DATA PROCESSING ADDENDUM

Part 1

Processing Details

Customer name	Dylan Meehan
Customer address	1749 N Wells St
Customer contact	dmeehanj@gmail.com
Customer role	Controller/business (or processor/service provider for Customer's controller, as applicable)
Categories of personal data stored or processed through the Services	● **Contact information, first name, last name, email address.** ● **Usage information,** ● **Registration/account information, name, email address, password.** ● **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	**Authorized Users and Customer's end users, as submitted by Customer**
Special categories of personal data	◉ None ○ Special categories of personal data include: _____
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 set out in Schedule 3
Supervisory authority (EU only)	

By signing below, the Customer agrees to the data processing terms set out in Part 2 of this Data Processing Addendum and warrants that the information in Part 1 of this Data Processing Addendum is complete and accurate.

Signed for and on behalf of the Customer: Dylan Meehan

Name: Dylan Meehan

Position: Co-Founder

Date: 04/04/2002

Part 2

Data Processing Terms

(Version dated August 5, 2025)

This Data Processing Addendum, comprising Part 1 (*Processing Details*) and Part 2 (*Data Processing Terms*) (together, the "**DPA**") supplements and, from the date on which Customer signs or otherwise agrees to this DPA, forms part of the agreement entered into between the Customer and Supabase, Inc ("**Supabase**") on the terms set out at https://supabase.com/terms (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.

1. DEFINITIONS

1.1 Capitalized terms used but not defined within this DPA will have the meaning set forth in the Agreement. 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 US Data Protection Laws.

"Biometric Data" means Personal Data resulting from technical processing of physical,

physiological or behavioral characteristics such as fingerprints, facial images, iris or voice recognition data, used to identify a natural person.

"**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.

"**Controller Purposes**" means: (a) aggregating and anonymising information for the purpose of undertaking internal research and development to monitor, test, improve and alter the functionality of the Services; (b) monitoring the Customer's and Authorized Users' use of the Services for billing purposes, ensuring the security of the Services and identify fraudulent or malicious use of the Services; and (c) administering the Customer's relationship with Supabase under the Agreement.

"**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 Part 1 (*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 Part 1 (*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 leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to (including unauthorized internal access to), Covered Data. Security Incidents do not include unsuccessful incidents that are trivial in nature, such as pings and other broadcast service attacks that do not compromise the security of Covered Data.

“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 offences.

"**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 service provider, an entity appointed by Supabase to Process Covered Data on its behalf.

"**Swiss Data Protection Laws**" means the Swiss Federal Act 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 for 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.*, Connecticut Senate Bill 6, An Act Concerning Personal Data Privacy and Online Monitoring (as such law is chaptered and enrolled).

"**Usage Data**" means Personal Data relating to Authorized Users' use of the Services, including information about how frequently Authorized Users access the Services, the pages Authorized Users view on the Services and information about the Customer Data that Authorized Users upload and manage through the Services, in each case that Supabase collects or generates in connection with the provision of the Services.

1.2 The terms "**controller**", "**processor**", "**business**" and "**service provider**" have the meanings given to them in the Applicable Data Protection Laws.

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. The Parties further acknowledge that, for purposes of GDPR, Supabase acts as a controller with respect to the Processing of Usage Data for the Controller Purposes.

3. DETAILS OF DATA PROCESSING

3.1 The nature, purpose, and duration of the Processing of Personal Data under the Agreement and this DPA are described in the Agreement and in Part 1 (*Processing Details*) to this DPA.

3.2 Supabase shall comply with its obligations under Applicable Data Protection Laws. Save with respect to any Processing of Usage Data for the Controller Purposes, 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. 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 behavioural 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.

3.3 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.

4. COMPLIANCE

4.1 Customer shall comply with its obligations under Applicable Data Protection Laws and shall:

(a) provide (or ensure that the Customer's Controller provides) such information to Data Subjects regarding the Processing of their Covered Data in connection with Customer's use of the Services as required under Applicable Data Protection Laws;

(b) to the extent required for the 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; and

(c) implement appropriate technical and organisational 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.

(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. Controller certifies that it is in compliance with all laws applicable to the collection, use, and storage of Sensitive Data.

5. CONFIDENTIALITY AND DISCLOSURE

5.1 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 Supabase may Process Covered Data anywhere that Supabase or its Sub-processors maintain facilities, subject to the remainder of this clause 7.

6.2 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 additional instructions, applicable law or as necessary to provide Services requested by Customer. Customer shall not direct Supabase to process Covered Data in a specific region to the extent such

instruction violates applicable law, and shall indemnify, defend and hold Supabase harmless with regard to any liability arising out of any such violation.

6.3 Customer grants Supabase general authorisation (or, where applicable, has Customer's Controller's general authorisation) to engage any of the Sub-processors listed in Schedule 3, as amended in accordance with clause 7.4 (the "**Authorised Sub-processors**"), to Process Covered Data.

6.4 Supabase shall:

(a) enter into a written agreement with each Authorised 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 Authorised Sub-processor's compliance with the obligations under this DPA.

6.5 Supabase will provide Customer with at least thirty (30) days' notice of any proposed changes to the Authorised Sub-processors. Customer shall notify Supabase if it objects to the proposed change to the Authorised 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**").

6.6 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

7.1 Supabase will promptly notify Customer of any request received by Supabase or any Authorised Sub-processor from a Data Subject to assert their rights in relation to Covered Data under Applicable Data Protection Laws (a "**Data Subject Request**").

7.2 Other than with respect to any Processing of Usage Data for the Controller Purposes, as between the Parties, Customer will have sole discretion in responding to 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.

7.3 Supabase will provide Customer with reasonable assistance as necessary for Customer to fulfil its obligation under Applicable Data Protection Laws to respond to Data Subject Requests.

8. SECURITY

8.1 Supabase will implement and maintain appropriate technical and organisational 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 unauthorised 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 Supabase shall notify Customer promptly if Supabase determines that it can no longer meet its obligations under Applicable Data Protection Laws.

9.2 Customer may take reasonable and appropriate steps to stop and remediate unauthorized use of Covered Data upon reasonable notice.

9.3 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.

9.4 With respect to any audits conducted in accordance with clause 10.3:

(a) Customer may engage a third-party auditor to conduct the audit on its behalf; and

(b) 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.

9.5 Customer shall promptly notify Supabase of any non-compliance discovered during an audit.

9.6 The results of the audit shall be Supabase's Confidential Information.

9.7 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 the technical and organisational data security measures in accordance with industry standards.

9.8 If an audit requested by Customer is addressed in the documents or certification provided by Supabase in accordance with clause 10.7, and:

(a) the certification or documentation is dated within twelve (12) months of Customer's audit request; and

(b) Supabase confirms that there are no known material changes to the controls audited,

Customer agrees to accept that certification or documentation in lieu of conducting a physical audit of the controls covered by the relevant certification or documentation.

10. SECURITY INCIDENTS

10.1 Supabase shall notify Customer in writing without undue delay, and where feasible, within forty-eight (48) hours, after becoming aware of any Security Incident.

10.2 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.

10.3 Supabase shall provide reasonable assistance with Customer's investigation of any Security Incidents and any of Customer's obligations in relation to the Security Incident under Applicable Data Protection Laws, including any notification to Data Subjects or supervisory authorities.

10.4 Supabase's notification of or response to a Security Incident under this clause 11 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 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 Supabase shall:

(a) 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; and

(b) on expiry of the Retention Period, delete all copies of Covered Data Processed by Supabase or any Authorised Sub-processors.

12. STANDARD CONTRACTUAL CLAUSES

12.1 The Standard Contractual Clauses shall, as further set out in Schedule 3, 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 Law applies 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 to Supabase under this DPA in the absence of a transfer mechanism implementing adequate safeguards in respect of the Processing of that Covered Data, and any one or more of the following applies:

(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; or

(c) the transfer is an "onward transfer" (as defined in the applicable module of the SCCs).

12.2 The Parties agree that execution 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

14.1 The Parties hereby certify that they understand the requirements in this DPA and will comply with them.

14.2 The Parties agree to negotiate in good faith any amendments to this DPA as may be required in connection with changes in Applicable Data Protection Laws.

All notices to be provided by Supabase to Customer under this DPA shall be sent to the contact details identified in Part 1 of this DPA, 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 unauthorised 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;
- 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
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 service 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, as well as 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 our 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 ciphersuites.

Segmentation

Customer projects and Supabase internal Control Plane services are deployed in separate networks with firewall enforcing that only the expected traffic across the two is allowed. Additionally, 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 Customer projects that contain the user’s 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 generated per-project, and are in turn 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 ciphersuites) 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 aims 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 testing of its systems by hiring reputable third-party security firms, and remediates any findings as appropriate.

SCHEDULE 2

STANDARD CONTRACTUAL CLAUSES

1. EU SCCS

With respect to any transfers referred to in clause 13, the Standard Contractual Clauses shall be completed as follows:

1.1 The following modules of the SCCs will apply:

(a) where the Customer act 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 7.4 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) Part 1 (*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 Part 1 (*Processing Details*) and includes the processing of contact information and access credentials relating to, and support requests submitted by, Authorized Users for the purposes of granting Authorized Users access to the Services and providing support in relation to the Services;

(c) the data importer is Supabase, Inc whose offices located at 970 Toa Payoh North #07-04, Singapore 318992 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 organisational 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 Agreement in accordance with clause 13 and this Schedule 2;

(b) Table 1 of the Approved Addendum shall be completed as set out in paragraph 1.7 of this Schedule 2;

(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 Swiss Addendum will apply to any Processing of Covered Data that is subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the EU GDPR.

3.2 Interpretation of this Addendum

(a) Where this Addendum uses terms that are defined in the Standard Contractual Clauses, those terms will have the same meaning as in the Standard Contractual Clauses. In addition, the following terms have the following meanings:

"**Addendum**" means this addendum to the Clauses;

"**Clauses**" means the Standard Contractual Clauses as incorporated into this DPA in accordance with clause 12 and as further specified in this Schedule 3; and

"**FDPIC**" means the Federal Data Protection and Information Commissioner.

(b) This Addendum shall be read and interpreted in a manner that is consistent with Swiss Data Protection Laws, and so that it fulfils the Parties' obligation to provide appropriate safeguards as required by Article 46 GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

(c) This Addendum will not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Data Protection Laws.

(d) Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Swiss Addendum has been entered into.

(e) In relation to any Processing of Personal Data subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the GDPR, this Addendum amends and supplements the Clauses to the extent necessary so they operate:

(i) for transfers made by the data exporter to the data importer, to the extent that Swiss Data Protection Laws apply to the data exporter's Processing when making that transfer; and

(ii) to provide appropriate safeguards for the transfers in accordance with Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

3.3 Hierarchy

In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to Data Subjects will prevail.

3.4 Changes to the Clauses for transfers exclusively subject to Swiss Data Protection Laws

To the extent that the data exporter's Processing of Personal Data is exclusively subject to Swiss Data Protection Laws, or the transfer of Personal Data from a data exporter to a data

importer under the Clauses is an "onward transfer" (as defined in the Clauses, as amended by the remainder of this paragraph 3.4 the following amendments are made to the Clauses:

(a) References to the "Clauses" or the "SCCs" mean this Swiss Addendum as it amends the SCCs.

(b) References to "Regulation (EU) 2016/679" or "that Regulation" or ""GDPR" are replaced by "Swiss Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" or "GDPR" are replaced with the equivalent Article or Section of Swiss Data Protection Laws extent applicable.

(c) References to Regulation (EU) 2018/1725 are removed.

(d) References to the "European Union", "Union", "EU" and "EU Member State" are all replaced with "Switzerland".

(e) Clause 13(a) and Part C of Annex I are not used; the "competent supervisory authority" is the FDPIC;

(f) Clause 17 is replaced to state

(g) "These Clauses are governed by the laws of Switzerland".

(h) Clause 18 is replaced to state:

"Any dispute arising from these Clauses relating to Swiss Data Protection Laws will be resolved by the courts of Switzerland. A Data Subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence. The Parties agree to submit themselves to the jurisdiction of such courts."

(i) Until the entry into force of the revised Swiss Data Protection Laws, the Clauses will also protect Personal Data of legal entities and legal entities will receive the same protection under the Clauses as natural persons.

3.5 Supplementary provisions for transfers of Personal data subject to both the GDPR and Swiss Data Protection Laws

(a) To the extent that the data exporter's Processing of Personal Data is subject to both Swiss Data Protection Laws and the GDPR, or the transfer of Personal Data from a data exporter to a data importer under the Clauses is an "onward transfer" under both the Clauses and the Clauses as amended by the remainder of this paragraph 3.5 of this Addendum:

(i) for the purposes of Clause 13(a) and Part C of Annex I:

(A) the FDPIC shall act as competent supervisory authority with respect to any transfers of Personal Data to the extent Swiss Data Protection Laws apply to the data exporter's Processing when making that transfer, or such transfer is an "onward transfer" as defined in the Clauses (as amended by paragraph 3.3 of this Addendum); and

(B) subject to the provisions of paragraph 2 of this Schedule 2 (UK Addendum), the supervisory authority identified in Part 1 (*Processing Details*) shall act as competent supervisory authority with respect to any transfers of Personal Data to the extent the GDPR applies to the data exporter's processing, or such transfer is an "onward transfer" as defined in the Clauses.

(b) the terms "European Union", "Union", "EU", and "EU Member State" shall not be interpreted in a way that excludes the ability of Data Subjects in Switzerland bringing a claim in their place of habitual residence in accordance with Clause 18(c) of the Clauses; and

(c) Until the entry into force of the revised Swiss Data Protection Laws, the Clauses will also protect Personal Data of legal entities and legal entities will receive the same protection under the Clauses as natural persons.

4. Transfers under the laws of other jurisdictions

4.1 With respect to any transfers of Personal Data referred to in clause 13.1(b) (each a "**Global Transfer**"), the SCCs shall not be interpreted in a way that conflicts with rights and obligations provided for in the Exporter Data Protection Laws.

4.2 For the purposes of any Global Transfers, the SCCs shall be deemed to be amended to the extent necessary so that they operate:

(a) for transfers made by the applicable data exporter to the data importer, to the extent the Exporter Data Protection Laws apply to that data exporter's Processing when making that transfer; and

(b) to provide appropriate safeguards for the transfers in accordance with the Exporter Data Protection Laws.

4.3 The amendments referred to in clause paragraph 4.2 include (without limitation) the following:

(a) references to the "GDPR" and to specific Articles of the GDPR are replaced with the equivalent provisions under the Exporter Data Protection Laws;

(b) reference 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 applicable supervisory in the Exporter Jurisdiction; and

(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 1;

(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
SUB-PROCESSORS

Name of Sub-processor	**Description of Processing**
Supabase Pte. Ltd	Provision of support services
Active Campaign, LLC d/b/a Postmark	Communication with Authorized Users in connection with the provision of the Services and support
Amazon Web Services, Inc	Provision of hosting services
Atlassian Corporation Plc	Provision of status page services
Braintrust Data, Inc	Provision of monitoring and tracing
Clay Labs Inc.	Provision of customer insight services
Clazar, Inc	Provision of marketplace services
Cloudflare, Inc	Provision of hosting services
ConfigCat Korlátolt Felelősségű Társaság	Feature flagging
Google, LLC	Provision of hosting services
Fly.io, Inc	Provision of hosting services
FrontApp, Inc	Communication with Authorized Users in connection with the provision of the Services and support
Functional Software, Inc d/b/a Sentry	Error monitoring and tracing
Github, Inc	Authorized Users account authentication
Hex Technologies, Inc	Provision of data analytics services
Hubspot, Inc	Communication with Authorized Users in connection with the provision of the Services and support
Notion Labs, Inc	Communication with Authorized Users in connection with the provision of the Services and support
OpenAI, LLC	Provision of natural language processing and generation services

PandaDoc, Inc	Communication with Authorized Users in connection with the provision of the Services and support
Slack Technologies, LLC	Communication with Authorized Users in connection with the provision of the Services and support
Upstash, Inc	Provision of serverless data hosting services
Vercel, Inc	Provision of hosting services

CERTIFICATE *of* SIGNATURE

REF. NUMBER
Z3TXD-TJX5L-XBTMD-UG3ZM

DOCUMENT COMPLETED BY ALL PARTIES ON
18 MAY 2026 19:44:19
UTC

SIGNER	TIMESTAMP	SIGNATURE
EMAIL DMEEHANJ@GMAIL.COM	SENT 18 MAY 2026 19:37:38 VIEWED 18 MAY 2026 19:39:00 SIGNED 18 MAY 2026 19:44:19	 IP ADDRESS 205.178.84.195 LOCATION CHICAGO, UNITED STATES

RECIPIENT VERIFICATION

EMAIL VERIFIED
18 MAY 2026 19:39:00

supabase

Data Processing Addendum

Part 1
Processing Details

Customer name	
Customer address	
Customer contact	
Customer role	Controller/business (or processor/service provider for Customer's controller, as applicable)
Categories of personal data stored or processed through the Services	• Contact information, first name, last name, email address. • Usage information. • Registration/account information, name, email address, password. • 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	Authorized Users and Customer's end users, as submitted by Customer
Special categories of personal data	☐ None ☐ Special categories of personal data include: _____
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.

Customer name	
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 set out in Schedule 3
Supervisory authority (EU only)	

By signing below, the Customer agrees to the data processing terms set out in Part 2 of this Data Processing Addendum and warrants that the information in Part 1 of this Data Processing Addendum is complete and accurate.

Signed for and on behalf of the Customer: _____

Name: _____

Position: _____

Date: _____

Part 2
Data Processing Terms
(Version dated May 4, 2026)

This Data Processing Addendum, comprising Part 1 (*Processing Details*) and Part 2 (*Data Processing Terms*) (together, the **"DPA"**) supplements and, from the date on which Customer signs or otherwise agrees to this DPA, 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"**) (and the agreement, 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.

1. DEFINITIONS

1.1 Capitalized terms used but not defined within this DPA will have the meaning set forth in the Agreement. 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 US Data Protection Laws.

"Biometric Data" means Personal Data resulting from technical processing of physical, physiological or behavioral characteristics such as fingerprints, facial images, iris or voice recognition data, used to identify a natural person.

"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.

"Controller Purposes" means: (a) aggregating and anonymizing information for the purpose of undertaking internal research and development to monitor, test, improve and alter the functionality of the Services; (b) monitoring the Customer's and Authorized Users' use of the Services for billing purposes, ensuring the security of the Services and identifying fraudulent or malicious use of the Services; and (c) administering the Customer's relationship with Supabase under the Agreement.

"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 Part 1 (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 Part 1 (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 leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to (including unauthorized internal access to), Covered Data. Security Incidents do not include unsuccessful incidents that are trivial in nature, such as pings and other broadcast service attacks that do not compromise the security of Covered Data.

"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).

"Usage Data" means Personal Data relating to Authorized Users' use of the Services, including information about how frequently Authorized Users access the Services, the pages Authorized Users view on the Services and information about the Customer Data that Authorized Users upload and manage through the Services, in each case that Supabase collects or generates in connection with the provision of the Services.

1.2 The terms **"controller"**, **"processor"**, **"business"** and **"service provider"** have the meanings given to them in the Applicable Data Protection Laws.

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. The Parties further acknowledge that, for purposes of GDPR, Supabase acts as a controller with respect to the Processing of Usage Data for the Controller Purposes.

3. DETAILS OF DATA PROCESSING

3.1 The nature, purpose, and duration of the Processing of Personal Data under the Agreement and this DPA are described in the Agreement and in Part 1 (Processing Details) to this DPA.

3.2 Supabase shall comply with its obligations under Applicable Data Protection Laws. Save with respect to any Processing of Usage Data for the Controller Purposes, 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. 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.

3.3 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.

4. COMPLIANCE

4.1 Customer shall comply with its obligations under Applicable Data Protection Laws and shall:

(a) provide (or ensure that the Customer's Controller provides) such information to Data Subjects regarding the Processing of their Covered Data in connection with Customer's use of the Services as required under Applicable Data Protection Laws;

(b) to the extent required for the 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. Controller certifies that it is in compliance with all laws applicable to the collection, use, and storage of Sensitive Data.

5. CONFIDENTIALITY AND DISCLOSURE

5.1 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 Supabase may Process Covered Data anywhere that Supabase or its Sub-processors maintain facilities, subject to the remainder of this clause 6.

6.2 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 additional instructions, applicable law or as necessary to provide Services requested by Customer. Customer shall not direct Supabase to Process Covered Data in a specific region to the extent such instruction violates applicable law, and shall indemnify, defend and hold Supabase harmless with regard to any liability arising out of any such violation.

6.3 Customer grants Supabase general authorization (or, where applicable, has Customer's Controller's general authorization) to engage any of the Sub-processors listed in Schedule 3, as amended in accordance with clause 6.4 (the **"Authorized Sub-processors"**), to Process Covered Data.

6.4 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.

6.5 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"**).

6.6 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

7.1 Supabase will promptly notify Customer of any request received by Supabase or any Authorized Sub-processor from a Data Subject to assert their rights in relation to Covered Data under Applicable Data Protection Laws (a **"Data Subject Request"**).

7.2 Other than with respect to any Processing of Usage Data for the Controller Purposes, as between the Parties, Customer will have sole discretion in responding to 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.

7.3 Supabase will 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

8.1 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 Supabase shall notify Customer promptly if Supabase determines that it can no longer meet its obligations under Applicable Data Protection Laws.

9.2 Customer may take reasonable and appropriate steps to stop and remediate unauthorized use of Covered Data upon reasonable notice.

9.3 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.

9.4 With respect to any audits conducted in accordance with clause 9.3:

(a) Customer may engage a third-party auditor to conduct the audit on its behalf; and

(b) 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.

9.5 Customer shall promptly notify Supabase of any non-compliance discovered during an audit.

9.6 The results of the audit shall be Supabase's Confidential Information.

9.7 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 the technical and organizational data security measures in accordance with industry standards.

9.8 If an audit requested by Customer is addressed in the documents or certification provided by Supabase in accordance with clause 9.7, and:

(a) the certification or documentation is dated within twelve (12) months of Customer's audit request; and

(b) Supabase confirms that there are no known material changes to the controls audited,

Customer agrees to accept that certification or documentation in lieu of conducting a physical audit of the controls covered by the relevant certification or documentation.

10. SECURITY INCIDENTS

10.1 Supabase shall notify Customer in writing without undue delay, and where feasible, within forty-eight (48) hours, after becoming aware of any Security Incident.

10.2 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.

10.3 Supabase shall provide reasonable assistance with Customer's investigation of any Security Incidents and any of Customer's obligations in relation to the Security Incident under Applicable Data Protection Laws, including any notification to Data Subjects or supervisory authorities.

10.4 Supabase's notification of or response to a Security Incident under this 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 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 Supabase shall:

(a) 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; and

(b) on expiry of the Retention Period, delete all copies of Covered Data Processed by Supabase or any Authorized Sub-processors.

12. STANDARD CONTRACTUAL CLAUSES

12.1 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 to Supabase under this DPA in the absence of a transfer mechanism implementing adequate safeguards in respect of the Processing of that Covered Data, and any one or more of the following applies:

(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;

(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; or

(c) the transfer is an "onward transfer" (as defined in the applicable module of the SCCs).

12.2 The Parties agree that execution 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

14.1 The Parties hereby certify that they understand the requirements in this DPA and will comply with them.

14.2 The Parties agree to negotiate in good faith any amendments to this DPA as may be required in connection with changes in Applicable Data Protection Laws.

14.3 All notices to be provided by Supabase to Customer under this DPA shall be sent to the contact details identified in Part 1 of this DPA, 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

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 Control Plane services are deployed in separate networks with firewalls enforcing that only the expected traffic across the two is allowed. Additionally, 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 generated per-project, and are in turn 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 testing of its systems by hiring reputable third-party security firms, and remediates any findings as appropriate.

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 6.5 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) Part 1 (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 Part 1 (Processing Details) and includes the processing of contact information and access credentials relating to, and support requests submitted by, Authorized Users for the purposes of granting Authorized Users access to the Services and providing support in relation to the Services; and

(c) the data importer is Supabase, Inc whose offices are located at 970 Toa Payoh North #07-04, Singapore 318992 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 2;

(b) Table 1 of the Approved Addendum shall be completed as set out in paragraph 1.7 of this Schedule 2;

(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 supervisory authority is the Swiss Federal Data Protection and Information Commissioner ("FDPIC") insofar as the data transfer is governed by the Swiss Data Protection Laws; and the supervisory authority is the 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) reference 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 applicable supervisory in the Exporter Jurisdiction; and

(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 Part 1 (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
SUB-PROCESSORS

Name of Sub-processor	Description of Processing
Supabase, Inc.	Provision of support services
Active Campaign, LLC d/b/a Postmark	Communication with Authorized Users in connection with the provision of the Services and support
Amazon Web Services, Inc	Provision of hosting services
Atlassian Corporation Plc	Provision of status page services
Braintrust Data, Inc	Provision of monitoring and tracing
Clay Labs Inc.	Provision of customer insight services
Clazar, Inc	Provision of marketplace services
Cloudflare, Inc	Provision of hosting services
ConfigCat Korlátolt Felelősségű Társaság	Feature flagging
Google, LLC	Provision of hosting services
Fly.io, Inc	Provision of hosting services
FrontApp, Inc	Communication with Authorized Users in connection with the provision of the Services and support
Functional Software, Inc d/b/a Sentry	Error monitoring and tracing
Github, Inc	Authorized Users account authentication
Hex Technologies, Inc	Provision of data analytics services
Hubspot, Inc	Communication with Authorized Users in connection with the provision of the Services and support
Notion Labs, Inc	Communication with Authorized Users in connection with the provision of the Services and support
OpenAI, LLC	Provision of natural language processing and generation services

Name of Sub-processor	Description of Processing
PandaDoc, Inc	Communication with Authorized Users in connection with the provision of the Services and support
Slack Technologies, LLC	Communication with Authorized Users in connection with the provision of the Services and support
Upstash, Inc	Provision of serverless data hosting services
Vercel, Inc	Provision of hosting services