As part of our commitment to customer privacy, we have prepared and pre-signed the following Data Processing Addendum ("DPA"). The DPA is intended to help Customers and Supabase (acting as a processor) meet their respective data protection obligations under applicable data protection laws. The DPA applies where the personal data that we process on behalf of Customers is subject to the EU General Data Protection Regulation (EU GDPR), the UK General Data Protection Regulation (UK GDPR) and/or Swiss data protection laws.

Customers should complete Schedule 1, then add their signature and send the completed document to privacy@supabase.io for our records.

Last updated: [22.05.03]

DATA PROCESSING AGREEMENT
(EEA AND UK AND SWITZERLAND)

PARTIES

(1) Customer, as defined below; and

(2) Supabase, Inc., a company registered in Delaware with number 7816270 whose registered office is at 970 Toa Payoh North #07-04, Singapore 318992 (the "**Company**" or "**Supabase**"),

(each a "**Party**" and collectively the "**Parties**").

BACKGROUND

(A) The Company provides the services ("**Services**") described in the Company's terms of service available at https://supabase.io/docs/company/terms (the "**Agreement**"). This Data Processing Agreement (the "**DPA**") supplements the Agreement with regard to the subject matter hereof. For the avoidance of doubt, this DPA shall in relation to its scope supersede any and all terms of previously concluded data processing agreements between Company and Customer.

(B) To the extent that the Company processes any personal data as a processor (as defined below) on behalf of the Customer (or, where applicable, the Customer Affiliates, i.e. (i) Customer's affiliates located in the European Economic Area ("**EEA**"), United Kingdom ("**UK**") and/or Switzerland and/or (ii) those affiliates located in other countries (but whose personal data is subject to the GDPR, the UK Data Protection Act 2018 and/or Swiss Data Protection Laws as defined in Section 3.4(a)) in connection with the provision of the Services, where that personal data falls within the scope of the GDPR, the Parties have agreed that it shall do so on the terms of this DPA.

1. DEFINITIONS

1.1 Terms defined in the Agreement shall, unless otherwise defined in this DPA, have the same meanings when used in this DPA and the following terms used in this DPA shall be defined as follows:

"**Customer Affiliate**" means a subsidiary of the Customer or a holding company of the Customer or any other subsidiary of that holding company;

"**Customer Personal Data**" means the personal data processed by the Company on behalf of the Customer in connection with the provision of the Services, as further described in Schedule 2;

"**EEA**" means the European Economic Area;

"**GDPR**" means Regulation (EU) 2016/679 (the "**EU GDPR**") or, where applicable, the "**UK GDPR**" as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 or, where applicable, the equivalent provision under Swiss Data Protection Laws as defined in Section 3.4(a);

"**Member State**" means a member state of the EEA, being a member state of the European Union, Iceland, Norway, or Liechtenstein;

"**Standard Contractual Clauses**" or "**SCC**" means Module Two (*controller to processor*) of the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914;

"**sub-processor**" means a processor appointed by the Processor to process Customer Personal Data.

The terms "**personal data**", "**controller**", "**processor**", "**data subject**", "**process**", "**personal data breach**" and "**supervisory authority**" shall have the same meaning as set out in the GDPR.

2. INTERACTION WITH THE AGREEMENT

2.1 This DPA supplements the Agreement with respect to any processing of Customer Personal Data by the Company and the Parties agree that with the execution of this DPA, this DPA including the SCC shall, by default, be concluded between Company (as data importer under the SCC) and Customer as well as any Customer Affiliate, directly or indirectly, bound by the Agreement, (respectively as data exporter under the SCC).

2.2 The Customer warrants that, with respect to the Customer Affiliates directly or indirectly, bound by the Agreement, it is duly authorised to conclude this DPA including the SCC for and on behalf of any such Customer Affiliates, and that, upon executing this DPA, each Customer Affiliate shall be bound by the terms of this DPA including the SCC as if they were the Customer. Where the Customer may not be duly authorized to conclude the DPA including the SCC for and on behalf of a Customer Affiliate, Customer warrants that such Customer Affiliate will submit to the Company without delay a signed copy of this DPA which shall have the same effect as the signature of Customer on behalf of a Customer Affiliate. Customer shall provide all the information necessary to complete Schedule 1 as to itself and Customer Affiliates

2.3 The Customer warrants that it is duly mandated by any Customer Affiliates on whose behalf the Company processes Customer Personal Data in accordance with this DPA to:

(a) enforce the terms of this DPA including the SCC on behalf of the Customer Affiliates, and to act on behalf of the Customer Affiliates in the administration and conduct of any claims arising in connection with this DPA; and

(b) receive and respond to any notices or communications under this DPA including the SCC on behalf of Customer Affiliates.

2.4 The Parties agree that any notice or communication sent by the Company to the Customer shall satisfy any obligation to send such notice or communication to a Customer Affiliate.

2.5 As explicitly allowed by Clause 2(a) s 2 of the SCC, Sections 1 through 14 of this DPA are meant to supplement the SCC, in particular, by way of providing guidance for their practical implementation and are not intended to contradict, directly or indirectly, any clauses of the SCC. In the event of any conflict between contractual documents, the order of prevalence shall be as follows (in accordance with Clause 5 SCC):

(a) the SCC (or, with respect to transfers of Customer Personal Data subject to the UK GDPR, the SCC as amended by clause 3.3, or, with respect to transfers of Customer Personal Data subject to the to Swiss Data Protection Laws, the SCC as amended by clause 3.4);

(b) the Schedules of this DPA to the extent that they are meant to complete the SCC;

(c) the main body of this DPA including its Schedules;

(d) the Agreement and any other contractual documents.

3. STANDARD CONTRACTUAL CLAUSES

3.1 Subject to clause 3.3, the SCC shall apply to any transfers of Customer Personal Data falling within the scope of the GDPR from the Customer and Customer Affiliates (respectively as data exporter) to the Company (as data importer).

3.2 For the purposes of the SCC:

(a) Annex I.A (*List of Parties*) shall be deemed to incorporate the information in Schedule 1;

(b) Annex I.B (*Description of Transfer*) shall be deemed to incorporate the information in Schedule 2;

(c) Annex I.C (*Competent Supervisory Authority*) shall be deemed to refer to the supervisory authority respectively identified in Schedule 1;

(d) Annex II (*Technical and Organisational Measures*) shall be deemed to incorporate the information in Schedule 4.

3.3 With respect to any transfers of Customer Personal Data falling within the scope of the UK GDPR from the Customer and Customer Affiliates (respectively as data exporter) to the Company (as data importer):

(a) neither the SCC nor the DPA shall be interpreted in a way that conflicts with rights and obligations provided for in any 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 (together, the "**UK Data Protection Laws**");

(b) the SCC are deemed to be amended to the extent necessary so they operate:

(i) for transfers made by the Customer and Customer Affiliates to the Company, to the extent that UK Data Protection Laws apply to the Customer's processing when making that transfer;

(ii) to provide appropriate safeguards for the transfers in accordance with Article 46 of the UK GDPR;

(c) the amendments referred to in clause 3.3(b) include (without limitation) the following:

(i) references to “Regulation (EU) 2016/679” or “that Regulation” are replaced by “UK GDPR” and references to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article of the UK GDPR;

(ii) references to Regulation (EU) 2018/1725 are removed;

(iii) references to the "Union", "EU" and "EU Member State" are all replaced with the "UK";

(iv) the "competent supervisory authority" shall be the Information Commissioner;

(v) clause 17 of the SCC is replaced with the following:

"*These Clauses are governed by the laws of England and Wales*";

(vi) clause 18 of the SCC is replaced with the following:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts";

(vii) any footnotes to the SCC are deleted in their entirety.

3.4 With respect to any transfers of Customer Personal Data falling within the scope of the Swiss Data Protection Laws from the Customer and Customer Affiliates (respectively as data exporter) to the Company (as data importer):

(a) neither the SCC nor the DPA shall be interpreted in a way that conflicts with rights and obligations provided for in any laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in Switzerland (together, the "**Swiss Data Protection Laws**");

(b) the SCC are deemed to be amended to the extent necessary so they operate:

(i) for transfers made by the Customer and Customer Affiliates to the Company, to the extent that Swiss Data Protection Laws apply to the Customer's processing when making that transfer;

(ii) to provide appropriate safeguards for the transfers in accordance with Swiss Data Protection Laws;

(c) the amendments referred to in clause 3.4(b) include (without limitation) the following:

(i) references to “Regulation (EU) 2016/679” or “that Regulation” are replaced by “Swiss Data Protection Laws” and references to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent provision of Swiss Data Protection Laws;

(ii) references to Regulation (EU) 2018/1725 are removed;

(iii) references to the "Union", "EU" and "EU Member State" are all replaced with the "Switzerland";

(iv) the "competent supervisory authority" shall be the competent Swiss data protection authority;

(v) clause 17 of the SCC is replaced with the following:

"*These Clauses are governed by the laws of Switzerland*";

(vi) clause 18 of the SCC is replaced with the following:

"Any dispute arising from these Clauses shall 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 any country in Switzerland. The Parties agree to submit themselves to the jurisdiction of such courts";

(vii) any footnotes to the SCC are deleted in their entirety.

4. INSTRUCTIONS FOR DATA PROCESSING

4.1 The Parties agree that, for the purposes of clause 8.1(a) of the SCC, the Agreement and this DPA including the SCC constitute Customer's instructions for the processing of Customer Personal Data.

4.2 To the extent that any of the Customer's instructions require processing of Customer Personal Data in a manner that falls outside the scope of the Services, the Company may:

(a) make the performance of any such instructions subject to the payment by the Customer of any costs and expenses incurred by the Company or such additional charges as the Company may reasonably determine; or

(b) terminate the Agreement and the Services.

4.3 Notwithstanding clause 8.1 of the SCC, the Company may process Customer Personal Data to the extent required by applicable law in the EEA or a Member State, the UK, or Switzerland, in each case to which the respective processing of Customer Personal Data is subject, whereas the Company shall, to the extent permitted by such applicable law, inform the Customer of that legal requirement before processing that Customer Personal Data.

4.4 The Customer may direct Company to process Customer Personal Data in connection with the Services in the specific geographic regions in which the Company elects to make the Services available from time to time (each a “Region”). Once Customer has provided such a direction, Company will not transfer Customer Data from Customer’s selected Region(s) except as necessary to comply with additional directions from Customer or to comply with law or with a binding order of a governmental body. Customer shall not direct Company to process Customer Personal Data in a specific Region in a manner that violates applicable law, and shall indemnify, defend and hold Company harmless with regard to any liability arising out of any such violation.

5. CUSTOMER WARRANTIES AND UNDERTAKINGS

The Customer represents and warrants that:

(a) it has provided all applicable notices to data subjects and, to the extent required, obtained consent from data subjects in each case as required for the lawful processing of Customer Personal Data in accordance with the Agreement and this DPA;

(b) without prejudice to the generality of clause 8 of the SCC (as applicable), taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the security measures set out in Schedule 4 are:

(i) appropriate to ensure the security of the Customer Personal Data, including protection against a personal data breach; and

(ii) otherwise consistent with the Customer's obligations under Article 32 of the GDPR.

6. SUB-PROCESSORS

6.1 The Parties agree that, in accordance with option 2 of clause 9 of the SCC, the Customer gives the Company general authorisation to engage sub-processors from the agreed list, as set out under Schedule 3.

6.2 In order to fulfil its obligation under option 2 of Clause 9(a) SCC, the Company shall provide the Customer with at least 10 days' notice of any proposed changes to the sub-processors it uses to process Customer Personal Data (including any addition or replacement of any sub-processors), including any information reasonably necessary to enable the Customer to exercise its right to object.

6.3 If the Customer objects to the Company's use of a new sub-processor (including when exercising its right to object under option 2 of clause 9(a) of the SCC), it shall provide the Company with:

(a) written notice of the objection within 10 days after the Company has provided notice to the Customer as described in clause 6.2; and

(b) documentary evidence that reasonably shows that the sub-processor does not or cannot comply with the requirements in this DPA (including the SCC),

(an "**Objection**").

6.4 In the event of an Objection, the Company will use reasonable endeavours to make available to the Customer a change in the Services, or will recommend a commercially reasonable change to the Services to prevent the applicable sub-processor from processing the Customer Personal Data.

6.5 If the Company is unable to make available such a change in accordance with clause 6.4 within a reasonable period of time, which shall not exceed 60 days, either Party may terminate the Agreement by providing not less than 60 days' written notice to the other Party. During such notice period, the Company may suspend the affected portion of the Services.

6.6 In accordance with Clause 9(b) SCC, any sub-processor is obliged before initiating the processing, to commit itself by way of written contract to comply with, in substance, the same data protection obligations as the ones under this DPA including the SCC

7. SECURITY AND AUDITS

7.1 The Company may, by written notice to the Customer, vary the security measures set out in Schedule 4, including (where applicable) following any review by the Company of such measures in accordance with clause 8.6 of the SCC, provided that such variation does not reduce the overall level of protection afforded to the Customer Personal Data by the Company under this DPA.

7.2 With respect to any audits conducted under clauses 8.9(c) and (d) of the SCC, the Parties agree that:

(a) all such audits shall be conducted:

(i) on reasonable written notice to the Company;

(ii) only during the Company's normal business hours; and

(iii) in a manner that does not disrupt the Company's business;

(b) the Customer (or, where applicable, a third party independent auditor appointed by the Customer) shall:

(i) enter into a confidentiality agreement with the Company prior to conducting the audit in such form as the Company may request; and

(ii) [be able to perform audits on Company's or sub-processor's premises, if Customer has justifiable reason to believe that Company is not complying with this DPA including the SCC, once per year (unless there are specific indications that require a more frequent inspection); and]

(iii) ensure that its personnel comply with the Company's and any sub-processor's policies and procedures when attending the Company's or sub-processor's premises, as notified to the Customer by the Company or sub-processor.

8. COSTS

The Customer shall pay to the Company on demand all costs and expenses incurred by the Company in connection with:

(a) implementing any changes to the Services under clause 6.4;

(b) facilitating and contributing to any audits of the Company under or clauses 8.9(c) and (d) of the SCC;

(c) facilitating and contributing to any audits of the Company conducted by a supervisory authority;

(d) responding to queries or requests for information from the Customer relating to the processing of Customer Personal Data under clauses 8.9(a), (c) or (e) of the SCC;

(e) any assistance provided by the Company to the Customer with its fulfilment of its obligations to respond to data subjects' requests for the exercise of their rights under the GDPR and under clauses 10(a), (b) or (c) of the SCC; and

(f) any assistance provided by the Company to the Customer with any data protection impact assessments or prior consultation with any supervisory authority of the Customer.

9. LIABILITY

9.1 Subject to clause 9.2, any exclusions or limitations of liability set out in the Agreement shall apply to any losses suffered by either Party (whether in contract, tort (including negligence) or for restitution, or for breach of statutory duty or misrepresentation or otherwise) under this DPA including the SCC as if this DPA was incorporated into, and formed a part of the Agreement.

9.2 Nothing in this DPA or the Agreement shall limit or exclude any liability of either Party to data subjects or not-for-profit bodies, organisations or associations under the conditions set out in Article 80(1) of the GDPR under the SCC.

9.3 The Customer shall indemnify the Company against any amounts paid by the Company to a data subject or not-for-profit body, organisation or association under the conditions set out in Article 80(1) of the GDPR in connection with any claim brought under the SCC, to the extent such amounts would not have been paid had the limitations and exclusions in the Agreement applied to such claims.

10. DURATION AND TERMINATION

The duration of this DPA depends on the duration of the Agreement. It commences and terminates with the provision of the Services under the Agreement, unless otherwise stipulated in the provisions of this DPA.

11. MODIFICATIONS

Company may modify or supplement these DPA, with notice to Customer, (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with applicable law, (iii) to implement amended standard contractual clauses laid down by the European Commission or (iv) to adhere to a code of conduct or certification mechanism approved or certified pursuant to Art. 40, 42 and 43 of the GDPR. Customer shall notify Company if it does not agree to a modification, in which case Company may terminate these DPA and the Master Services Agreement with two (2) weeks' prior written notice, whereby in the case of an objection not based on non-compliance of the modifications with applicable data protection law, Company shall remain entitled to claim its agreed remuneration until the term end.

12. LAW AND JURISDICTION

12.1 Notwithstanding the provisions of the Agreement, this DPA and the SCC (pursuant to its clause 17) shall be governed by, and construed in accordance with:

(a) to the extent that the EU GDPR applies to the processing of Customer Personal Data, the law of the Member State in which the Customer is established, provided such Member State

law allows for third-party beneficiary rights; otherwise, the law of the Federal Republic of Germany;

(b) to the extent that UK Data Protection Laws apply to the processing of Customer Personal Data, the law of England and Wales;

(c) to the extent that Swiss Data Protection Laws apply to the processing of Customer Personal Data, the law of Switzerland.

12.2 Notwithstanding the provisions of the Agreement, as regards to this DPA and the SCC (pursuant to its clause 18), the Parties submit themselves to the jurisdiction of the following courts:

(a) to the extent that the EU GDPR applies to the processing of Customer Personal Data, the courts of the Member State in which the Customer is established; otherwise, the courts of the Federal Republic of Germany;

(b) to the extent that UK Data Protection Laws apply to the processing of Customer Personal Data, the courts of England and Wales;

(c) to the extent that Swiss Data Protection Laws apply to the processing of Customer Personal Data, the courts of Switzerland.

13. THIRD PARTY RIGHTS

Other than the right of data subjects or not-for-profit bodies, organisations or associations under the conditions set out in Article 80(1) of the GDPR to bring claims under the SCC (as applicable), a person who is not a party to this DPA may not enforce any of its terms.

14. GENERAL

14.1 **Written Form**. Any side agreements to this DPA as well as changes and amendments of this DPA or the Services hereunder, including this clause 14.1, shall be in writing.

14.2 **Written Communications**. Applicable laws may require that some of the information or communications that the Parties send to each other should be in writing. The Parties agree, for the purposes of this DPA, that communication between them will mainly be electronic and that the Parties will contact each other by e-mail. For contractual purposes, the Parties agree to this electronic means of communication and the Parties acknowledge that all contracts, notices, information and other communications provided by one Party to the other electronically comply with any legal requirement that such communications be in writing.

14.3 **Notices.** Any notices given by one Party to the other will be served if validly served in accordance with the Agreement, and will be deemed received in accordance with the relevant provisions in the Agreement.

14.4 **Rights and remedies.** Except as expressly provided in the Agreement, the rights and remedies provided under the Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

14.5 **No partnership or agency.** Nothing in the DPA is intended to, or shall be deemed to, establish any partnership or joint venture between any of the Parties, constitute any Party the agent of another Party, or authorise any Party to make or enter into any commitments for or on behalf of any other Party. Each Party confirms it is acting on its own behalf and not for the benefit of any other person.

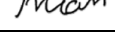
14.6 **Transfer of rights and obligations**. Neither Party shall transfer, assign or otherwise deal in the DPA, or any of its rights and obligations under this DPA, other than to an assignee of that Party's rights and obligations under the Agreement.

14.7 **Waiver**. No forbearance or delay by either Party in enforcing its rights shall prejudice or restrict the rights of that Party, and no waiver of any such rights or any breach of any contractual terms shall be deemed to be a waiver of any other right or of any later breach.

14.8 **Variation.** No variation of this DPA shall be effective unless it is in writing and signed by the Parties (or their authorised representatives).

14.9 **Severability**. If any provision of the DPA is judged to be illegal or unenforceable, the continuation in full force and effect of the remainder of the provisions of the DPA shall not be prejudiced.

SIGNED by the **Parties:**

Party	Name of Signee	Position of Signee	Date of Signature	Signature
[Controller] a company registered in [***] with number [***] whose registered office is at [***] (the "**Customer**")				
Company	**Inian Parameshwaran**	**Engineering**	22.04.25	

Schedule 1

PARTIES TO THE PROCESSING

1. Relevant Information on Company / data importer and Customer / data exporter

Party:	**Customer / data exporter** ***[to be completed by Customer]***	**Company / data importer**
Role	**Controller**	**Processor**
Contact person	Name: See signature line above. Position: See signature line above. Contact details: _____	Name: See signature line above. Position: See signature line above. Contact details: privacy@supabase.io
Where applicable: Data protection officer and/or UK representative		**Inian Parameshwaran**
Where applicable: Data protection officer and/or EU representative		**Inian Parameshwaran**
Activities relevant to the data transferred		Performance of the Services
Competent supervisory authority	To the extent that the EU GDPR applies and the competent supervisory authority is not explicitly stipulated herein,	n/a

	the text set out in Footnote 1 shall be incorporated herein.[1] To the extent that UK Data Protection Laws apply to the Customer's processing: The Information Commissioner	

2. Relevant Information of Customer Affiliates

Customer affiliate	***[complete for each affiliate]*** Name: Address:
Role	**Controller**
Contact person	Name: Position: Contact details:
Where applicable: Data protection officer and/or UK representative	
Where applicable: Data protection officer and/or EU representative	
Activities relevant to the data transferred	

[1] Each supervisory authority of the EU and EEA is competent for the performance of the tasks assigned to and the exercise of the powers on the territory of its own Member State. A list of the supervisory authorities across the European Union and EEA can be found under the following link: https://edpb.europa.eu/about-edpb/about-edpb/members_en

As to Germany, the supervisory authority mentioned under the aforementioned link called "*Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*" is responsible for supervising public authorities of the federal government, public-sector companies, insofar as they participate in the competition, and companies which process data from natural and legal persons in order to commercially provide telecommunication services while the responsibility for supervision does not already come from Section 115 para 4 of the Telecommunication Act ("*Telekommunikationsgesetzes*"). Additionally, there is also a supervisory authority in each federal state ("*Bundesland*") in Germany which is responsible for private entities established in its respective federal state. Please find a list of these German supervisory authorities under the following link: https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html;jsessionid=1D7E492F9E963C3ADC18161A232AADBD.intranet241

Where the data exporter is established in an EU Member State: The competent supervisory authority is the one at the establishment of the data exporter.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR: The competent supervisory authority is the one of the Member State in which the representative is established.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of the GDPR: The competent supervisory authority is the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located.

Competent supervisory authority	To the extent that the EU GDPR applies and the competent supervisory authority is not explicitly stipulated herein, the text set out in Footnote 1 shall be incorporated herein.[1] To the extent that UK Data Protection Laws apply to the Customer Affiliate's processing: The Information Commissioner

Schedule 2

DETAILS OF PROCESSING

1. **Categories of data subjects**

Company will process the categories of data subjects whose personal data Customer directs Company to process in connection with the Services.

2. **Categories of personal data**

Company will process the categories of personal data that Customer directs Company to process in connection with the Services.

3. **Special categories of personal data (if applicable)**

Company will process any special categories of data that Customer directs Company to process in connection with the Services, and implement any additional safeguards with regard this data as are mutually agreed by Customer and Company.

4. **Frequency of the transfer**

The transfers will occur as frequently as is directed by Customer in connection with the Services.

5. **Subject matter of the processing**

The subject matter of the processing is the performance of the Services.

6. **Nature of the processing**

The nature of the processing is the performance of the Services.

7. **Purpose(s) of the data transfer and further processing**

The purpose/s of the data transfer and further processing is the performance of the Services.

8. **Duration**

The period for which the personal data will be retained is as long as is needed for the performance of the Services.

9. **Sub-processor (if applicable)**

For transfers to sub-processors, specify subject matter, nature and duration of the processing is as set out in Schedule 3.

Schedule 3

SUBPROCESSORS

1. Please see https://supabase.com/docs/company/privacy#annex-1 for a full list of data subprocessors.

Schedule 4

TECHNICAL AND ORGANISATIONAL MEASURES

Description of the technical and organisational security measures implemented by the data importer / Company (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons.

1. Pseudonymisation and Encryption, Art. 32 para 1 point a GDPR

Pseudonymisation contains measures that enable one to process personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures. Encryption contains measures that enable one to convert clearly legible information into an illegible string by means of a cryptographic process.

- 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 data is encrypted in transit using TLS with modern ciphersuites.

2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, Art. 32 para 1 point b GDPR

Confidentiality and integrity are ensured by the secure processing of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

2.1 Confidentiality

6.1.1 Physical access control

Measures that prevent unauthorised persons from gaining access to data processing systems with which personal data are processed or used.

- Supabase does not maintain physical systems; it leases compute capacity from dedicated providers on an as-needed basis. Supabase ensures that the providers it works with conform to reasonable and appropriate practices regarding physical security of compute assets.

2.1.2 System/Electronic access control

Measures that prevent data processing systems from being used without authorisation.

- 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.
- All communication-including transmission of credentials-is conducted over connections protected by TLS configured with a set of modern ciphersuites.
- All relevant employees are required to complete general security training (which covers the proper treatment of sensitive data like passwords)
- All employee are also required to install and use a password manager at their workstations
- Audit trails are retained of user actions performed within Supabase infrastructure.
- 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.
- 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.

2.1.3 Internal Access Control

Measures that ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorisation in the course of processing or use and after storage.

- 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.

2.1.4 Isolation/Separation Control

Measures to ensure that data collected for different purposes can be processed (storage, amendment, deletion, transmission) separately.

- 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 projects that contain the Customer's data.

2.1.5 Job Control

Measures that ensure that, in the case of commissioned processing of personal data, the data are processed strictly corresponding the instructions of the principal.

- Supabase offers a platform that allows Customer to execute processing instructions by interfacing with it directly; Supabase is not involved as an intermediary in said execution. As such, the data is processed as instructed by Customer.

2.2. Integrity

2.2.1 Data transmission control

Measures ensure that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged.

- 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.

- 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 our firewalls.

2.2.2 Data input control

Measures that ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed.

- Supabase retains audit logs of all interactions with its internal services.

- Supabase retains audit logs of all interactions with Customer projects.

2.3 Availability and Resilience of Processing Systems and Services

Availability includes measures that ensure that personal data is protected from accidental destruction or loss due to internal or external influences. Resilience of processing systems and services includes measures that ensure the ability to withstand attacks or to quickly restore systems to working order after an attack.

- 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.

3. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, Art. 32 para 1 point c GDPR

Organisational measures that ensure the possibility to quickly restore the system or data in the event of a physical or technical incident.

- 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 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.

4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing, Art. 32 para 1 point d GDPR

Organisational measures that ensure the regular review and assessment of technical and organisational measures.

- 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.

5. Additional technical and organisational measures

The following additional technical and organisational measures will be implemented:

- Supabase is currently working towards SOC2 compliance, a comprehensive certification that evaluates the measures it has in place for data confidentiality, integrity, and privacy. Additionally, the relevant controls are monitored for on an on-going basis, and alerts are triggered if they're ever not in compliance.
- Supabase offers secure access to Customer data via multiple industry standard mechanisms, ensuring data portability.

- Supabase offers automated deletion of all project resources, ensuring that all relevant data is erased in an automated fashion.

6. Description of the specific technical and organisational measures to be taken by the to assist with the fulfilment of data subject requests (clause 10 (b) SCC)

In order to for the data importer / Company to assist the data exporter / Customer with fulfilling its obligations to respond to data subjects' requests in accordance with clause 10 (b) SCC, the Parties will set out the appropriate technical and organisational measures in the following, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required:

- Supabase maintains a checklist of automated and manual processes that need to be undertaken to fulfil data subject requests. Additionally, Supabase is working on completely automating any remaining relevant manual processes for additional efficiency and convenience.