TRANSFER IMPACT ASSESSMENT ("TIA")

FOR INTERNATIONAL DATA TRANSFERS TO SUPABASE, INC

OVERVIEW		
Date		23 January 2024
Name and address of Data Importer		Supabase Inc 6701 Koll Center Parkway Suite 250, Pleasanton, CA 94566-8062 ("**Supabase**")
Brief description of transfer and subsequent processing		The Data Exporter shares personal data for purposes including the provision of the services under the corresponding agreement between Supabase and Data Exporter, namely: ● provision of hosting services for the Data Exporter's applications and software services; and ● to enable the Data Exporter's authorized users (employees, consultants, contractors and agents) to access and manage hosted databases.
Data privacy role of the Data Importer regarding the data processing		Processor Controller
Utilized legal mechanism for the international transfer from the Data Exporter to the Data Importer		Module Two (*controller to processor*) of the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914
Note: *If the processing contains several different processing activities: Please outline where answers to the following questions may differ in relation to the respective processing activities.*		
A. SYSTEMATIC DESCRIPTION OF THE DATA PROCESSING		
Specific circumstances of the processing		Supabase provides database and tooling services for the development and operation of web and mobile applications (the "**Services**").
Purpose/s of the data processing	***1***	Provision of the Services, including data hosting and authentication.
	2	Provision of access to the Services to authorized users of the Data Exporter
	3	IT and customer support
	4	Analytics and improvement of the Services
Functional/technical description of the data processing		Supabase hosts data in dedicated PostgreSQL databases for each project managed by the Data Exporter through the Services. Each database is hosted in Amazon Web Services. Logs are hosted in BigQuery (Google Cloud) and real time processing is run through fly.io. Personal data collected about authorized users is stored in AuthO, Hubspot, Intercom, Notion, Slack, AWS and BigQuery.
Categories of personal data being processed		**Data hosted for Data Exporter in connection with the Services** ● **User authentication data** relating to the Data Exporter's web or mobile applications. ● Any other categories of personal data uploaded by the Data Exporter in connection with the development and operation of its web or mobile applications.

		Data relating to authorized users: ● **Contact information**, first name, last name, email address. ● **Usage information**, such as users' IP addresses from which they access the platform ● **Registration/account information**, name, email address, password. ● **Payment transaction information,** billing address, date and time of transactions. ● **Approximate location information,** ● **Chat, comments, opinions and questions,** comments and opinions via email. ● **Information from third-party social media sites,** name, profile information and any other information permitted by the user to be shared. ● **Preferences,** set for notifications, marketing communications and display and active functionalities of the proprietary hosted software platform.	
Sector in which processing occurs		Database hosting services, software development, mobile application development.	
Format of the data to be transferred		All data is encrypted in transit using TLS 1.2 with modern ciphersuites. Data (including backups) is encrypted at rest using industry-standard AES-256 algorithms. Encryption keys are generated per project and are in turn protected by keys stored using FIPS 140-2 compliant HSMs.	
The recipients of the personal data	**(In case of intragroup data flows) List the names, addresses and types** *(i.e., public/private; controller/ processor/ sub-processor)* **of the affiliates of the Data Importer involved in the processing**[7]	**Supabase Pte. Ltd** 65 CHULIA STREET, #38-02/03, OCBC CENTRE, Singapore 049513	Controller Subprocessor
	List the names, addresses and types (i.e., *public/private; controller/ processor/ sub-processor)* **of all (other) entities involved in the processing**[7]	**Amazon Web Services, Inc** 410 Terry Avenue North, Seattle, WA 98109-5210	Subprocessor Processor
		Google, LLC 1600 Amphitheatre Parkway Mountain View, CA 94043	Subprocessor Processor
		Fly.io, Inc 321 N Clark St, Chicago, Illinois	Subprocessor Processor
		Hubspot, Inc 25 First Street, 2nd Floor Cambridge, MA 02141 United States	Subprocessor
		Notion Labs, Inc 548 Market St Suite 74567 San Francisco, CA 94104	Subprocessor
		Slack Technologies, LLC 500 Howard Street San Francisco, CA 94105	Subprocessor
		Functional Software, Inc d/b/a Sentry	Subprocessor Processor

		45 Fremont Street, 8th Floor, San Francisco, CA 94105.	
		Upstash, Inc 1148 Holly Ann Pl, San Jose, CA 95120	Subprocessor
		Stripe, Inc. 354 Oyster Point Blvd South San Francisco, CA 94080 United States	Processor
		AC PM, LLC d/b/a Postmark N Dearborn Street, Suite 500, Chicago, IL 60602	Processor Subprocessor
		Twilio, Inc. 101 Spear St 5th Floor San Francisco, California 94105, United States	Subprocessor
		PandaDoc, Inc. 3739 Balboa St. #1083 San Francisco, CA 94121	Processor
		Github, Inc 88 Colin P. Kelly Jr. Street, San Francisco, California 94107 United States	Subprocessor
		Sequin Labs, Inc. 212 4th Avenue Venice CA 90291, United States	Subprocessor
		Tableau Software, LLC NorthEdge 1621 N 34th St. Seattle, WA 98103	Subprocessor
		Open AI, LLC 3180 18th St., San Francisco, California 94110	Subprocessor
		Common Room, Inc. 83 S King St Fl 8 Seattle 98104-3852 WA United States	Processor
		Mixpanel, Inc One Front Street, 28th Floor, San Francisco, CA 94111	Processor
		PLAUSIBLE INSIGHTS OÜ Tartu maakond, Tartu linn, Tartu linn, Västriku tn 2, 50403	Processor
		Vercel, Inc. 440 N Barranca Ave #4133 Covina, CA 91723	Subprocessor
		Cloudflare, Inc. 101 Townsend St, San Francisco, CA 94107	Subprocessor Processor
		ConfigCat Korlátolt Felelősségű Társaság 1136 Budapest, Tátra utca 5/A 1. em. 2. ajtó, Hungary	Subprocessor
Countries to which the personal data may be transferred		United States of America Singapore	
Could the personal data be subject to onward transfers (from the third country to the same or another third country)?		Yes, onward transfers to subprocessors in the US and Singapore	
B. REGULATORY FRAMEWORK – U.S.			

Foreign Intelligence Surveillance Act, Sec. 702 ("FISA 702")	Schrems II Judgment In the *Schrems II* decision, the CJEU determined that FISA 702 does not comply with the minimum safeguards under EU law (please see the judgment for specifics as to the shortcomings of FISA 702). The following risk analysis thus focusses on the application of FISA 702 to Supabase's and the Data Exporter's activities. General applicability of FISA 702 to the Data Importer and Sub-Processor(s) The term *"electronic communications service providers"* potentially subject to FISA 702 has been interpreted broadly by U.S. courts and the U.S. Department of Commerce to include companies such as Supabase. Based on recent guidance from the Department of Commerce, however, it seems rather remote to consider that U.S. intelligence agencies would seek to collect the ordinary commercial information Supabase processes on behalf of its customers and partners and their employees. Additionally, as the U.S. government has applied FISA 702, Supabase is not eligible to receive the type of order that was of principal concern to the CJEU in the *Schrems II* decision—i.e., a FISA 702 order for *"upstream"* surveillance. As the U.S. government has applied FISA 702, it uses upstream orders solely to target traffic flowing through internet backbone providers that carry Internet traffic for third parties (i.e., Google, Yahoo). Supabase does not provide such Internet backbone services. As a result, it is unlikely that Supabase would receive the type of order principally addressed in the *Schrems II* decision. Additionally, the U.S. Department of Commerce in September 2020 issued a white paper on *Schrems II*. According to this paper, "*Companies whose EU operations involve ordinary commercial products or services, and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence agencies would seek to collect that data*." We therefore believe it is unlikely U.S. intelligence agencies would seek to collect the ordinary commercial information Supabase processes in the course of providing its services. As of the date of this statement, Supabase has not been subject to a U.S. government request pursuant to FISA 702. In respect of Supabase's data processing that occurs in the cloud, Supabase uses AWS, Google, Fly.io and other processors and subprocessors who may be subject to FISA 702 as they constitute *"electronic communication service providers*". The term *"electronic communication service provider*" *inter alia* covers *a "provider of a remote computing service"* as defined in 18 U.S.C. § 2711 which *"prov[ides] to the public […] computer storage or processing services by means of an electronic communication system."* Certain conditions may be set for the utilization of such a service, which may include the charging of a fee. As providers of remote computer storage and processing services by means of an electronic communication system, certain processors and subprocessors of Supabase may constitute *"providers of a remote computing service".* While we believe that Supabase data is not the sort typically sought by U.S. intelligence agencies, the relevant subprocessors have

	implemented additional safeguards to mitigate the risk of access to personal data by U.S. intelligence agencies, as set forth further below in this assessment. On 10 July 2023, the European Commission adopted an adequacy decision in respect of the EU-U.S. Data Privacy Framework. An essential element of the US legal framework on which the adequacy decision is based is Executive Order 14086 and accompanying regulations adopted by the US Attorney General. These instruments were adopted to address the issues raised by the CJEU in the Schrems II judgment, namely: ● Binding safeguards that limit access to data by US intelligence authorities to what is necessary and proportionate to protect national security; ● Enhanced oversight of activities by US intelligence services to ensure compliance with limitations on surveillance activities; and ● The establishment of an independent and impartial redress mechanism, which includes a new Data Protection Review Court to investigate and resolve complaints regarding access to European data subjects' data by US national security authorities. These safeguards apply to all data transfers under the GDPR to companies in the US, regardless of the transfer mechanism used. The recognition of the above safeguards by the European Commission as addressing the issues raised in the Schrems II judgment indicates that US recipients of personal data such as Supabase are able to provide an essentially equivalent level of protection for personal data regardless of the application of FISA 702. This position was mirrored in the UK following the adoption of the UK GDPR extension to the EU-U.S. Data Privacy Framework. The UK Secretary of State designated the US as an adequate jurisdiction for the purposes of the UK GDPR on 21 September 2023, following the US designation of the UK as a "qualifying state" for the purposes of EO 14086 on 18 September 2023. This designation applied the above safeguards to all data transfers under the UK GDPR to companies in the US, regardless of the transfer mechanism used.

Executive Order 12333 & Presidential Policy Directive 28	Schrems II Judgment In the *Schrems II* decision, the CJEU determined that EO 12333, read in conjunction with PPD-28, does not comply with the minimum safeguards under EU law (please see the judgment for specifics as to its shortcomings). General applicability of EO 12333[1] to the Data Importer and Sub-Processor(s) The U.S. Department of Commerce, the U.S. Department of Justice, and the Office of the Director of National Intelligence have emphasized that "*unlike FISA 702, however, EO 12333 does not authorize the U.S. government to require any company or person to disclose data*."[2] Furthermore, the U.S. Department of Commerce, the U.S. Department of Justice, and the Office of the Director of National Intelligence state that "[b]*ulk data collection is permitted only in other contexts, such as clandestine intelligence activities involving overseas access to data – activities in which companies cannot legally be compelled to participat*e."[3] Based on these statements, access to the personal data at issue by an U.S. intelligence agency based on EO 12333 only seems possible if (i) the Data Importer or Sub-Processor(s) voluntarily decides to allow such access or (ii) the intelligence agency is able to access the personal data by itself without the cooperation and knowledge of the Data Importer or Sub-Processor(s). Given Supabase's processing activities, we view these restrictions as additional safeguards to further minimize the likelihood that customer or partner data would be subject to indiscriminate or unlawful search or seizure. As of the date of this statement, Supabase has not received any U.S. government request pursuant to EO 12333 for such data. In the event of an order from U.S. law enforcement, Supabase will carefully review any requests for information to ensure full compliance with applicable law. Any request from the U.S. government would be reviewed by the Supabase Legal team, to determine the appropriate response. It is Supabase's general practice to alert customers and partners of any governmental request prior to sharing their information. Additionally, Supabase has implemented a multitude of strong safeguards as set forth in further detail below. Executive Order 14086 As discussed above, the European Commission's (and UK government's) view is that the measures adopted under EO 14086 have addressed the issues raised in the Schrems II judgment with respect to EO 12333.

[1] Executive Order 12333, available under https://www.archives.gov/federal-register/codification/executive-order/12333.html (lastly checked on 12 November 2021) ("**EO 12333**").

[2] U.S. Department of Commerce, U.S. Department of Justice, and the Office of the Director of National Intelligence, Information on U.S. Privacy Safeguards Relevant to
SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II -White Paper Paper, September 2020, available under https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF (lastly checked on 28 November 2021) ("**Common White Paper**"), p 16.

[3] Common White Paper, p 17.

Is there any other reason why your entity may not be able to comply with its obligations under the utilized mechanism for the international transfer and, if so, specify this/these obligation/s and reason/s	Whilst the global regulatory landscape is constantly evolving, Supabase is committed to ensuring its customers and partners can continue to use its services and comply with the GDPR. Specifically, Supabase commits to complying with the instructions of its customers and partners when it enters into its DPAs and SCCs. In addition, and as required by the DPAs and SCCs Supabase enters into with its customers and partners, Supabase will promptly notify its customers and partners in the event of a change in applicable legislation that has a substantial adverse effect on the warranties and obligations that Supabase committed to when it enters into those DPAs and SCCs.
Please outline relevant aspects of the legal system in the applicable jurisdiction as regards to the processing at hand, in particular, in light of the elements listed in Art 45 para 2 GDPR	The U.S. follows the principle of the rule of law and has ratified various conventions on the protection of human rights.[4] The U.S. generally provides for legal redress and independent oversight over state actions. However, in relation to certain governmental access to personal data, legal redress and independent oversight is limited. Regarding FISA 702 and EO 12333, the following applies: <u>FISA 702</u> FISA 702 includes certain requirements for judicial oversight which is performed by the *Foreign Intelligence Surveillance Court*. Individual redress is also available for violations under FISA 702 for data subjects at hand should individuals become aware of access to their personal data.[5] Individuals can challenge unlawful electronic surveillance, which includes the possibility of bringing a civil cause of action for compensatory damages against the U.S., to sue U.S. government officials in their personal capacity for compensatory and punitive damages, and to challenge the legality of surveillance.[6] Additionally, Data Importer has the right to sue or file an injunction against an unlawful FISA 702 order including against a gag order (if applicable). <u>EO 12333</u> As outlined below in detail, surveillance under EO 12333 is subject to the restrictions set forth in PPD 28, which are intended to protect the privacy and civil liberties of all persons regardless of their nationality and place of residence. <u>Certain Information may not have been considered in the *Schrems II* Judgment</u> It should be noted that the U.S. Department of Commerce believes that, in the *Schrems II* Judgment, the CJEU did not take all available information into account. In particular, it missed assessing the safeguards applicable under U.S. law to EU data subjects as well as developments that occurred after 2016 according to the U.S. Department of Commerce.[7] <u>EO 14086</u> For data subjects in “qualifying states” (including the EU and UK), EO 14086 establishes a new two-layer redress

[4] See overview of the status of ratifications published by the United Nations Office of the High Commissioner for the Protection of Human Rights, available under https://www.ohchr.org/EN/countries/LACRegion/Pages/USIndex.aspx (lastly checked on 2 December 2021).

[5] Common White Paper, p 12 and 13.

[6] 5 U.S.C. § 702 (2018); 18 U.S.C. § 2712 (2018); 50 U.S.C. § 1810; Common White Paper, p 12 and 13.

[7] Common White Paper, p 6.

	mechanism, with independent and binding authority, to handle and resolve complaints about the collection and use of data by US intelligence agencies. For complaints to be admissible, individuals do not need to demonstrate that their data was in fact collected by US intelligence agencies. Individuals can submit a complaint to their national data protection authority, which will ensure that the complaint will be properly transmitted and that any further information relating to the procedure, including on the outcome, is provided to the individual.
Please outline (i) whether a comprehensive data protection law exists in your jurisdiction and/or (ii) any existing safeguards offered by local data privacy laws in relation to the data subjects of the processing at hand	The U.S. does not have a comprehensive federal data protection law similar to the GDPR. However, various U.S. laws offer protections of personal data similar to some of the protections offered by the GDPR, including: - The California Consumer Privacy Act (CCPA), as amended; - The Virginia Consumer Data Protection Act (VCDPA); - The Colorado Privacy Act (CPA); - Section 5 of the Federal Trade Commission Act and its state law equivalents in all 50 states; and - State laws requiring the notification of a data breach. These laws may not generally apply to the data subjects at hand. However, as companies usually structure their IT systems and data processing operations based on legal requirements applicable to them, data subjects at hand can also benefit from the existence of these laws.
Does an independent regulator and/or supervisory / data protection authority exist in the applicable jurisdiction and, if so, please describe its role as to the processing at hand (*in particular, as to whether it can support the data subject in case of a violation of its privacy rights and especially in case of any accessing of its personal data by a public authority*).	On a federal level, the Federal Trade Commission ("**FTC**") is tasked with enforcing promises made by companies to consumers in relation to the handling of their personal information.[8] As of the date of execution of this TIA, the FTC has brought numerous legal actions against companies based on alleged violations of consumers' privacy rights[9] and has imposed fines of up to US$ 5 billion.[10] The FTC is generally not competent to support individuals with the enforcement of their rights against an intelligence agency in the U.S. However, the enforcement authority and actions of the FTC in the data privacy field have made U.S. companies take data privacy more seriously and invest in the implementation of privacy safeguards as to its organizations and IT systems which the data subjects can also benefit from. In addition, state regulators, including for example, the California Attorney General, also oversee consumer privacy rights and regularly issue penalties for violation of state laws applicable to personal information.
Please describe the (i) application (or lack thereof) of the laws and practices outlined above <u>in practice</u> and (ii), in particular, the experience of actors operating within the same sector *(e.g., financial, telecommunication)* **as your entity**	<u>Risk of utilization of FISA 702 by an intelligence agency in the U.S. against the Data Importer and Sub-Processor(s)</u> The U.S. Department of Commerce, the U.S. Department of Justice, and the Office of the Director of National Intelligence stated in 2020: "*Companies whose EU operations involve ordinary commercial products or services, and whose EU-U.S.*

[8] FTC, Privacy and Security Enforcement, available under https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (lastly checked on 12 November 2021) ("**FTC, Privacy and Security Enforcement**")

[9] FTC, Privacy and Security Enforcement.

[10] FTC, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, available under https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions (lastly checked on 12 November 2021).

with requests for access and/or disclosure (related to similar transferred personal data) *(in particular, the frequency of such requests and its reasons and scope).*[11]	*transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence agencies would seek to collect that data*. *Indeed, the overwhelming majority of companies have never received orders to disclose data under FISA 702 and have never otherwise provided personal data to U.S. intelligence agencies.*"[12] Furthermore, the language of 50 U.S.C. § 1881a(a) provides that FISA 702 may solely be utilized by an U.S. intelligence agency as to non-US citizens and residents "*reasonably believed to be located outside the United States*" for obtaining "*foreign intelligence information*"[13], whereas according to 50 U.S.C. § 1881a(h)(2)(A)(v) a certification submitted to the *Foreign Intelligence Surveillance Court* for an authorization "*shall attest that a significant purpose of the acquisition is to obtain foreign intelligence information*". <u>Risk of utilization of EO 12333 by an intelligence agency in the U.S. against the Data Importer and Sub-Processor(s)</u> As outlined above, based on statements from the U.S. Department of Commerce, access to personal data by a U.S. intelligence agency based on EO 12333 only seems possible if (i) the Data Importer or Sub-Processor(s) voluntarily decides to allow such accessing or (ii) an intelligence agency is able to access the personal data by itself without the cooperation and knowledge of the Data Importer or Sub-Processor(s).[14] Furthermore, the main focus of EO 12333 is the authorization of certain surveillance activities by U.S. intelligence agencies outside the U.S.[15] Additionally, the likelihood of a U.S. intelligence agency being able to access the personal data without the cooperation of the Data Importer or Sub-Processor is reduced because the personal is encrypted in transit. Although a U.S. intelligence agency could decrypt the data, the encryption would make the access to the data more difficult for such agencies which might prompt them to seek alternative means to gather the information. <u>Restrictions based on PPD 28</u>

[11] Clause 14(b)(ii) and Footnote 12 SCC (all modules); EDPB, cf Rec 01/2020, v 2.0, p 15, rec 33; p 17, 18, rec 43, 43.1; p 19 rec 47.

[12] Common White Paper, p 2.

[13] 50 U.S.C. §1801a (e): *"Foreign intelligence information" means*

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against
(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to
(A) the national defense or the security of the United States; or
(B) the conduct of the foreign affairs of the United States.

[14] Common White Paper, p. 16 and 17.

[15] EO 12333, Part 2.2 *Purpose*.

	In addition, surveillance under EO 12333 is subject to the restrictions set forth in the PPD 28[16], which are intended to protect the privacy and civil liberties of all persons regardless of their nationality and place of residence; these restrictions include: ● "*In particular, when the United States collects nonpublicly available signals intelligence in bulk, it shall use that data only for the purposes of detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.*"[17] ● A requirement for the U.S. Intelligence Community to "*establish policies and procedures reasonably designed to minimize the dissemination and retention of personal information collected from signals intelligence activities*", whereas limitations as to the dissemination and retention of personal information of U.S. persons are extended to non-U.S. persons.[18] In light of Supabase's and the Data Exporter's processing activities and the categories of personal data at hand, we view these restrictions as additional safeguards to further minimize the likelihood of access by an intelligence agency in the U.S. Per EO 12333, Agencies of the U.S. Intelligence Community are also required to "*use the least intrusive collection techniques feasible within the United States […]*".[19] Such agencies "*are not authorized to use such techniques as electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes.*"[20] This limitation under EO 12333 also arguably reduces the likelihood of access to the personal data at issue by a U.S. intelligence agency during its processing in the U.S. by the Data Importer and Sub-Processor(s). <u>Additional redress mechanisms under EO 14086</u> As described above, EO 14086 establishes restrictions on access by US intelligence authorities to data relating to data

[16] Presidential Policy Directive 28, Subject: Signals Intelligence Agencies, available under https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (lastly checked on 12 November 2021) ("**PPD 28**").

[17] PPD 28, Section 2.

[18] PPD 28, Section 4(a)i.

[19] EO 12333, Part 2.4 *Collection Techniques*.

[20] EO 12333, Part 2.4 *Collection Techniques*.

	subjects in "qualifying states" (including the EU and UK), together with enhanced oversight and an impartial redress mechanism.
Please provide the sources[21] on which your answers in this Section B. are based.	The analysis under Section B was drafted by U.S. legal counsel based on knowledge of the U.S. legal system with support from experienced EU privacy counsel. U.S. counsel has partially relied on documents and information (i) released by U.S. government entities, (ii) leaked by Edward Snowden and/or (iii) released by a non-governmental organization (NGO).
B. REGULATORY FRAMEWORK – Singapore	
Criminal Procedure Code ("CPC")	The CPC gives authorities broad powers to seize, access and decrypt data in connection with criminal investigations.
Telecommunications Act ("TA")	Infocomm Media Development Authority ("**IMDA**") has the power under the TA to require any person to produce any document or information which the IMDA considers to be related to any matter relevant to an investigation or for discharging its functions under the TA.
Official Secrets Act ("OSA")	The OSA grants certain authorities the right to require (by warrant) the owner or controller of any telecommunication system used for sending or receiving messages to or from any place out of Singapore to produce such messages, if production is expedient and in the public interest.
Prevention of Corruption Act ("PCA")	The Director of the Corrupt Practices Investigation Bureau or any Magistrate, by warrant directed to any special investigator or police officer, may enter on premises and seize and detain any document or property, where there is reasonable cause to believe that it relates to the commission of a relevant offence.
Foreign Interference (Countermeasures) Act ("FICA")	Once in force, FICA will empower the competent authority to obtain information from organisations (which may potentially include personal information) regarding online communications activities that have been undertaken, or suspected of being or having been undertaken, by or on behalf of a foreign principal.
Please outline relevant aspects of the legal system in the applicable jurisdiction as regards to the processing at hand, in particular, in light of the elements listed in Art 45 para 2 GDPR	<u>Rule of law</u> The principle of the rule of law in Singapore is recognised and provided for in Singapore's legal system. <u>Rights</u> Part IV of the Constitution protects certain fundamental liberties (e.g. the right to life and personal liberty; equal protection of the law; freedom of speech, assembly and association; freedom of religion), and there is a broad framework of common law and statutory torts in Singapore, which indirectly protect privacy-related interests (e.g. nuisance, trespass to the person, defamation, and law of confidence). <u>Data protection rights</u> The primary data protection legislation is the Personal Data Protection Act (No. 26 of 2012) ("**PDPA**"), which sets out a

[21] The sources shall be relevant, objective, reliable, verifiable, and publicly available or otherwise accessible, *e.g., case-law; reports from (i) independent oversight or parliamentary bodies, (ii) trade associations, (iii) academic institutions, (iv) NGOs, (v) intergovernmental organization, (vi) private providers of business intelligence; Internal statements or records of the importer expressly indicating that no access requests were received for a sufficiently long period; and with a preference for statements and records engaging the liability of the importer and/or issued by internal positions with some autonomy such as internal auditors, DPOs*. Please see EDPB, Rec 01/2020, v 2.0, p 18/19 and Annex 3; cf Clause 14(b)(ii), Footnote 12 SCC (all modules).

	baseline standard of protection for personal data across organisations. The PDPA operates concurrently with other sector-specific regulations and other laws. The PDPA provides individuals with specific rights with regard to the processing of their personal data. <u>International commitments</u> Singapore has entered into the APEC Privacy Framework, which was developed in light of the 1980 Organisation for Economic Co-operation and Development ("**OECD**") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and applies to all APEC member economies. The APEC Privacy Framework sets out principles and implementation guidance for public and private sectors which control the collection, holding, processing, use, transfer, or disclosure of personal information.
Please outline (i) whether a comprehensive data protection law exists in your jurisdiction and/or (ii) any existing safeguards offered by local data privacy laws in relation to the data subjects of the processing at hand	The PDPA governs the processing of personal data in Singapore, alongside sector-specific legislation. While the PDPA does not apply to public agencies, these agencies will be familiar with the requirements and restrictions in the PDPA relating to the disclosure of data. The Public Sector (Governance) Act 2018 (2020 Revised Edition) ("**PSA**") also sets out directions regarding data sharing in the public sector and imposes criminal penalties on public officers who recklessly or intentionally disclose data (which may include personal data) without authorisation, misuse data for a gain or re-identify anonymised data.
Does an independent regulator and/or supervisory / data protection authority exist in the applicable jurisdiction and, if so, please describe its role as to the processing at hand (*in particular, as to whether it can support the data subject in case of a violation of its privacy rights and especially in case of any accessing of its personal data by a public authority*).	The relevant supervisory authority for administering and enforcing the PDPA is the Personal Data Protection Commission ("**PDPC**"). Individuals may lodge a complaint to the PDPC in respect of a contravention of the data protection provisions by an organisation. The PDPC has a broad range of enforcement powers, including issuing penalties. The PDPA (and the PDPC's oversight role) does not apply to public authorities; however public agencies are governed by their own separate set of laws and internal standards with regard to the protection of personal data and the preservation of confidentiality.
Please describe the (i) application (or lack thereof) of the laws and practices outlined above in practice and (ii), in particular, the experience of actors operating within the same sector as your entity with requests for access and/or disclosure (in particular, the frequency of such requests and its reasons and scope).	The above laws apply in relation to specific investigations carried out by public authorities, rather than a general right to access personal data. A number of oversight mechanisms are also in place in relation to the application of the above laws granting access to personal data to public authorities. Depending on the specific laws in question, these oversight mechanisms may include: ● the requirement for authorised officers to obtain court orders prior to requesting the production of material related to an investigation; ● avenues of appeal to the relevant Minister or designated appeal panel; and ● judicial review by the courts of administrative action or determinations by public bodies.

Please provide the sources on which your answers in this Section B. are based.	Desktop review of applicable law by EU privacy counsel.
C. REQUESTS FOR ACCESS / DISCLOSURE	
Please outline whether your entity has been subject to requests from public authorities for the access to or disclosure of personal data and, if so, please outline the number and frequency of cases and provide information on these cases.[22]	As of the date of this statement, Supabase has not disclosed customer or partner personal data pursuant to requests made by law enforcement agencies or government bodies, including under FISA 702 or EO 12333.
Please outline whether your entity regularly issues transparency reports which include information on request for access or disclosure by public authorities.	No.
D. MITIGATING MEASURES	
Please specify the implemented safeguards to mitigate the risk of access <u>during transit</u> (e.g., between data centers; from and to Data Exporter) of the personal data.[23]	● 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.
Please specify any relevant contractual, technical and/or organizational safeguards put in place to supplement the safeguards of the aforementioned mechanism for the international data transfer *(e.g., SCC)* **in order to avoid access from a public authority when the personal data is <u>at rest</u>** (in the third country[1] of destination).[24]	Supabase implements the following protocol in place for government requests: ● Supabase takes its obligations under all applicable data protection laws seriously and is committed to safeguarding customer and partner information. There is no reason to expect that FISA 702 will change the way Supabase has previously interacted with the U.S. government. ● In the event of an order from U.S. law enforcement, Supabase will carefully review any requests for information to ensure full compliance with applicable law. Any request from the U.S. government, including those that would potentially implicate FISA 702, would be reviewed by the Supabase Legal team, to determine the appropriate response. ● Where compliance with a valid request for customer or partner data would put Supabase in potential breach of applicable data protection or privacy laws, Supabase reserves the right to challenge such request in accordance with FISA 702 and other applicable laws, and to notify affected customers and partners. ● Finally, it is Supabase's general practice to notify customers and partners of any governmental request prior to sharing their information. Notwithstanding the above points regarding the legal restrictions on the use of FISA 702 requests and judicial recourse under Executive Order 14086, the following subprocessors and processors of Supabase that are likely, or view themselves as

[22] Clause 14(b)(ii) and Footnote 12 SCC (all modules), EDPB, Rec 01/2020, v 2.0, p 19, rec 47.

[23] Clause 14(b)(iii) SCC (all modules).

[24] Clause 14(b)(iii) SCC (all modules).

potential targets of requests under FISA 702 have either certified to the EU-U.S. Data Privacy Framework and/or assessed their exposure and, where appropriate, implemented additional safeguards:

Amazon Web Services	Certification to the EU-U.S. Data Privacy Framework and UK Extension. https://aws.amazon.com/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data/
Google, LLC	Certification to the EU-U.S. Data Privacy Framework and UK Extension. https://services.google.com/fh/files/misc/safeguards_for_international_data_transfers_with_google_cloud.pdf
Fly.io, Inc	https://fly.io/docs/reference/secrets/
Hubspot, Inc	Certification to the EU-U.S. Data Privacy Framework and UK Extension. https://legal.hubspot.com/security
Notion Labs, Inc	https://www.notion.so/Transfer-Impact-Assessment-Information-77d5463434bb4c9eb80371bb56c0f2c1
Slack Technologies, LLC	https://a.slack-edge.com/df18e75/marketing/downloads/compliance/22SLA0237-Transfer-Impact-Assessment-White-Paper-MC-FIN.pdf
Functional Software, Inc d/b/a Sentry	Certification to the EU-U.S. Data Privacy Framework and UK Extension. https://sentry.io/legal/dpa/
Upstash, Inc	Third party encryption key management
Stripe, Inc.	Certification to the EU-U.S. Data Privacy Framework and UK Extension. https://stripe.com/gb/legal/privacy-center#international-data-transfers

	AC PM LLC	Certification to the EU-U.S. Data Privacy Framework and UK Extension.
	Twilio, Inc	Certification to the EU-U.S. Data Privacy Framework and UK Extension. https://help.twilio.com/articles/360051805394-Measures-Twilio-Takes-to-Safeguard-the-Privacy-of-Customer-Personal-Data
	Github, Inc.	https://github.com/customer-terms/github-data-protection-agreement
	Salesforce, Inc (parent company of Tableau Software, LLC)	Certification to the EU-U.S. Data Privacy Framework and UK Extension. https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/SFDC-Online-Transfer-Risk-Assessment-Whitepaper-for-Customers-(Salesforce-Services)-february-2022.pdf
	Cloudflare, Inc.	Certification to the EU-U.S. Data Privacy Framework and UK Extension. https://www.cloudflare.com/trust-hub/gdpr/

I hereby declare that I am a duly authorized representative of the Data Importer and that the foregoing responses in the completed TIA Questionnaire set out above are true and correct.

Name of Signee	
Position of Signee	
Date of Signature	
Signature	