



MariaDB Customer Data Processing Addendum

This Data Processing Addendum, including its appendices ("**DPA**") forms a part of, and is subject to, any written agreement ("**Agreement**") between MariaDB Corporation Ab or MariaDB USA, Inc. (as applicable, "**MariaDB**") and the party identified as the "**Customer**" in the Agreement and referring to this DPA. This DPA is supplemental to the Agreement and sets out the roles and obligations that apply when MariaDB processes personal data on behalf of Customer in the course of providing the services, including SkySQL Services and/or Remote DBA Services protected by Applicable Data Protection Laws under the Agreement (the "**Services**").

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

Customer enters into this DPA, and the Model Clauses (as applicable) on behalf of itself and, to the extent required under Applicable Data Protection Law, in the name and on behalf of its Affiliates (if any) permitted to use the Services. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and such Affiliates.

The parties agree as follows:

1. **Definitions**

- 1.1 "**Applicable Data Protection Law**" means the European Data Protection Law and the CCPA.
- 1.2 "**CCPA**" means Title 1.81.5 California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100–1798.199), as amended, superseded or replaced.
- 1.3 "**European Data Protection Law**" means (i) General Data Protection Regulation 2016/679 ("**GDPR**"); (ii) Directive 2002/58/EC; (iii) any applicable national implementations of (i) and (ii); (iv) Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance; and (v) in respect of the United Kingdom, the Data Protection Act 2018; in each case, as may be amended, superseded or replaced.
- 1.4 "**Security Incident**" means any confirmed breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted stored or otherwise processed by MariaDB and/or its Sub-processors in connection with the provision of the Services. "Security Incident" shall not include unsuccessful attempts or activities that do not compromise the security of personal data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
- 1.5 "**Standard Contractual Clauses**" means the standard contractual clauses for processors as approved by the European Commission pursuant to its decision C(2010)593 of 5 February 2010.
- 1.6 "**Sub-processor**" means any processor engaged by MariaDB or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or MariaDB Affiliates but shall exclude any MariaDB employee, contractor or consultant
- 1.7 The terms "**personal data**", "**controller**", "**processor**" and "**processing**" shall have the meaning given to them in European Data Protection Law and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly. The terms "**consumer**", "**business**", "**business purpose**", "**sell**", "**service provider**" and "**personal information**" shall have the meaning given to it in the CCPA.

2. **Scope and Applicability of this DPA**

2.1 **Scope.** This DPA applies to the extent that MariaDB processes as a processor or service provider (as applicable) any protected by Applicable Data Protection Laws in providing the Services to Customer.

2.2 **Role of the Parties.** The parties acknowledge and agree that Customer is a business or the controller (as applicable) with respect to the processing of personal data, and MariaDB shall process personal data only as a processor or service provider (as applicable) on behalf of Customer, as further described in Annex A of this DPA. Any processing by either party of personal data under or in connection with the Agreement shall be performed in accordance with European Data Protection Laws, where applicable.

3. **Processing of Customer Data**

3.1 **Customer Instructions.** As a processor, MariaDB shall process personal data only for the purposes described in the Agreement (including this DPA) and only in accordance with Customer's documented lawful instructions. The parties agree that the Agreement (including this DPA), and Customer's use of the Services, set out the Customer's complete and final instructions to MariaDB in relation to the processing of personal data and processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and MariaDB. Without prejudice to Section 3.3 (Customer responsibilities), MariaDB shall notify Customer in writing, unless prohibited from doing so under applicable law, if it becomes aware or believes that any data processing instructions from Customer violates Applicable Data Protection Laws.

3.2 **Customer Responsibilities.** Customer is responsible for the lawfulness of personal data processing under or in connection with the Agreement. Customer represents and warrants that (i) it has provided, and will continue to provide all notice and obtained, and will continue to obtain, all consents, permissions and rights necessary under Applicable Data Protection Laws for MariaDB to lawfully process personal data for the purposes contemplated by the Agreement (including this DPA); (ii) it has complied with all Applicable Data Protection Laws as a controller and/or service provider of personal data for the collection and provision to MariaDB and its Sub-processors of such personal data; and (iii) it shall ensure its processing instructions comply with applicable laws (including Applicable Data Protection Laws) and that the processing of personal data by MariaDB in accordance with Customer's instructions will not cause MariaDB to be in breach of Applicable Data Protection Laws.

4. **Sub-processing**

4.1 **Authorized Sub-processors.** Customer acknowledges and agrees that MariaDB may engage Sub-processors to process personal data on Customer's behalf. The Sub-processors currently engaged by MariaDB and authorized by Customer are available at our Online Trust Center (located at <https://mariadb.com/trust>) where Customer may elect to be notified by MariaDB if it changes its Sub-processors at least 7 calendar days prior to any such changes.

5. **Security and Audits**

5.1 **Security Measures.** MariaDB shall implement and maintain appropriate technical and organizational security measures designed to protect personal data from Security Incidents and to preserve the security and confidentiality of personal data. Such measures will include, at a minimum, those measures described in Annex B of this DPA ("**Security Measures**"). MariaDB shall ensure that any person who is authorized by MariaDB to process personal data shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

- 5.2 **Updates to Security Measures.** Customer acknowledges that the Security Measures are subject to technical progress and development and that MariaDB may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.
- 5.3 **Customer Responsibilities.** Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, selecting appropriately narrow access controls and address whitelists, protecting the security of personal data when in transit to and from the Service, and taking any appropriate steps to securely encrypt or backup any personal data processed in connection with the Services. Customer shall implement and maintain appropriate technical and organizational security measures designed to protect personal data from Security Incidents and to preserve the security and confidentiality of personal data while in its dominion and control.
- 5.4 **Security Incident Response.** Upon becoming aware of a Security Incident, MariaDB shall notify Customer without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer.
- 5.5 **Security Audits.** On written request from Customer, MariaDB shall provide written responses (on a confidential basis) to all reasonable requests for information made by Customer related to its processing of personal data, including responses to information security and audit questionnaires that are necessary to confirm MariaDB's compliance with this DPA, provided that Customer shall not exercise this right more than once in any 12 month rolling period. Notwithstanding the foregoing, Customer may also exercise such audit right in the event Customer is expressly requested or required to provide this information to a data protection authority, or MariaDB has experienced a Security Incident, or on another reasonably similar basis.
6. **International Transfers**
- 6.1 **Processing Locations.** Customer acknowledges and agrees that MariaDB may transfer and process personal data to and in the United States and anywhere else in the world where MariaDB, its Affiliates or its Sub-processors maintain data processing operations. MariaDB shall at all times ensure such transfers are made in compliance with the requirements of Applicable Data Protection Laws and this DPA.
7. **Deletion or Return of Personal Data**
- 7.1 Upon termination or expiry of the Agreement, on Customer's written request, MariaDB shall delete or return all personal data (including copies) in its possession or control, in accordance with the terms of the Agreement, save that this requirement shall not apply to the extent MariaDB is required by applicable law to retain some or all of the personal data by applicable law or to personal data it has archived on back-up systems, which data MariaDB shall securely isolate and protect from any further processing and delete in accordance with its deletion practices, except to the extent required by applicable law.
8. **Rights of Data Subjects and Cooperation**
- 8.1 **Data Subject Requests.** To the extent that Customer is unable to independently access personal data through the Services, MariaDB shall provide all reasonable cooperation to assist Customer, taking into account the nature of the processing and in so far as is possible, to respond to any requests from individuals or applicable data protection authorities relating to the processing of personal data under the Agreement. In the event that any such request is made to MariaDB directly, MariaDB shall not respond to such

communication directly without Customer's prior authorization, unless legally compelled to do so. If MariaDB is required to r

8.2 respond to such a request, MariaDB shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

9. **Jurisdiction Specific Terms**

9.1 **Europe.** To the extent the personal data is subject to European Data Protection Laws, the following terms shall apply in addition to the terms in the remainder of this DPA:

- (a) Sub-processor Obligations. MariaDB shall: (i) enter into a written agreement with each Sub-processor imposing data protection terms that require the Sub-processor to protect personal data to the standard required by applicable European Data Protection Law and this DPA; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause MariaDB to breach any of its obligations under this DPA.
- (b) Objections to Sub-processors. Customer may object in writing to MariaDB's appointment of a new Sub-processor on reasonable grounds relating to data protection (e.g. if making personal data available to the Sub-processor would violate applicable European Data Protection Law or weaken the protections for such personal data) by notifying MariaDB promptly in writing within 7 calendar days of receiving notification from MariaDB in accordance with Section 4.1. Such notice shall explain the reasonable grounds for the objection and the parties shall discuss Customer's concerns in good faith with a view to achieving commercially reasonable resolution.
- (c) If Customer objects to a Sub-processor, MariaDB may give written notice of a price change to correspond with any change in the costs of processing of data as may result from Customer's rejection of the use of a Sub-processor, or terminate the Agreement with effect of no less than thirty (30) days from Customer's notice of rejection
- (d) Standard Contractual Clauses. To the extent that MariaDB processes (or causes to be processed) any personal data protected by European Data Protection Laws in a third country not recognised as providing an adequate level of protection for personal data (as described in applicable European Data Protection Laws), MariaDB agrees to abide by and process personal data in compliance with the Standard Contractual Clauses, which are incorporated in full by reference and form an integral part of this DPA.
- (e) For the purposes of the descriptions in the Standard Contractual Clauses: (i) MariaDB agrees that it is a "data importer" and Customer is the "data exporter" (notwithstanding that Customer may itself be an entity located outside the EEA); (ii) Annex A and Annex B of this DPA shall replace Appendix 1 and Appendix 2 of the Standard Contractual Clauses; and (ii) Annex C shall form Appendix 3 of the Standard Contractual Clauses. It is not the intention of either party, nor the effect of this DPA, to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses. Accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA, the Standard Contractual Clauses shall prevail to the extent of such conflict.
- (f) Data Protection Impact Assessment. To the extent MariaDB is required under applicable European Data Protection Law, MariaDB shall provide reasonably requested information regarding MariaDB processing of personal data under the Agreement to enable the Customer to

carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

9.2 **California.** To the extent the personal data is subject to the CCPA, the parties agree that Customer is a business and that it appoints MariaDB as its service provider to process as permitted under the Agreement (including this DPA) and the CCPA, or for purposes otherwise agreed in writing (the "**Permitted Purposes**"). Customer and MariaDB agree that: (a) personal information was not sold to MariaDB and MariaDB shall not "sell" personal information (as defined by the CCPA); (c) MariaDB shall not retain, use or disclose personal information outside of the direct business relationship between Customer and MariaDB; and (d) MariaDB may de-identify or aggregate personal information in the course of providing the Services. MariaDB certifies that it understands the restrictions set out in this sub-section 9.2 and will comply with them.

10. **Miscellaneous**

10.1 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

10.2 Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA (including the Standard Contractual Clauses) whether in contract, tort (including negligence) or under any other theory of liability, shall be subject to the limitations and exclusions of liability in the Agreement, and any reference in provisions to the liability of a party means the aggregate liability of that party and all of its Affiliates' under and in connection with the Agreement and this DPA together.


10.3 This DPA may be executed in counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.

10.4 If any provision or part-provision of this DPA is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of the DPA.

10.5 This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by European Data Protection Law.

IN WITNESS WHEREOF, the parties have caused this DPA to be executed by their authorized representative and this DPA shall effective on the date both parties sign this DPA:

Customer: _____
By: _____
Name: _____
Title: _____
Date: _____

MariaDB : 
By: _____
Name: Kenneth Paqvalen
Title: Chief Financial Officer
Date: 3/25/2020

Annex A Data Processing Description

This Annex A forms part of the Agreement and describes the processing that the processor will perform on behalf of the controller.

Duration

The duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms plus the period from the expiry of the Agreement until deletion of personal data by MariaDB in accordance with the terms of the Agreement.

Categories of data

Customer data uploaded by the Customer to the Services in accordance with the Agreement.

Special categories of data (if appropriate)

The parties do not intend for any special category data to be processed under the Agreement.

Data subjects

The personal data to be processed may include Customer's customers, employees, suppliers and end-users.

Processing operations

The personal data will be subject to the following basic processing activities (please specify):

- processing to provide the Service in accordance with the Agreement
- processing to perform any steps necessary for the performance of the Agreement
- processing initiated by Customer in its use of the Service
- processing to comply with other reasonable instructions provided by Customer (e.g. via email or support tickets) that are consistent with the terms of this Agreement

Annex B

MARIADB SECURITY MEASURES

MariaDB implements the following technical and organisational security measures to protect personal data it processes.

Physical Access Control

MariaDB has implemented, or has ensured that its subprocessors have implemented, specific measures to prevent unauthorized persons from gaining physical access to the premises, buildings or rooms where data processing systems are located which process personal data. These controls include:

- Restricted access to specified, authorized individuals, including to data centres/rooms where servers are located;
- Video surveillance and alarm devices for such access areas;

System Access Control

MariaDB has implemented controls to prevent data processing systems from being used without authorization. These controls include:

- Password protections for all systems processing personal data (including remote access);
- Access support by authentication which includes:
 - Individual user passwords;
 - dedicated user IDs against systems user management for every individual;
- Access granted to authorized personnel only;
- Access granted to minimum required to perform the individual's function/role;
- Password policy prohibiting the sharing of passwords and outlines processes after a disclosure of a password;
- Passwords always stored in encrypted form;
- Procedure to deactivate user accounts (including administrator permissions) when a user leaves MariaDB or a specific function/role;
- Access logs;
- Review of such access logs for any security incidents.

Data Access Control

MariaDB has implemented controls to ensure persons entitled to use a data processing system shall gain access only to the data to which they have a right of access, and personal data must not be read, copied, modified or removed without authorization in the course of processing. These include:

- Restriction of file and program access to a "need-to-know-basis";
- Prevention of use/installation of unauthorized hardware and/or software;
- Rules for the safe and permanent destruction of data that are no longer required;
- Access granted to authorized personnel only;
- Access granted is the minimum required to perform the individual's function/role.

Data Transmission Control

MariaDB has implemented controls to ensure personal data is not read, copied, modified or removed without authorization during storage and that it is possible to establish to whom personal data was transferred. MariaDB has implemented controls to provide for the encryption of data during any transmission.

Data Entry Control

MariaDB has controls in place to examine and establish whether and by whom personal data have been entered into data processing systems, modified or removed. These controls include:

- Access logs showing administrators' and users' activities;
- Restriction on modification of personal data to authorized personnel only.

Job Control

MariaDB has implemented controls to ensure personal data is processed in the performance of a service for the Customer. These include ensuring:

- Processing of personal data is only for contractual performance;
- Staff members and contractors comply with written instructions and contracts;
- Personal data is always logically separated so that, in each step of the processing, the client from whom personal data originated can be identified.

Availability Control

MariaDB implements the following controls to protect personal data against disclosure, accidental or unauthorized destruction or loss:

- Back-up copies stored in protected environments;
- Contingency plans and/or business recovery strategies;
- Restriction on use of data only for purposes MariaDB is contracted to perform;
- Firewalls to prevent unauthorized access to systems and services

Organizational Requirements

MariaDB implements technical and organizational measures to avoid the accidental mixing of personal data, including:

- A designated individual responsible for data protection;
- Written commitments from employees to maintain confidentiality;
- Staff training on data privacy and security;
- Security incident response procedures and staff training where applicable.

Annex C

This Appendix forms part of the Clauses. All defined terms used in this Appendix 3 shall have the meaning given to it in the Standard Contractual Clauses unless otherwise defined in this Appendix.

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix sets out the parties' interpretation of their respective obligations under specific Clauses identified below. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

For the purposes of this Appendix, "**DPA**" means the Data Processing Addendum in place between data importer and data exporter and to which these Clauses are incorporated and "**Agreement**" shall have the meaning given to it in the DPA.

Clause 4(h) and 8: Disclosure of these Clauses

1. Data exporter agrees that these Clauses constitute data importer's Confidential Information as that term is defined in the Agreement and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

Clause 5(a): Suspension of data transfers and termination:

1. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.
2. The parties acknowledge that if data importer cannot provide such compliance for whatever reason, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract.
3. If the data exporter intends to suspend the transfer of personal data and/or terminate these Clauses, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("**Cure Period**").
4. If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend or terminate the transfer of personal data immediately. The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit:

1. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in Section 5 (Security and Audits) of the DPA.

Clause 5(j): Disclosure of subprocessor agreements

1. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.

2. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.
3. 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 in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

1. Any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

1. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "*FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC*" the data exporter may provide a general consent to onward subprocessing by the data importer.
2. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out in Section 9.1 of the DPA.