDB Atlas environment, including our production environment and your MongoDB Atlas Clusters, leverages configuration management systems to fully automate configuration based on one-time decisions that are securely applied to new and existing environments to ensure consistency every time. Our production environment and your MongoDB Atlas Clusters use in-house built machine images with secure configuration management applied via industry standard automation software, which includes hardening steps.

4. Access Controls.

4.1. Customer Access. MongoDB Atlas supports multiple authentication and authorization options and methods to give you the flexibility to meet your individualized requirements and needs. You are responsible for understanding the security configuration options available to you and the impact of your selected configurations on your MongoDB Atlas environment, which consists of a web application administrative interface (“MongoDB Atlas UI”) and any MongoDB Atlas Cluster you deploy. MongoDB Atlas provides you with configurable authentication and authorization options for both the MongoDB Atlas UI and your MongoDB Atlas Clusters.

4.1.1. MongoDB Atlas UI Authentication and Authorization. User credentials for the MongoDB Atlas UI are stored using industry standard and audited one-way hashes. The MongoDB Atlas UI supports multi-factor authentication (MFA), including a security

key/biometrics option that enables you to use hardware security keys or built-in authenticators. The MongoDB Atlas UI also supports federated authentication functionality for Single Sign-On (SSO) utilizing Security Assertion Markup Language (SAML).

4.1.2. MongoDB Atlas Cluster Authentication and Authorization. Authentication control for a MongoDB Atlas Cluster is enabled by default with the Salted Challenge Response Authentication Mechanism (SCRAM). You may choose to manage user authentication with self-managed X.509 certificates or through AWS IAM Users or Roles. MongoDB Atlas allows you to define permissions for individual users or applications in order to restrict the Customer Data that is accessible in a query. Further, you may choose to assign each user a MongoDB Atlas Project-specific role, which authorizes that user to perform specific actions on the MongoDB Atlas Clusters within that MongoDB Atlas Project. The MongoDB Atlas UI allows you to tailor your access controls by combining multiple roles and privileges for particular users. You can review, limit, and revoke user access to your MongoDB Atlas Clusters at any time. MongoDB Atlas also provides you with the ability to manage user authentication and authorization using your own Lightweight Directory Access Protocol (LDAP) server over TLS. A single LDAP over TLS (LDAPS) configuration applies to all MongoDB Atlas Clusters in a MongoDB Atlas Project.

4.1.3. Credential Requirements. As part of the configuration options, you may establish minimum password requirements (e.g., length, complexity) through your identity provider after federating authentication to the MongoDB Atlas UI via SAML and to the MongoDB Atlas Clusters via LDAPS.

4.1.4. Customer Database Auditing. MongoDB Atlas offers granular auditing that monitors actions in your MongoDB Atlas environment and is designed to prevent and detect any unauthorized access to Customer Data, including create, read, update, and delete (CRUD) operations, encryption key management, and role-based access controls. You are responsible for enabling database auditing and selecting the users, roles, groups, and event actions that you want to audit.

4.2. MongoDB Personnel Access to MongoDB Atlas Clusters.

4.2.1. Privileged User Access. As a general matter, MongoDB personnel do not have authorization to access your MongoDB Atlas Clusters. Only a small group of Privileged Users are authorized to access your MongoDB Atlas Clusters in rare cases where required to investigate and restore critical services. MongoDB adheres to the principle of “least privilege” with respect to those Privileged Users, and any access is limited to the minimum time and extent necessary to repair the critical issue. Privileged Users may only access your MongoDB Atlas Clusters via a gated process that uses a bastion host, requires MFA both to log in to our MongoDB Systems and to establish a Secure Shell connection (SSH) via the bastion host, and requires approval by MongoDB senior management.

4.2.2. Restricting MongoDB Personnel Access. MongoDB Atlas provides you with the option to entirely restrict access by all MongoDB personnel, including Privileged Users, to your MongoDB Atlas Clusters. If you choose to restrict such access and MongoDB determines that access is necessary to resolve a particular support issue, MongoDB must first request your permission and you may then decide whether to temporarily restore Privileged User access for up to 24 hours. You can revoke the temporary 24-hour access grant at any time. Enabling this restriction may result in increased time for the response and resolution of support issues and, as a result, may negatively impact the availability of your MongoDB Atlas Clusters. If you enable client-side field level encryption, even Privileged Users will be unable to access Customer Data within your MongoDB Atlas Clusters in the clear unless you provide MongoDB with the encryption keys.

4.2.3. Credential Requirements. Privileged User accounts may only be used for privileged activities, and Privileged Users must use a separate account to perform non-privileged activities. Privileged User accounts may not use shared credentials. The password requirements described in Section 4.3.3 also apply to Privileged User accounts.

4.2.4. Access Review and Auditing. MongoDB reviews Privileged User access authorization on a quarterly basis. Additionally, we revoke a Privileged User’s access when it is no longer needed, including within 24 hours of that Privileged User changing roles or leaving the company. We also log any access by MongoDB personnel to your MongoDB Atlas Clusters. Audit logs are retained for at least six years, and include a

timestamp, actor, action, and output. MongoDB utilizes a combination of automated and human review to scan those audit logs.

4.3. MongoDB Personnel Access to MongoDB Systems.

4.3.1. General. MongoDB's policies and procedures regarding access to MongoDB Systems adhere to the principles of role-based access control (RBAC), least privilege, and separation of duties. In accordance with these principles, with respect to MongoDB Atlas, MongoDB developers are only granted access to our development environments, and access to our production environment is limited to Privileged Users with appropriate authorizations. We review access authorizations to MongoDB Systems on a quarterly basis and we review any changes to authorizations for Privileged Users immediately. As part of the employee off-boarding process, access to MongoDB Systems is revoked within 24 hours of an employee's departure.

4.3.2. Access to MongoDB Atlas Production Environment. Our backend production environment that runs MongoDB Atlas is only accessible by a dedicated group of Privileged Users whose privileges must be approved by senior management. Privileged Users may only access our backend production environment via a bastion host and doing so requires MFA both to log in and to establish a SSH via the bastion host.

4.3.3. Credential Requirements. All MongoDB personnel passwords must conform to industry-standard complexity rules. Additionally, MFA is mandatory for all MongoDB personnel and cannot be disabled.

4.4. Physical Controls at MongoDB Offices. As noted in Section 3.1, Customer Data is deployed at the data centers of your selected Cloud Provider, and not at facilities owned or operated by MongoDB. At MongoDB offices, we follow industry best practices to employ physical security controls that are appropriate to the level of risk posed by the information stored and the nature of operations at our offices. In our offices, we: (i) issue access cards for all personnel through formal provisioning and approval processes; (ii) limit access to restricted areas to personnel with a need to access those areas to carry out their job functions; (iii) require visitors to sign in, execute a non-disclosure agreement, and be escorted in all non-public spaces; (iv) employ surveillance systems to monitor activity at points of entry from public spaces; and (v) revoke personnel access within 12 hours of termination.

4.5. Secure Deletion of Customer Data. If you terminate a MongoDB Atlas Cluster, it will become unavailable to you immediately and any Cloud Backup associated with that MongoDB Atlas Cluster will be terminated. MongoDB may retain a copy of the Customer Data stored in the terminated MongoDB Atlas Cluster for up to 5 days. If you terminate Cloud Backups, all snapshots will become unavailable to you immediately and it may take up to 24 hours for the Customer Data contained in the snapshots to become unrecoverable. When you terminate a MongoDB Atlas Project, the master key used to encrypt Customer Data is securely wiped, rendering all Customer Data effectively unrecoverable. If you choose to use MongoDB Atlas Online Archive, you can delete the entire archive, or pre-define automatic deletion dates for different data sections within MongoDB Atlas Online Archive to help automate any applicable retention restrictions or policies.

5. MongoDB Systems Security.

5.1. Separation of Production and Non-Production Environments.MongoDB Atlas has strict separation between production and non-production environments. Our MongoDB Atlas production environment, your MongoDB Atlas Clusters, and your Customer Data are never utilized for non-production purposes. Our non-production environments are utilized for development, testing, and staging. MongoDB also maintains firewalls to achieve strict separation of our MongoDB Atlas production environment and MongoDB's internal network.

5.2. Software Development Lifecycle. MongoDB has a dedicated security team, reporting to the Chief Information Security Officer, that leads security initiatives in the software development lifecycle (SDLC). We develop new products and features in a multistage process using industry standard methodologies that include defined security acceptance criteria and align with NIST and OWASP guidance. The SDLC includes regular code reviews, documented policies and procedures for tracking and managing all changes to our code, continuous integration of source code commits, code versioning, static and dynamic code analysis, vulnerability management, threat modeling, and bug hunts, as well as automated and manual source code analysis.

5.3. Monitoring and Alerting. MongoDB monitors the health and performance of MongoDB Atlas without needing to access your MongoDB Atlas Clusters. MongoDB maintains a centralized log management system for the collection, storage, and analysis of log data for our MongoDB Atlas production environment and your MongoDB Atlas Clusters. We use this information for

health monitoring, troubleshooting, and security purposes, including intrusion detection. We maintain our log data for at least six years, and we utilize a combination of automated scanning, automated alerting, and human review to monitor the data.

5.4. Vulnerability Management.

5.4.1. MongoDB Atlas Vulnerability Scanning. MongoDB maintains a documented vulnerability enumeration and management program that identifies internet-accessible company assets, scans for known vulnerabilities, evaluates risk, and tracks issue remediation. We conduct quarterly scans of both the underlying systems upon which MongoDB Atlas is deployed, as well as all third-party code integrated into our products. MongoDB's vulnerability management policy requires individual engineering teams to identify known vulnerabilities in system components, and develop remediation timeframes commensurate to the severity of an identified issue. We also utilize automated tooling in conjunction with monitoring security bulletins for relevant software and libraries, and implement patches if security issues are discovered.

5.4.2. Vulnerability Remediation. MongoDB uses a central company-wide ticketing system to track all security issues until remediation. We implement patches to our operating system and applications on a need-to-update basis, as determined in accordance with the Common Vulnerability Scoring System (CVSS). We are also a Mitre CVE Numbering Authority (CNA). Development tasks for all patches, bug fixes, and new features are defined as issues for specific target releases and are deployed to production only after completing requisite checkpoints, including quality assurance testing, staged deployment, and management review.

5.5. Penetration Testing and Internal Risk Assessments. MongoDB Atlas undergoes regular reviews from both internal and external security teams.

5.5.1. External Testing. Our MongoDB Atlas production environment is subject to an external penetration test by a nationally recognized security firm at least once per calendar year. Upon request, we will provide you with a summary letter of engagement that includes the number of high, medium, and low issues identified, but due to the sensitivity of the information gathered during these tests, we cannot allow customers to perform testing of our production platform.

Application-level security testing uses a standard application assessment methodology (e.g., OWASP). Additionally, external engagements with security consultants may include social engineering and phishing testing.

5.5.2. Internal Testing. Internally, MongoDB Atlas undergoes periodic risk assessments, including technical vulnerability discovery and analysis of business risks and concerns. The MongoDB security team is also routinely involved in source code review, architecture review, code commit peer review, and threat modeling.

6. Contingency Planning.

6.1. High Availability and Failover. Every MongoDB Atlas Cluster is deployed as a self-healing replica set that provides automatic failover in the event of a failure. Replica set members are automatically provisioned by MongoDB Atlas across multiple availability zones within a region, providing resilience to localized site failures. All replica set members are full data-bearing nodes, ensuring majority writes in the event of single node failure and higher resilience during recovery. Concurrent writes across replica sets occur in real time. MongoDB Atlas also offers multi-region and multi-cloud deployment options.

6.2. Backups. MongoDB Atlas offers Cloud Backups, which use the native snapshot functionality of your selected Cloud Provider to locally back up your Customer Data. You may enable Cloud Backups when you create or modify a MongoDB Atlas Cluster, and you have control over how often a Cloud Backup is captured and the length of time for which Cloud Backups are retained. Cloud Backup snapshots are stored with your selected Cloud Provider in the primary region of your MongoDB Atlas Cluster. All Cloud Backups are encrypted at rest and you may choose to use self-managed keys with the WiredTiger Encrypted Storage Engine. You may also optionally enable Continuous Cloud Backups with point-in-time recovery stored on our encrypted S3 buckets.

6.3. Business Continuity and Disaster Recovery. MongoDB maintains a documented business continuity and disaster recovery (“BCDR”) plan that aligns with ISO/IEC 22301:2019. Our BCDR plan includes: (i) clearly defined roles and responsibilities; (ii) availability requirements for customer services, including recovery point objectives (RPOs) and recovery time objectives (RTOs); and (iii) backup and restoration procedures. We review, update, and

test our BCDR plan at least annually. In the event of an incident that triggers the BCDR plan, the RPO will depend on your impacted MongoDB Atlas Cluster and backup configurations. You can test how your application handles a replica set failover at any time using the MongoDB Atlas UI or API.

7. Incident Response and Communications.

7.1. Security Incident Response Plan. As part of the Information Security Program, MongoDB maintains an established Security Incident Response Plan that aligns with NIST and ISO/IEC 27001:2013. In the event that MongoDB becomes aware of a Data Breach or other security incident, MongoDB will follow the Security Incident Response Plan, which includes: (i) clearly defined roles and responsibilities, including designation of a security incident task force; (ii) reporting mechanisms; (iii) procedures for assessing, classifying, containing, eradicating, and recovering from security incidents; (iv) procedures and timeframes for required notifications to relevant authorities and customers; (v) procedures for forensic investigation and preservation of event and system log data; and (vi) a process for post-incident and resolution analysis designed to prevent future similar incidents. The Security Incident Response Plan is reviewed, updated, and tested annually, including a security tabletop exercise at least once per year.

7.2. Security Incident Tracking. MongoDB maintains a comprehensive security incident tracking system that aligns with ISO/IEC 27001:2013 and documents: (i) incident type and suspected cause; (ii) whether there has been unauthorized or unlawful access, disclosure, loss, alteration, or destruction of data; (iii) if so, the categories of data affected by the incident, including categories of personal information; (iv) the time when the incident occurred or is suspected to have occurred; and (v) the remediation actions taken.

7.3. Customer Communications. MongoDB will notify you without undue delay if we become aware of any Data Breach. Taking into account the information available to us, such notice will include a description of the nature and cause of the Data Breach and the expected resolution time. To the extent possible, we will subsequently update you with information regarding evaluation of the root cause, potential impact, remediation actions taken, and actions planned to prevent a future similar event.

8. Audit Reporting.

8.1. Third-Party Certifications and Audit Reports. Upon request, and subject to the confidentiality obligations set forth in the Agreement, we will make available to you (or your independent, third-party auditor) information regarding MongoDB’s compliance with the security obligations set forth in these Security Measures in the form of third-party certifications and audit reports.

8.2. Security Questionnaires. No more than once per year, we will complete a written security questionnaire provided by you regarding the controls outlined in these Security Measures.

# 3. DigitalOcean

| Technical and Organizational Security Measure | Evidence of Technical and Organizational Security Measure |
|---|---|
| Measures of pseudonymisation and encryption of personal data | DigitalOcean's databases that store Customer Personal Data are encrypted using the Advanced Encryption Standard (AES). Customer data is encrypted in transit between the Customer's software application and DigitalOcean using TLS v1.2. |
| Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services<br><br>Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident | DigitalOcean uses a variety of tools and mechanisms to achieve high availability and resiliency. DigitalOcean's infrastructure spans multiple fault-independent availability zones in geographic regions physically separated from one another. DigitalOcean's infrastructure is able to detect and route around issues experienced by hosts or even whole data centers in real time and employ orchestration tooling that has the ability to regenerate hosts, building them from the latest backup. DigitalOcean also leverages specialized tools that monitor server performance, data, and traffic load capacity within each availability zone and colocation data center. If suboptimal server performance or overloaded capacity is detected on a server within an availability zone or colocation data center, these tools increase the capacity or shift traffic to relieve any suboptimal server performance or capacity overload. DigitalOcean is also immediately notified in the event of any suboptimal server performance or overloaded capacity. |
| Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing | DigitalOcean has developed and implemented a security control environment designed to protect the confidentiality, integrity, and availability of customers' systems. The Customer Data Use Policy governs the requirements for use of customer data in accordance with several industry standards.<br><br>DigitalOcean conducts a variety of regular internal and external audits that are inclusive of security operations. For more information please visit: https://www.digitalocean.com/trust/certification-reports/ |
| Measures for user identification and authorization | Access control policies require that access to DigitalOcean assets be granted based on business justification, with the asset owner's authorization and limits based on "need to-know" and "least-privilege" principles. In addition, the policy also addresses requirements for access management lifecycle including access provisioning, authentication, access authorization, removal of access rights and periodic access reviews.Documentation of these requirements is recorded and provided to external auditors for security certification testing. |
| Measures for the protection of data during transmission<br><br>Measures for the protection of data during storage | DigitalOcean's databases that store Customer Personal Data are encrypted using the Advanced Encryption Standard (AES). Customer data stored by DigitalOcean is encrypted in transit between the Customer's software application and DigitalOcean using TLS v1.2. |
| Measures for ensuring physical security of locations at which personal data are processed | DigitalOcean data centers are located in nondescript buildings that are physically constructed, managed, and monitored 24 hours a day to protect data and services from unauthorized access as well as environmental threats. All data centers are surrounded by a fence with access restricted through badge controlled gates. |

| Technical and Organizational Security Measure | Evidence of Technical and Organizational Security Measure |
|---|---|
| | CCTV is used to monitor physical access to data centers and the information systems. Cameras are positioned to monitor perimeter doors, facility entrances and exits, interior aisles, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facilities. |
| Measures for ensuring events logging | Logging of service, user and security events (web server logs, FTP server logs, etc.) is enabled and retained centrally. DigitalOcean restricts access to audit logs to authorized personnel based on job responsibilities.<br><br>Audit logging procedures are reviewed as part of external audits for security standards. |
| Measures for internal IT and IT security governance and management<br><br>Measures for certification/assurance of processes and products | DigitalOcean has developed and implemented a security control environment designed to protect the confidentiality, integrity, and availability of customers' systems. DigitalOcean performs an annual internal review of all security management policies and procedures. External auditors perform an annual review of these policies and procedures.<br><br>DigitalOcean conducts a variety of regular internal and external audits that are inclusive of security operations. For more information please visit: https://www.digitalocean.com/trust/certification-reports/. |
| Measures for ensuring data minimization<br><br>Measures for ensuring data quality<br><br>Measures for ensuring limited data retention<br><br>Measures for ensuring accountability<br><br>Measures for allowing data portability and ensuring erasure | More information about how DigitalOcean processes personal data is set forth in the Privacy Policy available at: https://www.digitalocean.com/legal/privacy-policy/. |
| Technical and organizational measures to be taken by the [sub]-processor to provide assistance to the controller and, for transfers from a processor to a [sub]-processor, to the Customer. | When DigitalOcean engages a Subprocessor, DigitalOcean and the Subprocessor enter into an agreement with data protection obligations substantially similar to those contained in this Schedule. Each Subprocessor agreement must ensure that DigitalOcean is able to meet its obligations to Customer. In addition to implementing technical and organizational measures to protect personal data, sub-processors must (a) notify DigitalOcean in the event of a Security Incident so DigitalOcean may notify Customer; (b) delete personal data when instructed by DigitalOcean in accordance with Customer's instructions to DigitalOcean; © not engage additional sub-processors without DigitalOcean's authorization; (d) not change the location where personal data is processed; or (e) process personal data in a manner which conflicts with Customer's instructions to DigitalOcean. |