Data Processing Agreement (DPA) - TOTHEMOON

Structure

This DPA is structured as follows:

Section	Content
Section A – Key Terms	**The key variables that apply to the DPA are defined in Section A.**
Section B – Legal Terms	**Sets out the general legal terms applicable to the processing.**
Section C – TOMs	**The applicable technical and organizational measures.**

Section A – Key Terms

Variable	Value
Responsible Party(s)	**Controller, Controller address** **Contact: Controller person (Controller email)**
Operator(s)	**ToTheMoon** **Contact: TOBIAS JACQUES WINTERBACH (Jacques@tothemoon.build)** **(together with the Responsible Party, the "Parties")**
Processing purpose	**Processing in the context of the Privacy policy dated 22 October 2024 (the "Base Agreement")**
Duration of processing	**As long as required for the Base Agreement**

Categories of data subjects	**· Customers (natural and juristic persons)** **· Potential clients (natural and juristic persons)**
Categories of personal data	**· Contact data (email, phone)** **· Name** **· Company names** **· Registration numbers** **· Financial information**
Place of storage & processing	**Data will be stored and processed primarily in the EU (AWS region eu-west-1) and the UK (if applicable) through AWS services (e.g., Lambda, S3, and RDS) as managed by Laravel Vapor. Data may also be processed by the following sub-operators outside the EU/UK: OpenAI, Anthropic, and Pinecone, where appropriate data transfer mechanisms (such as Standard Contractual Clauses) are applied, and in compliance with POPIA and UK GDPR requirements for cross-border data transfers.**
On-premise audits	**No**
Sub-processors	**Sub-processors:** **- AWS: Ireland (eu-west-1) for cloud infrastructure (hosting, databases, object storage).** **- OpenAI: U.S. for LLM processing (configurable for "No Log" mode).** **- Anthropic: U.S. for LLM processing.** **- Pinecone: Vector database services, available in U.S. and EU regions.**

Transfer Outside of EU/EEA, UK, and South Africa	**Only allowed to countries where the operator or an approved sub-operator is registered and where adequate protection measures are in place as per GDPR, UK GDPR, and POPIA.**

The variables defined in Section A serve as definitions in Section B.

Section B – Legal Terms

1. Purpose and Scope

a) The purpose of this Data Processing Agreement (the "DPA") is to ensure compliance with Article 28(3) and (4) of the EU General Data Protection Regulation ("GDPR"), the UK GDPR, and the relevant provisions of the Protection of Personal Information Act ("POPIA") of South Africa, with respect to each law only if and to the extent applicable to the respective processing activity.

b) This DPA applies with respect to the processing of personal information as specified in Section A.

2. Interpretation

a) Where this DPA uses terms defined in the GDPR, UK GDPR, or POPIA, as applicable, those terms shall have the same meaning as in those laws.

b) This DPA shall be read and interpreted in the light of the provisions of the GDPR, UK GDPR, and POPIA.

c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in the GDPR, UK GDPR, or POPIA, or prejudices the fundamental rights or freedoms of the data subjects.

3. Hierarchy

In the event of a conflict between this DPA and the provisions of any other agreement between the Parties existing at the time when this DPA is agreed or entered into thereafter, this DPA shall prevail, except where explicitly agreed otherwise in writing.

4. Description of Processing

The details of the processing operations, and in particular the categories of personal information and the purposes of processing for which the personal information is processed on behalf of the responsible party, are specified in Section A.

5. Obligations of the Parties

5.1 General

a) The operator shall process personal information only on documented instructions from the responsible party, unless required to do so by law to which the operator is subject. Such instructions are specified in Section A. In such cases, the operator shall inform the responsible party of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the responsible party throughout the duration of the processing of personal information. Such instructions shall always be documented.

b) The operator shall immediately inform the responsible party if, in its opinion, an instruction infringes applicable data protection laws.

c) The operator agrees to process personal information with the knowledge or authorization of the responsible party and shall treat all personal information as confidential.

5.2 Purpose Limitation

The operator shall process the personal information only for the specific purpose(s) of the processing, as set out in Section A.

5.3 Erasure or Return of Data

a) Processing by the operator shall only take place for the duration specified in Section A.

b) Upon termination of the provision of personal information processing services or termination pursuant to Clause 9, the operator shall, at the choice of the responsible party, delete or return all personal information processed on behalf of the responsible party and certify to the responsible party that it has done so, unless retention of the personal information is required by law.

5.4 Security of Processing

a) The operator shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- **Access Control: Measures to prevent unauthorized persons from gaining access to personal information processing systems.**
- **Data Access Control: Measures to ensure that persons entitled to use a data processing system gain access only to such personal information as they are entitled to access.**
- **Transmission Control: Measures to ensure that personal information cannot be read, copied, modified, or removed without authorization during electronic transmission or transport.**
- **Input Control: Measures to ensure that it is possible to check and establish whether and by whom personal information has been entered into data processing systems.**

- **Job Control: Measures to ensure that personal information is processed strictly in accordance with the instructions of the responsible party.**
- **Availability Control: Measures to ensure that personal information is protected against accidental destruction or loss.**
- **Separation Control: Measures to ensure that personal information collected for different purposes can be processed separately.**

b) In assessing the appropriate level of security, the operator shall take due account of the risks involved in the processing, the nature of the personal information, and the nature, scope, context, and purposes of processing.

c) The operator shall ensure that persons authorized to process the personal information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

d) If the processing involves special categories of personal information, the operator shall apply specific restrictions and/or additional safeguards as reasonably required by the responsible party.

5.5 Documentation and Compliance

a) The operator shall make available to the responsible party all information necessary to demonstrate compliance with the obligations set out in this DPA and under applicable data protection laws.

b) Upon the responsible party's written request, the operator shall provide responses to reasonable data protection questionnaires that are necessary to confirm compliance with this DPA.

c) The operator may satisfy the obligations in this Clause by providing up-to-date attestations, certifications, or reports from independent sources (e.g., external auditors, data protection authorities), or by providing a summary of its data processing facilities and safeguards.

d) The operator and responsible party agree that audits and inspections shall be limited to the information necessary to demonstrate compliance and shall not include access to the operator's premises or physical infrastructure, except as required by applicable law.

e) Any audits shall be conducted during regular business hours, with reasonable advance notice, and in a manner that does not disrupt the operator's business operations.

5.6 Use of Sub-Operators

a) The responsible party provides a general authorization for the operator to engage sub-operators to assist in the processing of personal information under this DPA, provided that the operator informs the responsible party of any intended changes concerning the addition or replacement of sub-operators, thereby giving the

responsible party the opportunity to object to such changes within 15 days after being informed.

b) The operator shall ensure that any sub-operator it engages to process personal information on its behalf is bound by data protection obligations compatible with those of the operator under this DPA.

c) The operator shall remain fully responsible to the responsible party for the performance of the sub-operator's obligations under its contract with the operator.

d) The operator shall, upon the responsible party's request, provide the responsible party with a list of sub-operators and the categories of processing they perform.

5.7 International Transfers

a) Data transfers to countries outside the EU/EEA and South Africa (e.g., the U.S.) shall be made in compliance with Chapter V of the GDPR, UK GDPR, and Sections 72 and 73 of POPIA, using Standard Contractual Clauses or other approved transfer mechanisms.

b) The operator shall ensure that appropriate safeguards are in place for international transfers and shall provide evidence of such safeguards upon the responsible party's reasonable request.

6. Assistance with Data Subject Rights

a) The operator shall assist the responsible party by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the responsible party's obligations to respond to requests for exercising the data subject's rights under GDPR, UK GDPR, and POPIA.

b) The operator shall promptly notify the responsible party if it receives a request from a data subject under any data protection law in respect of personal information processed under this DPA.

c) The operator shall not respond to such requests except on the documented instructions of the responsible party or as required by applicable laws.

d) The operator shall be entitled to charge the responsible party on a time and materials basis in the event that the operator considers, in its reasonable discretion, that assistance under this Clause 6 exceeds the scope of the services agreed in the Base Agreement.

7. Data Breach Notifications

a) The operator shall notify the responsible party without undue delay after becoming aware of a personal data breach affecting personal information processed under this DPA.

b) The notification shall include sufficient information to allow the responsible party to meet any obligations to report or inform data subjects or supervisory authorities of the personal data breach under applicable data protection laws.

c) The operator shall cooperate with the responsible party and take reasonable commercial steps as directed by the responsible party to assist in the investigation, mitigation, and remediation of each such personal data breach.

8. Data Protection Impact Assessments and Prior Consultation

The operator shall provide reasonable assistance to the responsible party with any data protection impact assessments and prior consultations with supervisory authorities or other competent data privacy authorities, in each case solely in relation to processing of personal information and taking into account the nature of the processing and information available to the operator.

9. Deletion or Return of Personal Information

a) Subject to Clause 9b, the operator shall promptly and in any event within 30 days of the date of cessation of any services involving the processing of personal information (the "Cessation Date"), delete and procure the deletion of all copies of those personal information.

b) The operator shall, subject to the Base Agreement, return all the personal information to the responsible party and delete existing copies unless applicable law requires storage of the personal information.

10. Audit Rights

a) The operator shall make available to the responsible party on request all information necessary to demonstrate compliance with this DPA.

b) The operator shall allow for and contribute to audits, including inspections, conducted by the responsible party or an auditor mandated by the responsible party, provided that:

- **Audits shall be limited to once per year, except in case of a data breach or suspected non-compliance.**
- **The responsible party shall give the operator at least 30 days' prior written notice of any audit or inspection.**
- **Audits shall be conducted during regular business hours, in a manner that does not interfere with the operator's business operations.**
- **The scope of the audit shall be limited to information necessary to demonstrate compliance with this DPA.**

c) The operator may require the responsible party to enter into a non-disclosure agreement before the audit.

d) Each party shall bear its own costs in relation to any audits or inspections.

11. Liability

a) Each party's liability arising out of or related to this DPA shall be subject to the limitations and exclusions of liability set out in the Base Agreement, except to the extent that such liability cannot be limited under applicable law.

b) The operator's total aggregate liability towards the responsible party, whether in contract, tort, or under any other theory of liability, shall be limited to the total fees paid under the Base Agreement in the 12 months preceding the event giving rise to the liability.

12. Governing Law and Jurisdiction

a) This DPA shall be governed by and construed in accordance with the laws specified in the Base Agreement.

b) Any disputes arising out of or in connection with this DPA shall be subject to the exclusive jurisdiction of the courts specified in the Base Agreement.

Section C – Technical and Organizational Measures (TOMs)

The operator shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- **Access Control: Measures to prevent unauthorized persons from gaining access to personal information processing systems.**
- **Data Access Control: Measures to ensure that persons entitled to use a data processing system gain access only to such personal information as they are entitled to access.**
- **Transmission Control: Measures to ensure that personal information cannot be read, copied, modified, or removed without authorization during electronic transmission or transport.**
- **Input Control: Measures to ensure that it is possible to check and establish whether and by whom personal information has been entered into data processing systems.**
- **Job Control: Measures to ensure that personal information is processed strictly in accordance with the instructions of the responsible party.**
- **Availability Control: Measures to ensure that personal information is protected against accidental destruction or loss.**
- **Separation Control: Measures to ensure that personal information collected for different purposes can be processed separately.**

The operator may update or modify these measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the processing of personal information.