DATA PROCESSING AGREEMENT

GATHERED

On the one hand, the Client, in its capacity as Data Controller (hereinafter, the "Client" or the "Data Controller").

On the other hand, OneVisa Technologies, Ltd., with Tax ID 105365389300001, registered address at IH-00-01-03-OF-05, Level 3, Innovation One building, Dubai International Financial Centre, represented by Mr. Alexis Roque and Mr. Alberto Carlos Alcaraz Moreno, acting in their capacity as Directors (hereinafter, the "Platform" or the "Data Processor").

All parties shall be referred to jointly and severally as the "Parties," and individually as the "Party."

The Parties, in their capacity as such, warrant that they have the necessary legal capacity to be bound by the terms of this agreement and, by virtue thereof,

DECLARE

I. That the term "Client" refers to a legal entity named as a Client in the service agreement signed by ONEVISA and the Client (the "Service Agreement") that is incorporated into and forms an integral part of the Terms and Conditions, which have been accepted by the Client.
II. That, in order to execute the Service Agreement and be able to provide the services, the Platform will process personal data on behalf of the Client.
III. That by virtue of the foregoing, the Parties wish to regulate such processing in accordance with the GDPR and, consequently, agree to enter into this data processing agreement (the "Agreement") in accordance with the following

CLAUSES

1. Purpose and scope

1.1. This Agreement regulates the processing of personal data that the Platform will carry out on behalf of the Client exclusively to provide the services described in the Service Agreement and in this document.
1.2. The Client acts as the Data Controller and the Platform as the Data Processor with respect to such processing.
1.3. Any processing for the Platform's own purposes is outside the scope of this Agreement and shall be governed by its own legal basis and information documentation.

2. Prevalence and interpretation

2.1. This Agreement forms part of the Service Agreement.

2.2. In the event of any contradiction, this document shall prevail only in matters of data protection; in all other matters, the Service Agreement shall prevail.

2.3. If any of the provisions of this Agreement is declared null and void or inapplicable, the clause in question shall be excluded from the Agreement, without this implying the nullity of the remaining clauses of the Agreement. In the event of the nullity of any of the provisions, the parties shall make every effort to replace the clause or provision declared null and void with an equivalent one that is legally valid.

3. Instructions from the Data Controller

3.1. The Platform shall process the data in accordance with the Client's documented instructions.

3.2. The instructions must be lawful, reasonable, technically feasible, and consistent with the scope of the contracted Service.

3.3. If an instruction involves unforeseen additional costs, developments, or operational burdens, the Parties shall agree in advance on its scope, deadline, and economic impact.

3.4. The Platform may reject instructions that are manifestly contrary to applicable regulations or the Service Agreement, informing the Client thereof.

4. Obligations of the Platform

4.1. The Platform and all its personnel under its authority, if any, whether employees or collaborators, undertake to:

a) process data solely for the purpose of providing the Service and fulfilling the purposes set out in the Service Agreement, as well as the documented instructions received from the Client;

b) guarantee the confidentiality of authorized personnel;

c) apply appropriate technical and organizational measures in accordance with Article 32 of the GDPR and the state of the art;

d) reasonably assist the Client in requests for regulatory rights and obligations, to the extent that this is proportionate and based on the information available;

e) Notify the Client, without undue delay and within a maximum period of forty-eight (48) hours from becoming aware of it, of any security breaches of the personal data it processes under this Agreement, including all information available to it at that time in relation to such breach;

f) Make available to the Data Controller all information necessary to demonstrate compliance with its obligations, as well as for the performance of audits or inspections carried out by the controller or another auditor authorized by it;

g) Maintain an internal record of categories of processing activities where legally required, containing:

   i) the name and contact details of the processor or processors and of each controller on whose behalf the processor acts.
   ii) the categories of processing carried out on behalf of each controller.
   iii) a general description of the appropriate technical and organizational security measures being applied.

h) At the Client's discretion, delete or return all personal data once the processing services have been provided, and delete any existing copies to unless the retention of personal data is required under Union or Member State law;

5. Obligations of the Client

5.1. Without prejudice to its obligations under applicable personal data protection legislation, the Client guarantees and undertakes to:

a) that it has a valid legal basis for communicating data to the Platform and for instructing the processing;
b) adopt and implement the necessary measures to provide data subjects with information on the processing of their personal data, in accordance with the principles of information and transparency
c) that the instructions do not infringe regulations or the rights of third parties;
d) hold the data processor harmless from any liability that may be imposed on it by a competent authority or third party by virtue of administrative or judicial proceedings, including the right to compensation that may be claimed by a data subject for failure to adopt and implement measures that have not been communicated by the data controller;
e) to deal primarily with requests for rights and relations with the supervisory authority, without prejudice to the assistance of the Processor;
f) not to transfer special categories of data unless strictly necessary and on an appropriate legal basis, informing the data subject in advance where possible.

6. Sub-processors

6.1. The Client grants the Platform a general authorization to engage subprocessors to perform personal data processing on behalf of the Client, provided that:
- the engagement of the subprocessor is necessary for the provision of the Services;
- the Platform has entered into a written agreement with the subprocessor imposing data protection obligations no less protective than those in this Agremeent or the applicable data protection provisions embedded in the Service Agreement. The Platform remains fully liable for any acts or omissions of its subprocessors in respect of personal data processed on behalf of the Client;
- the Platform evaluates the security, privacy, and confidentiality practices of each subprocessor before engagement to ensure that it is capable of providing the level of protection required under this Agremeent.

6.2. The initial list of subcontractors is included in Annex I.

6.3. The Platform may incorporate or replace sub-processors by giving at least 15 calendar days' notice by electronic means.

6.4. The Client may object only on objective and justified grounds of data protection, within the notification period.

6.5. If no reasonable alternative is possible, the Platform may partially terminate the affected service or the Service Agreement without additional liability, refunding, where applicable, any prepaid amounts not accrued for the affected service.

7. International transfers

7.1. The Client authorizes the Platform and its subcontractors to make international transfers necessary for the Service, provided that there is a valid mechanism under Chapter V of the GDPR.

7.2. The Platform shall apply the appropriate legal mechanism (adequacy, SCC, or other enabling mechanism) and complementary measures where appropriate.

7.3. The Client acknowledges that certain global providers may involve transfers inherent to their technical architecture.

8. Rights of data subjects

8.1. As a general rule, the Client shall be responsible for responding to requests for rights.

8.2. If the Platform receives a request directly, it will forward it to the Client, unless the law requires direct action.

8.3. Assistance from the Platform that exceeds the standard functionalities of the Service may be billed at current professional rates.

9. Security breaches

9.1. The Platform will notify the Client without undue delay of any confirmed security breach affecting data covered by the order.

9.2. The notification may be made in stages as reliable information becomes available.

9.3. The Platform shall take reasonable containment and mitigation measures.

9.4. Unless legally required, the Platform will not directly notify interested parties or authorities on behalf of the Client without prior instruction.

10. Audit and evidence of compliance

10.1. The Platform shall make reasonable information available to the Client to demonstrate compliance, preferably through standard security/compliance documentation (reports, certifications, questionnaires).

10.2. On-site audits will only be conducted when:

- there is a legal obligation that has not been satisfied with documentary evidence, or
- there is a serious security incident that is duly justified.

10.3. Audit conditions: minimum 30 calendar days' notice, working hours, once per year, no access to other customers' information, no intrusive testing or active scanning, and subject to NDA.

10.4. Internal and external audit costs will be borne by the Client, except in the case of proven material breach by the Platform.

11. Security measures

11.1. The Platform shall maintain a security program appropriate to the risk and proportional to the nature of the Service.

11.2. The Client acknowledges that security measures evolve and may be updated by the Platform provided that they do not substantially reduce the overall level of protection.

12. Liability

12.1. The Parties shall be separately liable for any liability that may be required of them, holding the other party harmless provided that the liability arises from an action or omission by each of them that has caused damage to the other in accordance with applicable data protection legislation.

12.2. The Platform may not rely on a breach of obligations by another data processor it has engaged to avoid its own responsibilities.

12.3. With regard to the subject matter of this Agreement, the Controller shall be liable for any breaches and damages resulting from any infringement of the applicable data protection legislation to which it is subject and, in such a case, shall immediately inform the Processor thereof so that the latter may in turn assess the adoption of any measures, such as the termination of this Agreement.

13. End of service: return and deletion

13.1. Upon termination of the provision of personal data processing services, the Parties agree that the Platform shall retain them for a maximum period of one (1) month, unless otherwise required by applicable law.

13.2. After this period, the Platform shall take the necessary measures for its deletion, unless it is obliged to keep it for longer under European Union law or applicable national legislation in order to respond to any liability arising from the processing of such personal data or relating to the provision of the service that has involved the processing of personal data.

13.3. The same rule shall apply in the case of sub-processors and their processors.

13.4. During the time that the data processor processes the personal data, it shall adopt and implement the necessary technical and organizational measures to ensure the confidentiality and security of the personal data.

13.5. Backup copies will be purged in accordance with regular backup cycles.

14. Platform's own processing

14.1. This Agreement does not authorize the Platform to reuse data from the order for its own commercial purposes.

14.2. If the Platform offers its own services directly to data subjects, it shall act as an independent Data Controller for that purpose and shall fulfill its information and legitimation obligations separately.

15. Notifications

15.1. The Parties stipulate the following email addresses for notification purposes:

1. Processor: hello@onevisa.ai
2. Controller:

16. Applicable legislation

16.1. This Agreement is governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

ANNEX I

LIST OF SUB-PROCESSORS

Sub-Processor	Service	Country
Supabase Inc	Database services	USA (AWS data centers)
PostHog, Inc	Product analytics	EU or USA (depending on instance; EU hosted instances use AWS/GCP in EU regions)
Stripe, Inc	Payment processing	USA
OpenAI	AI processing	USA