

Data Processing Addendum

Version 1 — August 1, 2026

This Data Processing Addendum (the "DPA") supplements and forms part of the Supabase Terms of Service available at <https://supabase.com/terms>, or such other agreement entered into between the Customer and Supabase Pte. Ltd ("Supabase") relevant to Customer's use of the Services (the "Agreement"), and in case of any conflict, supersedes the Agreement in relation to the transfer and processing of Covered Data in connection with the performance of the Services. This DPA is effective as of the Effective Date of the Agreement.

1. Definitions.

Capitalized terms used but not defined within this DPA will have the meaning set forth in the Agreement. The terms "controller", "processor", "business" and "service provider", whether capitalized or in the lower-case, have the meanings given to them under the Applicable Data Protection Laws. The following capitalized terms used in this DPA will be defined as follows:

"Applicable Data Protection Laws" means all applicable laws, rules, regulations, and governmental requirements relating to the privacy, confidentiality, or security of Personal Data, as they may be amended or otherwise updated from time to time, including (without limitation): the GDPR, Swiss Data Protection Laws and the CCPA.

"Biometric Data" means Personal Data resulting from physiological or behavioral characteristics such as facial features, voice, or fingerprint recognition data, used to identify a natural person.

We use cookies to collect data and improve our services. [Learn more](#)

Accept

Opt out

Privacy settings

[Skip to content](#)

"CCPA" means the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq., as amended, including its implementing regulations and the California Privacy Rights Act of 2020.

"Covered Data" means: (a) Personal Data that is provided by or on behalf of Customer to Supabase in connection with Customer's use of the Services, as further described in Schedule 3 (Processing Details) of this DPA; (b) contact information and access credentials relating to, and support requests submitted by, Authorized Users; and (c) any other Personal Data that is otherwise collected, generated or Processed by Supabase in connection with the provision of the Services.

"Customer's Controller" means, where the Customer acts as a processor or service provider (as identified in Schedule 3 (Processing Details)), the controller or business on whose behalf the Customer Processes Covered Data.

"Data Subject" means a natural person whose Personal Data is Processed.

"Deidentified Data" means data created using Covered Data that cannot reasonably be linked to such Covered Data, directly or indirectly.

"GDPR" means Regulation (EU) 2016/679 (the **"EU GDPR"**) or, where applicable, the **"UK GDPR"**, as defined in section 3 of the Data Protection Act 2018.

"Personal Data" means any data or information that: (a) is linked or reasonably linkable to an identified or identifiable natural person; or (b) is otherwise "personal data," "personal information," "personally identifiable information," or similarly defined data or information under Applicable Data Protection Laws.

"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means. "Process", "Processes" and "Processed" will be interpreted accordingly.

"Security Incident" means a confirmed breach of security, including but not limited to destruction, loss, alteration, unauthorized disclosure, or unauthorized internal access to) Covered Data, or any other incident that is not trivial in nature, such as phishing or malware attacks.

the security of Covered Data.

We use cookies to collect data and improve our services. [Learn more](#)

"Sensitive Data" means any Personal Data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; Biometric Data used to uniquely identify a natural person; data concerning health or a person's sex life or sexual orientation; or data relating to criminal convictions and offenses.

"Standard Contractual Clauses" or "SCCs" means the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914.

"Sub-processor" means, with respect to any Processing performed by Supabase as a processor or service provider, an entity appointed by Supabase to Process Covered Data on its behalf.

"Swiss Data Protection Laws" means the Swiss Federal Act on Data Protection of 19 June 1992 and the Swiss Ordinance to the Swiss Federal Act on Data Protection of 14 June 1993, and any new or revised version of these laws that may enter into force from time to time.

"US Data Protection Laws" means all applicable federal and state laws, rules, regulations, and governmental requirements relating to data protection, the Processing of Personal Data, privacy and/or data protection in force from time to time in the United States, including (without limitation): the CCPA, the Virginia Consumer Data Protection Act, Code of Virginia Title 59.1 Chapter 52 § 59.1-571 et seq., the Colorado Privacy Act, Colorado Revised Statute Title 6 Article 1 Part 13 § 6-1-1301 et seq., the Utah Consumer Privacy Act, Utah Code § 13-6-101 et seq., and Connecticut Senate Bill 6, An Act Concerning Personal Data Privacy and Online Monitoring (as such law is chaptered and enrolled).

2. Role of the Parties.

The Parties acknowledge and agree that Supabase acts as a processor/service provider, and Customer as controller/business under the Agreement and this DPA. To the extent Customer Processes Covered Data on behalf of its own Controller, Supabase acts as a subprocessor.

3. Details of Data Processing.

3.1 Nature, Purpose and Duration.

[Skip to content](#)

We use cookies to collect data and improve our services. [Learn more](#)

The nature, purpose, and duration of the Processing of Personal Data under the Agreement and this DPA are described in the Agreement and in Schedule 3 (Processing Details) to this DPA.

3.2 Instructions.

Supabase shall comply with its obligations under Applicable Data Protection Laws. Supabase shall only Process Covered Data on behalf of and under the instructions of Customer and in accordance with Applicable Data Protection Laws. The Agreement and this DPA shall constitute Customer's instructions for the Processing of Covered Data. Customer may issue further written instructions in accordance with this DPA. Supabase will: (a) provide reasonable assistance to Customer to enable Customer to conduct and document any data protection assessments required under Applicable Data Protection Laws; and (b) promptly inform Customer if, in its opinion, an instruction from Customer infringes the Applicable Data Protection Laws.

3.3 Supabase Prohibitions.

Without limiting the foregoing, Supabase is prohibited from: (a) selling Covered Data or otherwise making Covered Data available to any third party for monetary or other valuable consideration; (b) sharing Covered Data with any third party for cross-context behavioral advertising; (c) retaining, using, or disclosing Covered Data for any purpose other than for the business purposes specified in the Agreement or as otherwise permitted by Applicable Data Protection Laws; (d) retaining, using, or disclosing Covered Data outside of the direct business relationship between the Parties; and (e) except as otherwise permitted by Applicable Data Protection Laws, combining Covered Data with Personal Data that Supabase receives from or on behalf of another person or persons, or collects from its own interaction with the Data Subject.

4. Compliance.

Customer shall comply with its obligations under Applicable Data Protection Laws to provide (or ensure that the Customer's Controller provides) the necessary instructions regarding the Processing of their Covered Data to Supabase. Customer shall ensure that its Services as required under Applicable Data Protection Laws.

We use cookies to collect data and improve our services. [Learn more](#)

lawful Processing of Covered Data under Applicable Data Protection Laws, obtain (or ensure that the Customer's Controller obtains) valid consents from Data Subjects for such Processing in the form required under Applicable Data Protection Laws; (c) implement appropriate technical and organizational measures to give effect to Data Subject rights under Applicable Data Protection Laws, and shall comply with requests from Data Subjects (or, where applicable, Customer's Controller) to exercise their rights under Applicable Data Protection Laws within the timeframe and subject to any exemptions prescribed in the Applicable Data Protection Laws; and (d) ensure it has provided notice and obtained all necessary explicit consents from Data Subjects for the collection and Processing of any Sensitive Data by the Processor on Controller's behalf. Customer certifies that it is in compliance with all laws applicable to the collection, use, and storage of Sensitive Data.

5. Supabase Personnel.

Supabase shall: (a) limit access to Covered Data to personnel who have a business need to have access to such Covered Data; and (b) ensure that such personnel are subject to obligations at least as protective of the Covered Data as the terms of this DPA and the Agreement, including duties of confidentiality with respect to any Covered Data to which they have access.

6. Sub-processors.

6.1 Location.

Supabase may Process Covered Data anywhere that Supabase or its Sub-processors maintain facilities, subject to the remainder of this clause 6, its obligations with respect to data transfers as required by Applicable Data Protection Laws and clause 12 of this DPA. Where Customer directs Supabase to Process Covered Data in a specific geographical region, Supabase shall ensure that such Covered Data is stored and primarily Processed in that region unless otherwise required to comply with Customer's obligations. Supabase shall ensure that it is necessary to provide Services requested by Customer. Supabase shall not Process Covered Data in a specific region to the detriment of other regions, and shall indemnify, defend and hold Supabase

We use cookies to collect data and improve our services. [Learn more](#)

6.2 Authorization.

Customer grants Supabase general authorization (or, where applicable, has Customer's Controller's general authorization) to engage any of the Sub-processors provided in Supabase's Sub-processor list, available at <https://supabase.com/legal/customer-resources/subprocessor-list> ("Subprocessor List"), as amended from time to time in accordance with clause 6.3 (the "Authorized Sub-processors"), to Process Covered Data. Supabase shall: (a) enter into a written agreement with each Authorized Sub-processor imposing data protection obligations that, in substance, are no less protective of Covered Data than Supabase's obligations under this DPA; and (b) remain liable for each Authorized Sub-processor's compliance with the obligations under this DPA.

6.3 Updates to the Subprocessor List.

Supabase offers a mechanism for Customer to subscribe to notifications of changes to the Subprocessor List via <https://supabase.com/legal/customer-resources/subprocessor-list>. If Customer subscribes to receive such updates, Supabase will provide Customer with at least thirty (30) days' notice of any proposed changes to the Authorized Sub-processors. Customer shall notify Supabase if it objects to the proposed change to the Authorized Sub-processors (including, where applicable, when exercising its right to object under clause 9(a) of the SCCs) by providing Supabase with written notice of the objection within five (5) days after Supabase has provided notice to Customer of such proposed change (an "Objection"). In the event Customer submits an Objection to Supabase, Supabase and Customer shall work together in good faith to find a mutually acceptable resolution to address such Objection. If Supabase and Customer are unable to reach a mutually acceptable resolution within a reasonable timeframe, which shall not exceed thirty (30) days, Customer may terminate the portion of the Agreement relating to the Services affected by such change by providing written notice to Supabase.

7. Data Subject Rights Requests.

Supabase will promptly notify Customer of an Authorized Sub-processor from a Data Subject which Supabase associates with Customer or which identifies its Covered Data. As between the Parties, Customer will have sole discretion in responding to

We use cookies to collect data and improve our services. [Learn more](#)

the Data Subject Request, and Supabase shall not respond to the Data Subject Request, except to advise the Data Subject that their request has been forwarded to Customer. Supabase will, taking into account the nature of the Services, provide Customer with reasonable assistance as necessary for Customer to fulfill its obligation under Applicable Data Protection Laws to respond to Data Subject Requests.

8. Security.

Supabase will implement and maintain appropriate technical and organizational data protection and security measures designed to ensure security of Covered Data, taking into account the nature, scope, context, and purpose of the Processing and its associated risks, including, without limitation, protection against unauthorized or unlawful Processing and against accidental loss, destruction, or damage of or to Covered Data. Such measures will meet the minimum standards set out in Schedule 1.

9. Information and Audits.

9.1 Information.

Supabase shall notify Customer promptly if Supabase determines that it can no longer meet its obligations under Applicable Data Protection Laws. Customer may take reasonable and appropriate steps to stop and remediate unauthorized use of Covered Data upon reasonable notice.

9.2 Audit Reports.

Upon request, Supabase shall provide to Customer: (a) data protection compliance certifications issued by a commonly accepted certification issuer which has been audited by a data security expert, or by a publicly certified auditing company; or (b) such other documentation reasonably evidencing the implementation of data security measures in accordance with applicable law and clause 9.2, the "Audit Reports"). If an audit request is received, Supabase shall provide the Audit Reports, and the certification or documentation to Customer within 30 days of the audit request; and Supabase confirms that there are no known material changes to

We use cookies to collect data and improve our services. [Learn more](#)

the controls audited, then Customer agrees to accept that certification or documentation in lieu of conducting a physical audit of the controls pursuant to clause 9.3.

9.3 Customer Audit Rights.

To the extent Customer is unable to retrieve the information it needs to comply with its diligence requirements under Applicable Data Protection Laws via the Audit Reports, Customer may audit Supabase's compliance with this DPA no more than once per calendar year to the extent required by Applicable Data Protection Laws. The Parties agree that all such audits will be conducted: (a) upon at least thirty (30) days' written notice to Supabase; (b) only during Supabase's normal business hours; and (c) in a manner that does not materially disrupt Supabase's business or operations and at Customer's sole expense. With respect to any such audits, Customer may engage a third-party auditor to conduct the audit on its behalf. Supabase shall not be required to facilitate any such audit unless and until the Parties have agreed in writing the scope and timing of such audit.

9.4 Results.

Customer shall promptly notify Supabase of any non-compliance discovered during an audit. The results of the audit shall be Supabase's Confidential Information.

10. Security Incidents.

Supabase shall notify Customer in writing without undue delay, and where feasible, within forty-eight (48) hours, after becoming aware of any Security Incident to the contact details for Customer associated with its Supabase account. Supabase shall take reasonable steps to contain, investigate, and mitigate any Security Incident, and shall send Customer timely information about the Security Incident, including, but not limited to, the nature of the Security Incident, the measures taken to mitigate or contain the Security Incident, and the status of the investigation. Supabase shall provide reasonable assistance with Customer's investigation of any Security Incidents and any of Customer's obligations under Applicable Data Protection Laws, including notifying relevant supervisory authorities. Supabase's notification

We use cookies to collect data and improve our services. [Learn more](#)

clause 10 shall not be construed as an acknowledgement by Supabase of any fault or liability with respect to the Security Incident.

11. Term, Deletion and Return.

11.1 Term.

This DPA shall commence on the Effective Date and, notwithstanding any termination of the Agreement, will remain in effect until, and automatically expire upon, Supabase's deletion of all Covered Data as described in this DPA.

11.2 Deletion and Return.

Supabase shall, if requested to do so by Customer within thirty (30) days of expiry of the Agreement (the "Retention Period"), provide a copy of all Covered Data in such commonly used format as requested by Customer, or provide a self-service functionality allowing Customer to download such Covered Data. On expiry of the Retention Period, Supabase shall delete all copies of Covered Data Processed by Supabase or any Authorized Sub-processors.

12. Standard Contractual Clauses.

12.1 Incorporation of the SCCs.

The Standard Contractual Clauses shall, as further set out in Schedule 2, apply to the transfer of any Covered Data from Customer to Supabase, and form part of this DPA, to the extent that:

(a) the GDPR or Swiss Data Protection Laws apply to the Customer when making that transfer; or

(b) the Applicable Data Protection Laws that apply to the Customer when making that transfer (the "Exporter Data Protection Laws") prohibit the transfer of Covered Data under this DPA in the absence of a transfer mechanism approved by the relevant data protection authority of the Processing of that Covered Data, and a

We use cookies to collect data and improve our services. [Learn more](#)

- (i) the relevant authority with jurisdiction over the Customer's transfer of Covered Data under this DPA has not formally adopted standard data protection clauses or another transfer mechanism under the Exporter Data Protection Laws; or
 - (ii) such authority has issued guidance that entering into standard contractual clauses approved by the European Commission would satisfy any requirement under the Exporter Data Protection Laws to implement adequate safeguards in respect of that transfer; or
 - (iii) established market practice in relation to transfers subject to the Exporter Data Protection Laws is to enter into standard contractual clauses approved by the European Commission to satisfy any requirement under the Exporter Data Protection Laws to implement adequate safeguards in respect of that transfer.
- (c) the transfer is an "onward transfer" (as defined in the applicable module of the SCCs).

12.2 Signature of the SCCs.

The Parties agree that acceptance of the Agreement shall have the same effect as signing the SCCs.

13. Deidentified Data.

If Supabase receives Deidentified Data from or on behalf of Customer, Supabase shall: (a) take reasonable measures to ensure the information cannot be associated with a Data Subject; (b) publicly commit to Process the Deidentified Data solely in deidentified form and not to attempt to reidentify the information; and (c) contractually obligate any recipients of the Deidentified Data to comply with the foregoing requirements and Applicable Data Protection Laws.

14. General.

The Parties hereby certify that they understand and agree to the terms and conditions of this Agreement with them. The Parties agree to negotiate in good faith the changes to the Agreement required in connection with changes in Applicable Laws. The Parties agree to the terms provided by Supabase to Customer under this DPA and to be bound by the terms and conditions of this DPA.

We use cookies to collect data and improve our services. [Learn more](#)

Customer associated with its Supabase account or as otherwise stated in the Agreement, unless the Parties agree otherwise in writing.

SCHEDULE 1 — TECHNICAL AND ORGANIZATIONAL MEASURES

Introduction

Supabase employs a combination of policies, procedures, guidelines and technical and physical controls to protect the personal data it processes from accidental loss and unauthorized access, disclosure or destruction.

Governance and policies

Supabase:

- assigns personnel with responsibility for the determination, review and implementation of security policies and measures;
- reviews its security measures and policies on a regular basis to ensure they continue to be appropriate for the data being protected; and
- establishes and follows secure configurations for systems and software, and ensures that security measures are considered during project initiation and the development of new IT systems.

Breach response

Supabase maintains internal monitoring systems that can alert its operational teams regarding any service outages, in some cases even in advance of the outage thresholds being breached.

Supabase has a breach response plan that has been developed to address data breach events. The plan is regularly tested and updated.

Access controls

We use cookies to collect data and improve our services. [Learn more](#)

Supabase limits access to personal data by implementing appropriate access controls, including the following:

- Access to infrastructure and internal resources is managed on the basis of the Principle of Least Privilege: individuals are granted only the privileges they require to execute their business duties, and said privilege is revoked when it is no longer needed.
- Access management is centralized to identity providers, and wherever feasible, internal services delegate both authentication and authorization to these providers. This ensures that off-boarding and privilege revocation can be handled in a timely fashion.
- Supabase infrastructure requires approvals from at least one additional authorized person before any changes can be made. Authorized persons are designated based on the relevance of the system in question to their business roles.
- User authentication for Supabase internal resources is protected with both a strong password policy and mandatory 2FA that disallows the use of SMS-based 2FA.
- Supabase never knowingly stores plaintext passwords; if necessary, Supabase stores hashed, salted results of authentication material, as appropriate for the use case.
- Supabase devices that are used for accessing internal resources enforce strong security measures, including strong passwords, use of anti-virus software, and full-disk encryption.
- Audit trails are retained of user actions performed within Supabase infrastructure. Supabase retains audit logs of all interactions with its internal services and all interactions with Customer projects.
- Traffic flow logs are retained that enable retroactive analysis of all connections to Supabase infrastructure if needed.
- Only pre-approved and secure means of communicating with Supabase services are exposed by Supabase's firewalls.
- All communication—including transmission of credentials—is conducted over connections protected by TLS configured with a set of modern cipher suites.

Segmentation

Customer projects and Supabase internal Core
networks with firewalls enforcing that only the

We use cookies to collect data and improve our services. [Learn more](#)

[Skip to content](#) logs are retained of metadata about the traffic flowing across the two.

Logs and metrics used for observability and debugging are automatically extracted and sent to systems that are segregated from Customer projects that contain Customer's data.

Encryption

Stored data is encrypted where appropriate, including any backup copies of the data.

- All hard disks are encrypted-at-rest using the industry-standard AES-256 algorithm. Similarly, the regularly scheduled backups are also encrypted-at-rest using AES-256.
- The encryption keys are protected by keys stored using FIPS 140-2 compliant HSMs.

All network communication is conducted over encrypted links protected by modern security standards (TLS 1.2, modern cipher suites) to preserve confidentiality and integrity of the data.

Availability and backup

Supabase takes daily backups of Customer projects by default. Additional backups can be scheduled based on Customer requirements and service agreements.

All backups are encrypted in-transit and at-rest.

Backups are stored on a storage system independent of the Customer's project resources, and aim for 99.99% availability.

Supabase has employees strategically placed around the world, which allows it to utilize a follow-the-sun model for supporting and monitoring its operations, and to expedite the response to any service incidents.

Testing

Supabase uses reasonable and appropriate security and compliance monitoring systems across its infrastructure, in order to detect any violations of its security policies.

Supabase regularly conducts penetration tests with external security firms, and remediates any findings as soon as possible.

We use cookies to collect data and improve our services. [Learn more](#)

SCHEDULE 2 – STANDARD CONTRACTUAL CLAUSES

1. EU SCCs

With respect to any transfers referred to in clause 12, the Standard Contractual Clauses shall be completed as follows:

1.1 The following modules of the SCCs will apply:

(a) where the Customer acts as a controller and Supabase acts as a processor, Module Two (controller to processor) shall apply; and

(b) to the extent that Customer acts as a processor and Supabase acts as a subprocessor, Module Three (processor to processor) shall apply.

1.2 Clause 7 of the Standard Contractual Clauses (Docking Clause) does not apply.

1.3 Option 2 of Clause 9(a) (General written authorization) shall apply, and the time period to be specified is determined in clause 6.3 of the DPA.

1.4 The option in Clause 11(a) of the Standard Contractual Clauses (Independent dispute resolution body) does not apply.

1.5 With regard to Clause 17 of the Standard Contractual Clauses (Governing law), the Parties agree that option 1 will apply and the governing law will be Irish law.

1.6 In Clause 18 of the Standard Contractual Clauses (Choice of forum and jurisdiction), the Parties submit themselves to the jurisdiction of the courts of Ireland.

1.7 For the purpose of Annex I of the Standard Contractual Clauses:

(a) Schedule 3 (Processing Details) of this DPA sets out the details of the Customer and the competent supervisory authority;

(b) the description of the transfer is set out in the DPA, including the processing of contact information and access to the Services submitted by, Authorized Users for the purpose of the Services and providing support in relation to the Services; and

We use cookies to collect data and improve our services. [Learn more](#)

(c) the data importer is Supabase Pte. Ltd whose offices are located at 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513 and whose contact details are privacy@supabase.io.

1.8 For the purpose of Annex II of the Standard Contractual Clauses, Schedule 1 of the DPA contains the technical and organizational measures.

2. UK Addendum

2.1 This paragraph 2 (UK Addendum) shall apply to any transfer of Covered Data from Customer (as data exporter) to Supabase (as data importer), to the extent that:

(a) the UK Data Protection Laws apply to Customer when making that transfer; or

(b) the transfer is an "onward transfer" as defined in the Approved Addendum.

2.2 As used in this paragraph 2:

"Approved Addendum" means the template addendum, version B.1.0 issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018 and laid before the UK Parliament on 2 February 2022, as it may be revised according to Section 18 of the Approved Addendum.

"UK Data Protection Laws" means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

2.3 The Approved Addendum will form part of this DPA with respect to any transfers referred to in paragraph 2.1, and execution of this DPA shall have the same effect as signing the Approved Addendum.

2.4 The Approved Addendum shall be deemed completed as follows:

(a) the **"Addendum EU SCCs"** shall refer to the SCCs as they are incorporated into this DPA in accordance with clause 12 and this Schedule

(b) Table 1 of the Approved Addendum shall be
Schedule 2;

We use cookies to collect data and improve our services. [Learn more](#)

(c) the "Appendix Information" shall refer to the information referred to in paragraph 1.7 of this Schedule 2 and set out in Schedule 1;

(d) for the purposes of Table 4 of the Approved Addendum, neither party may terminate the Approved Addendum in accordance with Section 19 of the Approved Addendum; and

(e) Section 16 of the Approved Addendum does not apply.

3. Swiss Addendum

3.1 This paragraph 3 (Swiss Addendum) shall apply to any transfer of Covered Data from Customer (as data exporter) to Supabase (as data importer), to the extent that the Swiss Data Protection Laws apply to Customer when making that transfer.

3.2 The Standard Contractual Clauses will apply to such transfers, subject to the modifications described in paragraph 3.3.

3.3 The following modifications shall be made to the SCCs:

(a) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss Data Protection Laws, and references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent Article or Section of the Swiss Data Protection Laws;

(b) references to "EU", "Union" and "Member State" shall be interpreted as references to Switzerland;

(c) the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the SCCs;

(d) references to personal data in the SCCs also refer to data about identifiable legal entities until the entry into force of revisions to the Swiss Data Protection Laws that eliminate this broader scope;

(e) under Annex I.C of the SCCs (Competent supervisory authority) the Swiss Federal Data Protection and Information Commission, the transfer is governed by the Swiss Data Protection Laws.

We use cookies to collect data and improve our services. [Learn more](#)

supervisory authority designated in accordance with paragraph 1.7 of this Schedule 2 insofar as the data transfer is governed by the EU GDPR.

4. Transfers of personal data from Other Jurisdictions

4.1 If the SCCs apply pursuant to clause 12.1(b) of the DPA, then:

- (a) Module One (controller to controller) of the SCCs will apply where Customer is acting as a controller of Covered Data and Supabase is acting as a controller of Covered Data;
- (b) Module Two (controller to processor) of the SCCs will apply where Customer is acting as a controller of Covered Data and Supabase is acting as a processor of Covered Data;
- (c) Module Three (processor to processor) of the SCCs will apply where Customer is acting as a processor of Covered Data and Supabase is acting as a sub-processor of Covered Data; and
- (d) Module Four (processor to controller) of the SCCs will apply where Customer is acting as a processor of Covered Data and Supabase is acting as a controller of Covered Data.

4.2 If, under the Exporter Data Protection Laws, the SCCs require modifications when used for the purpose of transferring data from a non-EU jurisdiction (the data exporter's jurisdiction) to another country, the Parties shall be deemed to have incorporated the SCCs into this Schedule 2 with such modifications, and shall comply with such modified SCCs in connection with such transfers.

4.3 If clause 12.1(b) of the DPA applies, the SCCs shall apply with the following modifications:

- (a) references to "Regulation (EU) 2016/679" and any specific articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent references to the Exporter Data Protection Laws;
- (b) references to the "Union", "EU" and "EU Member State" are all replaced with reference to the jurisdiction in which the Exporter Data Protection Laws were issued (the "Exporter Jurisdiction");
- (c) the "competent supervisory authority" shall be the supervisory authority in the Exporter Jurisdiction; and

We use cookies to collect data and improve our services. [Learn more](#)

(d) Clauses 17 and 18 of the SCCs shall refer to the laws and courts of the Exporter Jurisdiction respectively.

4.4 Where, at any time during the Supabase's Processing of Covered Data under this DPA, a transfer mechanism other than the SCCs is approved under the Exporter Data Protection Laws with respect to transfers of Covered Data by Customer to Supabase, the Parties shall promptly enter into a supplementary agreement that:

(a) incorporates any standard data protection clauses or another transfer mechanism formally adopted by the relevant authority in the Exporter Jurisdiction;

(b) incorporates the details of Processing set out in Schedule 3 (Processing Details) of this DPA;

(c) shall, with respect to the transfer of Personal Data subject to the Exporter Data Protection Laws, take precedence over this DPA in the event of any conflict.

4.5 Where required under the Exporter Data Protection Laws, the relevant data exporter shall file a copy of the agreement entered into in accordance with paragraph 4.4 with the relevant national authority.

SCHEDULE 3 — PROCESSING DETAILS

Customer Name: Customer.

Customer Address: The address for Customer associated with its Supabase account or as otherwise stated in the Agreement.

Contact: The contact details for Customer associated with its Supabase account or as otherwise stated in the Agreement.

Customer Role: Controller/business (or processor/service provider for Customer's controller, as applicable).

Categories of Personal Data stored or processed: The categories of Personal Data depend on the nature of the processing.

We use cookies to collect data and improve our services. [Learn more](#)

include for example: Contact information, first name, last name, email address, Usage information, Registration/account information, name, email address, password, and any other information as determined by the Customer in accordance with the Agreement.

Categories of Data Subjects to whom the personal data mentioned above relates: The specific categories of data subjects depend on the nature of Customer's use of the Services but may include for example: Authorized Users and Customer's end users, as submitted by Customer.

Special categories of Personal Data: The specific categories of Sensitive Data depend on the nature of Customer's use of the Services, but may include for example: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Notwithstanding the foregoing, Customer is not permitted to submit and shall not submit personal data to the Services which would be defined as Personal Health Information under the Health Insurance Portability and Accountability Act of 1996 without first agreeing to sign a separate business associate agreement with Supabase.

Frequency of the transfer: continuous.

Nature of the processing: Storage, deletion, rectification, analysis, transfer, aggregation.

Purpose of the processing: The performance of the Services, namely the provision of database and tooling services for the development and operation of web and mobile applications.

Retention period: The duration of the Agreement, unless earlier deletion is requested by the Customer in accordance with the functionality of the Services.

Subprocessors: As found in the Subprocessor List.

Supervisory Authority: The competent supervisory authority determined in accordance with Applicable Data Protection Laws.

We use cookies to collect data and improve our services. [Learn more](#)

We protect your data.
[Skip to content](#)

✓ HIPAA Compliant



Get product updates and news from Supabase.

Subscribe

Product

Pricing

Database

Auth

Functions

Compute

Realtime

Storage

Vector

Cron

Feature Catalog

Launch Week

Solutions

AI Builders

No Code

Beginners

Developers

Postgres Devs

Vibe Coders

Hackathon Contestants

Startups

Agencies

Enterprise

Innovation Teams

Hosted Postgres

B2B SaaS

FinServ

Healthcare

We use cookies to collect data and improve our services. [Learn more](#)

Resources

[Blog](#)

[Support](#)

[System Status](#)

[Become a Partner](#)

[Partner Catalog](#)

[Brand Assets](#)

[Security & Compliance](#)

[Regions](#)

[SOC2](#)

[HIPAA](#)

Developers

[Documentation](#)

[Supabase Library](#)

[Changelog](#)

[RSS](#)

Community

[Events & Webinars](#)

[SupaSquad](#)

[Contributing](#)

[Open Source](#)

[DevTo](#)

Company

[Company](#)

[Careers](#)

[General Availability](#)

[Legal Hub](#)

[Privacy Policy](#)

[Privacy Settings](#)

[Acceptable Use Policy](#)

[Humans.txt](#)

[Lawyers.txt](#)

[Security.txt](#)

[Contact Us](#)