Data Processing Agreement

This Data Processing Agreement (**DPA**) forms part of and is incorporated into the Services Agreement / Terms of Service dated [date] (the **Agreement**) between:

1. **Dinesh Kumar Gahlot**, an individual trading as **DivineAPI**, of WZ-96, Kh No. 38, Village Dabri, New Delhi, South West Delhi, Delhi 110045, India (GSTIN 07AHTPG5962D3Z1) (**DivineAPI**, **we**, **us**, the **Processor**); and
2. **[Customer legal name]**, registered in [jurisdiction] under number [number], whose registered office is at [address] (**Customer**, **you**, the **Controller**),

each a **party** and together the **parties**.

Background. The Customer operates a website through which individuals submit birth and related details to obtain astrological and numerological reports. The Customer transmits those details to DivineAPI through the DivineAPI application programming interface. DivineAPI performs the calculations, generates the report and returns it to the Customer, and the Customer displays the report to the individual on the Customer's own website. DivineAPI has no direct relationship with those individuals and does not present itself to them.

1. Definitions

1.1 In this DPA:

Applicable Data Protection Law means, as applicable to a party's Processing: (a) the EU GDPR; (b) the UK GDPR and the Data Protection Act 2018; (c) the Swiss Federal Act on Data Protection where relevant; and (d) the Indian Digital Personal Data Protection Act 2023 and rules made under it; in each case with any implementing, amending or successor legislation and any binding guidance issued by a Supervisory Authority.

Customer Personal Data means Personal Data that DivineAPI Processes on behalf of the Customer under the Agreement, including data submitted to the Service by or on behalf of the Customer's end users.

EU GDPR means Regulation (EU) 2016/679.

EU SCCs means the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

Restricted Transfer means a transfer of Customer Personal Data to, or access to it from, a country or territory that is not the subject of an adequacy decision under the Applicable Data Protection Law governing that transfer.

Service means the DivineAPI astrology and numerology API service, including the calculation endpoints, PDF report generation and, where the Customer subscribes to it, the chatbot endpoint.

Special Category Data means Personal Data of the categories listed in Article 9(1) EU GDPR, and Personal Data relating to criminal convictions and offences within Article 10 EU GDPR.

Sub-processor means any third party engaged by DivineAPI to Process Customer Personal Data.

UK Agreement means the International Data Transfer Agreement to the EU SCCs issued by the Information Commissioner under section 119A of the Data Protection Act 2018, version B1.0.

UK GDPR has the meaning given in section 3(10) of the Data Protection Act 2018.

1.2 *Controller*, *Processor*, *Data Subject*, *Personal Data*, *Personal Data Breach*, *Processing*, *Supervisory Authority* and cognate terms have the meanings given in the EU GDPR, and are to be read as including the equivalent terms in the UK GDPR where that applies.

1.3 Where a term is defined both in the Agreement and in this DPA, the definition in this DPA governs the Processing of Personal Data.

2. Roles, scope and duration

2.1 The Customer is the Controller of Customer Personal Data. DivineAPI is the Processor. Neither party will act as a joint controller with the other in respect of Customer Personal Data.

2.2 Where the Customer is itself a processor acting for a third party controller, DivineAPI acts as a sub-processor. The Customer warrants that it has that controller's authority to enter into this DPA on its behalf and to give the instructions in it, and references to the Customer's instructions include that controller's instructions as passed on by the Customer.

2.3 DivineAPI has no direct relationship with the Customer's end users and will not seek one. The Customer is solely responsible for its website, for the privacy information given to its end users, and for the lawfulness of its collection of Personal Data from them.

2.4 Annex 1 sets out the subject matter, duration, nature and purpose of the Processing, the types of Personal Data and the categories of Data Subject, as required by Article 28(3) EU GDPR. Annex 1 forms part of the Customer's documented instructions.

2.5 This DPA applies for as long as DivineAPI Processes Customer Personal Data, whether or not the Agreement has expired or terminated.

3. Customer instructions

3.1 DivineAPI will Process Customer Personal Data only on the Customer's documented instructions, including in relation to transfers to a third country or an international organisation, unless required to Process it by Union or Member State law, or UK law, to

which DivineAPI is subject. In that case DivineAPI will inform the Customer of that legal requirement before Processing, unless that law prohibits it on important grounds of public interest.

3.2 The Customer's documented instructions are (a) this DPA and its Annexes, (b) the Agreement, (c) the parameters and configuration of the API calls the Customer makes, and (d) any further written instruction agreed under clause 3.3.

3.3 The Customer may give further written instructions. Where an instruction falls outside the description in Annex 1, requires a change to the Service, or requires material effort, DivineAPI may charge its reasonable costs on a time and materials basis, having first told the Customer in writing what those costs will be. DivineAPI will not refuse an instruction that is necessary for the Customer to comply with Applicable Data Protection Law.

3.4 DivineAPI will inform the Customer without undue delay if, in its opinion, an instruction infringes Applicable Data Protection Law, and may suspend performance of that instruction until it is withdrawn, amended or confirmed in writing.

3.5 Except under clause 3.4, DivineAPI is not responsible for determining whether the Customer's instructions comply with law applicable to the Customer.

4. Restrictions on DivineAPI's use of Customer Personal Data

4.1 DivineAPI will not:

1. Process Customer Personal Data for any purpose other than performing the Service and complying with this DPA and the Agreement;
2. sell, rent, licence, share or otherwise disclose Customer Personal Data to any third party, except to a Sub-processor under clause 10 or as clause 12 permits;
3. use Customer Personal Data to train, fine-tune, evaluate, ground or otherwise develop any machine learning or artificial intelligence model, whether its own or a third party's, or permit any Sub-processor to do so;
4. combine Customer Personal Data with Personal Data from any other source, or use it to enrich, profile or target any Data Subject;
5. use Customer Personal Data for its own marketing, research, benchmarking or product development;
6. permit any human review of the content of chatbot sessions or report content except where strictly necessary to investigate a fault or a security incident, by named personnel, with the event logged; or
7. retain Customer Personal Data for longer than Annex 1 permits.

4.2 DivineAPI may create and use aggregated or statistical data derived from the Processing, provided that the data is irreversibly anonymised so that no Data Subject can be identified by DivineAPI or by any other person by any means reasonably likely to be used, that the underlying Customer Personal Data is deleted in accordance with Annex 1, and that

the data does not identify the Customer. Pseudonymised data remains Personal Data and clause 4.1 applies to it.

4.3 DivineAPI will keep Customer Personal Data logically separated from data it Processes as a controller for its own account, and will not treat Customer Personal Data as an asset of its business on any insolvency, sale, merger or restructuring.

5. Confidentiality and personnel

5.1 DivineAPI will keep Customer Personal Data confidential and will not disclose it except as this DPA permits.

5.2 DivineAPI will ensure that every person it authorises to Process Customer Personal Data is bound by an enforceable duty of confidentiality, whether contractual or statutory, that survives the end of their engagement.

5.3 Access to Customer Personal Data is limited to personnel who need it to perform the Service. DivineAPI will maintain a current list of personnel with production access, review it at least quarterly, and revoke access within 24 hours of a person ceasing to need it.

5.4 DivineAPI will give personnel with access to Customer Personal Data data protection and security training on appointment and at least annually, and will apply its disciplinary process to breaches of this clause.

6. Security

6.1 DivineAPI will implement and maintain the technical and organisational measures set out in Annex 2 and, more generally, measures appropriate to the risk within the meaning of Article 32 EU GDPR, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing, and the risk to Data Subjects.

6.2 DivineAPI may update the measures in Annex 2, provided the level of security is not reduced. It will notify the Customer in advance of any change that materially affects the protection of Customer Personal Data.

6.3 DivineAPI will review the measures at least annually.

7. Personal Data Breach

7.1 DivineAPI will notify the Customer without undue delay and in any event within 72 hours of becoming aware of a Personal Data Breach affecting Customer Personal Data. Notification goes to the Customer's data protection contact in clause 18.

7.2 The notification will describe, to the extent known: the nature of the breach, including the categories and approximate number of Data Subjects and records affected; the likely consequences; the measures taken or proposed to address it and to mitigate its effects; and

the name and contact details of a point of contact. Where the information is not all available at once, DivineAPI will provide it in phases without further undue delay.

7.3 DivineAPI will, at its own cost where the breach arose from its breach of this DPA, take immediate steps to contain, investigate and remediate the breach, preserve evidence, co-operate with the Customer, and provide a written root cause analysis and remediation plan within 30 days of the notification.

7.4 DivineAPI will assist the Customer with notifications to Supervisory Authorities and Data Subjects under Articles 33 and 34 EU GDPR.

7.5 DivineAPI will not notify any Supervisory Authority or Data Subject, and will make no public statement, about a Personal Data Breach affecting Customer Personal Data without the Customer's prior written consent, unless required by law, in which case it will tell the Customer first.

7.6 DivineAPI will keep a record of all Personal Data Breaches affecting Customer Personal Data, including the facts, effects and remedial action, and make it available to the Customer on request.

7.7 Notification under this clause is not an acknowledgement of fault or liability.

8. Data Subject rights

8.1 DivineAPI will, by appropriate technical and organisational measures, assist the Customer insofar as possible in fulfilling its obligation to respond to requests to exercise rights under Chapter III of the EU GDPR or UK GDPR.

8.2 If DivineAPI receives a request directly from a Data Subject relating to Customer Personal Data, it will not respond substantively other than to acknowledge the request and direct the Data Subject to the Customer, will not disclose the Customer's identity unless the Customer agrees or the law requires it, and will forward the request to the Customer within three business days.

8.3 Assistance includes locating, exporting, correcting, restricting and deleting Customer Personal Data on the Customer's written instruction, within 10 business days of the instruction or such shorter period as the Customer reasonably requires to meet its own statutory deadline.

8.4 DivineAPI will provide the assistance in clauses 8.1 to 8.3 at no additional charge where the Service provides the necessary functionality. Where a request requires disproportionate manual effort, DivineAPI may charge its reasonable costs at the rates in the Agreement, having first told the Customer what those costs will be.

9. Data protection impact assessments and prior consultation

9.1 DivineAPI will provide reasonable assistance to the Customer with data protection impact assessments under Article 35 EU GDPR and prior consultation with a Supervisory Authority under Article 36, taking into account the nature of the Processing and the information available to DivineAPI.

9.2 That assistance includes providing the information in Annexes 1 and 2, information about Sub-processors and transfer arrangements, and reasonable answers to a security or privacy questionnaire.

10. Sub-processors

10.1 The Customer gives DivineAPI general written authorisation to engage Sub-processors. The Sub-processors authorised at the date of this DPA are listed in Annex 4.

10.2 DivineAPI will notify the Customer in writing at least 30 days before a new Sub-processor begins Processing Customer Personal Data, stating the Sub-processor's name, location, the Processing it will perform and the transfer mechanism relied on. Notice goes to the Customer's contact in clause 18.

10.3 The Customer may object on reasonable data protection grounds within that 30 day period. The parties will discuss the objection in good faith. If DivineAPI cannot offer an alternative that reasonably addresses it within 30 days, the Customer may terminate the affected part of the Service, or the Agreement as a whole where the affected part is material to it, on written notice and without penalty, and DivineAPI will refund prepaid fees for the unused period on a pro rata basis.

10.4 DivineAPI will appoint each Sub-processor under a written contract imposing data protection obligations no less protective than this DPA, including the obligations in Article 28(3) EU GDPR, and, where the appointment involves a Restricted Transfer, an appropriate transfer mechanism.

10.5 DivineAPI will carry out documented due diligence on the security and data protection practices of each Sub-processor before appointment and at least annually thereafter.

10.6 DivineAPI remains fully liable to the Customer for the acts and omissions of each Sub-processor as if they were its own.

10.7 The chatbot endpoint uses the large language model providers listed in Annex 4. If the Customer objects to those providers under clause 10.3, DivineAPI may disable the chatbot endpoint for the Customer rather than terminate the rest of the Service, with a pro rata refund for that endpoint.

11. International transfers

11.1 Customer Personal Data is Processed in India, in the AWS ap-south-1 (Mumbai) region and on DigitalOcean servers in Bangalore, and, where the Customer uses the chatbot endpoint, in the United States by the providers listed in Annex 4. The Customer instructs DivineAPI to make those transfers.

11.2 **EU GDPR transfers.** For Customer Personal Data subject to the EU GDPR, the parties enter into the EU SCCs, which are incorporated into and form part of this DPA, completed as set out in Annex 3. Module Two (controller to processor) applies where the Customer is a controller. Module Three (processor to sub-processor) applies where the Customer is a processor acting for a third party controller. By signing this DPA the parties are treated as having signed the EU SCCs and their Annexes.

11.3 **UK GDPR transfers.** For Customer Personal Data subject to the UK GDPR, the parties enter into the UK Agreement, completed as set out in Annex 3, which amends the EU SCCs accordingly.

11.4 **Swiss transfers.** For Customer Personal Data subject to the Swiss FADP, the EU SCCs apply with these amendments: the competent supervisory authority is the Federal Data Protection and Information Commissioner; references to the GDPR are to the FADP; the governing law is Swiss law; and the term *Member State* is read so as not to deprive a Data Subject in Switzerland of the right to sue in their place of habitual residence.

11.5 If the EU SCCs, the UK Agreement or any other mechanism relied on is invalidated, replaced or amended, the parties will co-operate in good faith to put an alternative lawful mechanism in place without undue delay. Pending that, the Customer may instruct DivineAPI to suspend the transfer, and DivineAPI will comply.

11.6 Where a country in which Customer Personal Data is Processed becomes the subject of an adequacy decision covering the transfer, the parties may agree in writing to rely on it instead.

11.7 **Transfer risk assessment.** DivineAPI will provide the Customer, on request and without charge, the information it reasonably needs to carry out and keep under review a transfer impact assessment, including the information in Annex 3 about Indian law, the supplementary measures applied, and the records kept under clause 12.

11.8 DivineAPI warrants that it has no reason to believe that the laws and practices applicable to it in India, including the Information Technology Act 2000, prevent it from fulfilling its obligations under the EU SCCs, and that it has not created and will not create any back door, direct access facility or similar arrangement, and has not disclosed and will not disclose any encryption key, that would allow a public authority access to Customer Personal Data otherwise than under clause 12. DivineAPI will notify the Customer promptly if it can no longer give this warranty.

11.9 In the event of conflict between the EU SCCs or the UK Agreement and any other term of this DPA or the Agreement, the EU SCCs or the UK Agreement prevail.

12. Government and law enforcement access

12.1 If DivineAPI or a Sub-processor receives a legally binding request from a public authority, including a judicial authority, for disclosure of Customer Personal Data, DivineAPI will:

1. notify the Customer promptly and, where possible, before disclosure, and provide a copy of the request unless prohibited;
2. where prohibited from notifying, use best efforts to obtain a waiver of the prohibition, and challenge the prohibition itself, and document those efforts so that they can be shown to the Customer or a Supervisory Authority on request;
3. challenge the request where there are reasonable grounds to consider it unlawful under the law of the requesting authority, excessive, or inconsistent with the Applicable Data Protection Law, and pursue available avenues of appeal, seeking interim measures to suspend disclosure until the challenge is resolved;
4. disclose only the minimum amount of Customer Personal Data permissible on a reasonable interpretation of the request; and
5. keep a record of each request, the response and the reasoning.

12.2 DivineAPI will not give any public authority direct, indirect, bulk or remote access to Customer Personal Data, nor provide any encryption key, except under a legally binding request handled in accordance with clause 12.1.

12.3 DivineAPI will publish, or provide to the Customer on request at least annually, aggregate information about the number and types of requests it has received, to the extent lawful. Where it has received none, it will say so.

12.4 Nothing in this clause requires DivineAPI to act unlawfully in India.

13. Records and audits

13.1 DivineAPI will maintain the records of Processing required by Article 30(2) EU GDPR and make them available to the Customer and to any Supervisory Authority on request.

13.2 DivineAPI will make available to the Customer all information reasonably necessary to demonstrate compliance with Article 28 EU GDPR and this DPA, and will allow for and contribute to audits and inspections conducted by the Customer or an auditor it mandates.

13.3 Audits may be carried out once in any 12 month period, and additionally where a Supervisory Authority requires it or following a Personal Data Breach affecting Customer Personal Data. The Customer will give at least 30 days' written notice, the parties will agree the scope, timing and duration in advance, and audits will take place during business hours and in a way that does not unreasonably disrupt DivineAPI's business.

13.4 An auditor mandated by the Customer must not be a competitor of DivineAPI and must be bound by confidentiality obligations no less protective than those in the Agreement. No audit may extend to data, systems or premises of DivineAPI's other

customers, or to information whose disclosure would breach DivineAPI's obligations to a third party.

13.5 Each party bears its own costs of an audit, and the Customer bears DivineAPI's reasonable costs of supporting an on-site audit at rates agreed in advance, except where the audit reveals material non-compliance with this DPA, in which case DivineAPI bears the reasonable costs of the audit and will remediate the non-compliance at its own cost within a period the parties agree in writing, acting reasonably.

13.6 DivineAPI may discharge clause 13.2 in part by providing a current third party certification or audit report, such as ISO/IEC 27001 or SOC 2 Type II, where it holds one, and a completed security questionnaire. That does not remove the Customer's right to audit under clause 13.3.

13.7 DivineAPI will submit to audits and inspections by a Supervisory Authority with jurisdiction over the Customer's Processing and will co-operate with them.

14. Retention, return and deletion

14.1 DivineAPI will retain Customer Personal Data only for the periods in Annex 1. End user data is deleted from live systems on that schedule automatically, without either party having to act.

14.2 At the Customer's choice, on expiry or termination of the Agreement DivineAPI will delete or return all Customer Personal Data and delete existing copies. The Customer must make its election in writing within 30 days of termination; DivineAPI will complete deletion or return within 30 days of the election, or, if the Customer makes no election, will delete within 60 days of termination.

14.3 Where the Customer elects return, DivineAPI will provide the data in a structured, commonly used, machine readable format (JSON) over a secure channel.

14.4 The Customer may request deletion of all or part of the Customer Personal Data at any time during the term. DivineAPI will delete it from live systems within seven days of a written request to admin@divineapi.com and confirm completion in writing.

14.5 **Backups.** Database backups are encrypted, held for disaster recovery only, and roll over on a 90 day window, so they cannot be edited record by record. Data deleted from live systems remains in backups until those backups expire, at most 90 days, and is not accessed or used during that time other than to restore the Service after a disaster. DivineAPI logs every deletion and, if a backup is restored, re-applies the logged deletions before the restored data is returned to service.

14.6 **Statutory retention.** DivineAPI will retain invoices, payment records and related accounting data for the period required by Indian tax and accounting law, currently up to eight years from the end of the relevant financial year. It cannot delete these on request. DivineAPI will limit that retained data to what the law requires, continue to apply clause 4

and Annex 2 to it, and delete it once the period expires. The parties acknowledge this is a legal obligation on DivineAPI within the meaning of Article 28(3)(g) EU GDPR.

14.7 On written request following deletion under clause 14.2 or 14.4, DivineAPI will provide a signed certificate of deletion listing what was deleted, when, and what was retained under clause 14.6.

15. Customer obligations and warranties

15.1 The Customer warrants that it has and will maintain a lawful basis under Article 6 EU GDPR for the Processing it instructs, and where relevant a condition under Article 9.

15.2 The Customer will provide its end users with the information required by Articles 13 and 14 EU GDPR before submitting their data to the Service, including that a third party processor is used, that Personal Data is transferred to and Processed in India and, where the chatbot endpoint is enabled, in the United States, and the safeguards relied on.

15.3 The Customer is responsible for the accuracy, quality and legality of the Customer Personal Data it submits and for the means by which it acquired it.

15.4 **Special Category Data.** The Service is not designed for Special Category Data. The Customer will not submit Special Category Data and will use reasonable technical and organisational measures to prevent its end users from doing so. The Customer acknowledges that free text submitted to the chatbot endpoint may reveal health, sex life, sexual orientation, or religious or philosophical beliefs. Where the Customer enables free text input it will: identify and document an Article 9(2) condition; display a clear notice telling users not to include such information; and apply filtering or moderation where reasonably practicable. Where Special Category Data is nonetheless Processed, DivineAPI will apply the additional measures in Annex 2 paragraph 15, and neither party's compliance with this clause limits its obligations under Article 9.

15.5 **Children.** The Customer will not knowingly submit Personal Data of a child below the age at which that child can consent to information society services under Article 8 EU GDPR in the relevant Member State, or below 13 where the UK GDPR applies, without the consent or authorisation of the holder of parental responsibility. The Customer will apply age assurance measures proportionate to the risk and will tell DivineAPI in writing if the Service is directed at or likely to be accessed by children, so that DivineAPI can apply appropriate measures.

15.6 **Credentials.** The Customer will keep its API keys confidential, rotate them at least annually, restrict them to its own server side systems rather than exposing them in client side code, and notify DivineAPI without undue delay of any actual or suspected compromise. The Customer is responsible for Processing carried out under its credentials except where the compromise was caused by DivineAPI's breach of this DPA.

15.7 The Customer will indemnify DivineAPI against losses, fines and reasonable costs arising from the Customer's breach of this clause 15, subject to clause 16.

16. Liability and indemnity

16.1 The total aggregate liability of each party to the other arising out of or in connection with this DPA and the Agreement, however arising, whether in contract, tort (including negligence), breach of statutory duty, under any indemnity or otherwise, and taking all claims together, will not exceed the total fees paid by the Customer to DivineAPI under the Agreement in the three months immediately before the first event giving rise to the liability.

16.2 DivineAPI will indemnify the Customer against claims by Data Subjects, administrative fines and reasonable costs to the extent they arise from DivineAPI Processing Customer Personal Data in breach of this DPA or outside the Customer's lawful documented instructions.

16.3 Where both parties are responsible for damage caused by Processing, Article 82(5) EU GDPR applies, and a party that has paid full compensation to the Data Subject may recover from the other the part corresponding to the other's responsibility.

16.4 A party claiming under an indemnity in this DPA will notify the other promptly, will not admit liability without its consent (not to be unreasonably withheld), will allow it to participate in the defence, and will take reasonable steps to mitigate.

16.5 The cap in clause 16.1 applies to the indemnity in clause 15.7, the indemnity in clause 16.3 and any recovery between the parties under clause 16.4.

16.6 The parties agree that the cap in clause 16.1 is reasonable and that the fees under the Agreement have been set on that basis.

17. Representatives

17.1 If and for so long as DivineAPI is subject to Article 3(2) EU GDPR, it will designate a representative in the Union under Article 27 EU GDPR and give the Customer its name and contact details. The equivalent applies to a UK representative under Article 27 UK GDPR.

17.2 Each party will give the other the contact details of its data protection officer, where it is required to appoint one, or of the person responsible for data protection matters.

18. Notices

18.1 Notices under this DPA, including breach notifications and sub-processor notices, must be in writing and sent to:

- DivineAPI: admin@divineapi.com, marked for the attention of Dinesh Kumar Gahlot
- Customer: [name, role, email]

18.2 Each party will keep its contact details current and notify the other of any change. A notice sent by email is deemed received when sent, provided no delivery failure is received.

19. General

19.1 **Precedence.** This DPA prevails over any conflicting term of the Agreement in respect of the Processing of Personal Data. The EU SCCs and UK Agreement prevail over this DPA.

19.2 **Variation.** This DPA may be varied only in writing signed by both parties, except that DivineAPI may amend it on 30 days' written notice to reflect a change in Applicable Data Protection Law or the adoption of a replacement transfer mechanism, provided the amendment does not reduce the protection given to Customer Personal Data. The Customer may terminate without penalty if it reasonably objects to such an amendment.

19.3 **Assignment and change of control.** DivineAPI will notify the Customer at least 30 days before transferring its business, including on incorporation of the sole proprietorship into a company, and will procure that the transferee assumes this DPA. The Customer may terminate the Agreement without penalty if the transferee cannot meet the obligations in this DPA.

19.4 **Severability.** If a provision is held invalid, the rest continues in force.

19.5 **Third party rights.** No person other than the parties has a right to enforce this DPA, except that Data Subjects have the third party beneficiary rights conferred by the EU SCCs and the UK Agreement.

19.6 **Governing law.** This DPA is governed by the law stated in the Agreement and subject to the same jurisdiction, except that the EU SCCs are governed by the law and courts specified in Annex 3.

19.7 **Counterparts.** This DPA may be signed in counterparts and by electronic signature.

Execution

By signing below, each party also signs the EU SCCs and the UK Agreement incorporated by clauses 11.2 and 11.3, in the capacities set out in Annex 3.

Signed for and on behalf of Dinesh Kumar Gahlot trading as DivineAPI (data importer)

Name: _____ Title: _____

Signature: _____ Date: _____

Signed for and on behalf of [Customer legal name] (data exporter)

Name: _____ Title: _____

Signature: _____ Date: _____

Annex 1 — Description of the Processing and retention

This Annex is the description required by Article 28(3) EU GDPR and also serves as Annex I.B to the EU SCCs.

Subject matter. Provision of the Service under the Agreement.

Duration. The term of the Agreement, plus the retention periods below.

Nature and purpose. Receiving API requests from the Customer's systems; performing astrological and numerological calculations; generating and returning reports; where enabled, operating the chatbot endpoint; and maintaining the logs necessary to provide, bill for and secure the Service.

Frequency. Continuous, on each API call made by the Customer.

Types of Personal Data. Date, time and place of birth; name where the Customer chooses to send it; derived attributes such as zodiac sign, timezone and calculated chart values; free text questions where the chatbot endpoint is used; technical data in request logs (IP address, requesting domain, device and browser details, API key); and the Customer's account and billing contact details.

Special Category Data. None is intended to be Processed. See clause 15.4 for the position on free text. Where Special Category Data is Processed, the restrictions in Annex 2 paragraph 15 apply.

Categories of Data Subject. The Customer's end users, and the Customer's personnel who administer its account.

Competent supervisory authority. Where the Customer is established in an EEA Member State, the supervisory authority of that Member State. Where the Customer is not established in the EEA but is subject to the EU GDPR under Article 3(2), the supervisory authority of the Member State in which its representative under Article 27 EU GDPR is established or, failing that, in which the Data Subjects are located. For Customer Personal Data subject to the UK GDPR, the Information Commissioner's Office. For Customer Personal Data subject to the Swiss FADP, the Federal Data Protection and Information Commissioner.

Retention schedule

Deletion means removal from live systems. Backups are held for disaster recovery only on a rolling 90 day window, so a deleted record leaves the backups within 90 days of its live deletion (clause 14.5).

Data	Purpose	Deleted from live systems after

API request parameters (calculation endpoints)	Computing the response	Not retained once the response is returned
API request logs: calling account, endpoint, time, caller IP, domain, device, API key	Operations, abuse prevention, billing accuracy	90 days, including any archive copy
PDF report content, including the birth details used to generate it	Re-serving a purchased report	90 days
Chatbot sessions: question text, birth details, API key	Operating the chatbot endpoint	90 days
Error and diagnostic logs	Service reliability	90 days
Aggregated usage counts per account and endpoint, with no IP, key or device	Billing and quota	Retained; contains no end user data
Customer account record: name, email, API key	Operating the account	Life of the account, then within 7 days of a written deletion request
Invoices and payment records	Statutory accounting and tax	Period required by Indian tax and accounting law, currently up to 8 years from the end of the financial year; not deleted on request (clause 14.6)

The Customer's own account and billing records are Processed by DivineAPI as a controller under its privacy policy, not as a processor under this DPA.

Annex 2 — Technical and organisational measures

This Annex is the description required by Article 32 EU GDPR and serves as Annex II to the EU SCCs.

1. **Encryption in transit.** All API traffic is served over TLS 1.2 or higher. Plain HTTP is redirected or refused.
2. **Encryption at rest.** The production database is encrypted with AES-256 via AWS KMS. Automated backups and snapshots inherit that encryption. Keys are managed in AWS KMS in ap-south-1 and access to them is restricted to named personnel.

3. **Pseudonymisation and minimisation.** Request logs record the API key rather than the end user identity. Aggregated usage counts hold no IP address, key or device data. Report content is stored against a report identifier, not an end user profile.
4. **Network isolation.** Production databases are not publicly routable; database ports are firewalled and reachable only from application subnets. Administrative access is by SSH with individual keys issued to named personnel, restricted by firewall to approved IP addresses.
5. **Access control.** Production access is limited to named personnel on a need to know basis, authenticated by SSH key with multi-factor authentication enforced. Password login is disabled. Multi-factor authentication is enforced on the AWS console, the domain registrar, the source code repository and the payment provider.
6. **Least privilege.** Read-only credentials are used for reporting and analysis. Application credentials are scoped to the minimum required.
7. **Logging and monitoring.** Access to production systems and API usage is logged. Logs are retained for 90 days.
8. **Rate limiting and abuse controls.** API keys are rate limited per account; anomalous call patterns trigger alerts and, where necessary, suspension.
9. **Backups and resilience.** Automated database backups are encrypted, held in ap-south-1 (Mumbai), retained on a 90 day rolling window and used only for disaster recovery.
10. **Business continuity.** A documented recovery plan with a recovery time objective of 24 hours and a recovery point objective of 24 hours.
11. **Vulnerability and patch management.** Security updates are applied monthly. Critical vulnerabilities are patched within 7 days of a fix becoming available.
12. **Secure development and change management.** Code changes are reviewed before release, deployed through a controlled pipeline, and can be rolled back. Production data is not used in development or test environments.
13. **Personnel.** Staff and contractors with access are bound by written confidentiality obligations, receive data protection and security training on appointment and annually. Access is revoked within 24 hours of departure.
14. **Additional measures where Special Category Data is Processed.** Storage restricted to the shortest retention period in Annex 1; access limited to a named subset of personnel; access logged and reviewed monthly; no use in any analytics, model development or testing; excluded from any data export other than to the Customer.
15. **Sub-processor management.** Documented due diligence before appointment and at least annually, written contracts under clause 10.4, and a maintained register of Sub-processors and the data each receives.
16. **Incident response.** A documented process for detecting, triaging, escalating, containing and notifying Personal Data Breaches, with named owners and the timescales in clause 7.
17. **Disposal.** Media and storage are securely wiped or destroyed before disposal or reuse; cloud storage is deleted through the provider's deletion process.

18. **Physical security.** Processing takes place in AWS data centres in ap-south-1 (Mumbai) and DigitalOcean data centres in Bangalore. DivineAPI holds no Customer Personal Data on portable media, and devices used to access production are encrypted at rest and screen locked.
19. **Governance.** Records of Processing under Article 30(2); annual review of this Annex; a named individual responsible for data protection.

Annex 3 — Transfer mechanisms

Data exporter. [Customer legal name], [address]. Role: controller (Module Two) or processor (Module Three), as applicable. Contact: [name, role, email].

Data importer. Dinesh Kumar Gahlot trading as DivineAPI, WZ-96, Kh No. 38, Village Dabri, New Delhi 110045, India. Role: processor (Module Two) or sub-processor (Module Three). Contact: admin@divineapi.com.

Annex I.A (parties) is as above. **Annex I.B** (description of transfer) is Annex 1 of this DPA. **Annex I.C** (competent supervisory authority) is as stated in Annex 1. **Annex II** (technical and organisational measures) is Annex 2 of this DPA. **Annex III** (sub-processors) is Annex 4 of this DPA.

EU Standard Contractual Clauses — selections

Clause	Selection
Module	Two (controller to processor) where the Customer is a controller; Three (processor to sub-processor) where the Customer is a processor
Clause 7 (docking)	Applies
Clause 9 (sub-processors)	Option 2, general written authorisation, 30 days' notice
Clause 11(a) (independent dispute resolution)	The optional redress-body wording does not apply
Clause 13 / Annex I.C	Supervisory authority as stated in Annex 1
Clause 17 (governing law)	Option 1, the law of Ireland
Clause 18(b) (jurisdiction)	The courts of Ireland

UK International Data Transfer Agreement

Version B1.0 applies to transfers subject to the UK GDPR, amending the EU SCCs as the Agreement provides.

Table	Entry
Table 1 (parties)	As stated above; start date is the date of this DPA
Table 2 (selected SCCs)	The EU SCCs as completed in this Annex, Module Two or Three as applicable
Table 3 (appendix information)	Annex 1, Annex 2 and Annex 4 of this DPA
Table 4 (ending the Agreement)	Neither party may end the Agreement when the Approved Agreement changes

Transfer risk assessment — information about India

Provided under clause 11.7 to help the Customer complete its own assessment. It is not the assessment itself; the Customer, as exporter, must carry that out and keep it under review.

- India is not the subject of an adequacy decision under Article 45 EU GDPR or the equivalent UK regime. Transfers therefore rely on the EU SCCs and UK Agreement plus the supplementary measures below.

- The principal Indian laws under which a public authority may seek access are the Information Technology Act 2000 (in particular sections 69 and 69B), the Indian Telegraph Act 1885, and the Code of Criminal Procedure. Access is generally by order to the entity holding the data rather than by bulk or direct access.
- Oversight of interception orders in India is by an executive review committee rather than by a court, and there is no general right for a foreign data subject to be notified of, or to challenge, an order. The Customer should treat this as the principal residual risk in its assessment.
- The Digital Personal Data Protection Act 2023 imposes obligations on DivineAPI as a data fiduciary or data processor under Indian law, including security safeguards and breach notification to the Data Protection Board.
- **Practical likelihood.** The data transferred is birth details used to generate astrological reports. It is not of a type ordinarily sought by law enforcement or intelligence agencies. DivineAPI has received no government access requests to date.
- **Supplementary measures relied on.** Encryption in transit and at rest with keys held by DivineAPI and not by any Sub-processor or authority (Annex 2 paragraphs 1 and 2); short retention periods (Annex 1); minimisation of identifiers in logs; the government access commitments in clause 12; the warranty in clause 11.8; and the Customer's right to suspend transfers under clause 11.5.

Onward transfer to the United States (chatbot endpoint only)

Where the chatbot endpoint is used, DivineAPI transfers question text and the associated birth details to the large language model providers listed in Annex 4 for the sole purpose of generating a response. DivineAPI will procure that each such provider: does not use the data to train or improve any model; retains it for no longer than 30 days and, where the provider offers zero data retention, that this is enabled; and is bound either by a valid EU-US Data Privacy Framework certification covering the data or by the EU SCCs Module Three with equivalent UK and Swiss provisions.

Annex 4 — Approved Sub-processors

This Annex serves as Annex III to the EU SCCs.

Sub-processor	Registered address	Processing carried out	Location of Processing	Transfer mechanism
Amazon Web Services, Inc. / AWS India	410 Terry Avenue North, Seattle, WA 98109, USA	Hosting, database, backups, key management	India (ap-south-1, Mumbai)	Covered by this DPA; importer is DivineAPI

DigitalOcean, LLC	105 Edgeview Drive, Suite 425, Broomfield, CO 80021, USA	Application and API server hosting; request logs in transit	India (Bangalore, blr1)	Covered by this DPA; importer is DivineAPI
Zoho Corporation Pvt. Ltd.	Estancia IT Park, Plot 140 and 151, GST Road, Vallancherry, Chengalpattu, Tamil Nadu 603202, India	Customer support chat and demo bookings (Customer personnel only, no end user data)	India	Covered by this DPA; importer is DivineAPI
OpenAI, Anthropic, Google (Gemini)	OpenAI: 1960 Bryant Street, San Francisco, CA 94110, USA. Anthropic PBC: 548 Market Street, San Francisco, CA 94104, USA. Google LLC: 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Generating chatbot responses	United States	EU-US Data Privacy Framework certification or EU SCCs Module Three, per provider
Stripe, Inc.	354 Oyster Point Boulevard, South San Francisco, CA 94080, USA	Processing Customer payments only. Receives no API request data.	United States and EU	EU-US Data Privacy Framework certification
Mailchimp Transactional (Mandrill), The Rocket Science Group LLC	675 Ponce de Leon Avenue NE, Suite 5000, Atlanta, GA 30308, USA	Sending account and notification email	United States	EU-US Data Privacy Framework certification
Sentry (Functional Software, Inc.)	45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Diagnostic logs	United States	EU-US Data Privacy Framework certification

Changes to this list are notified under clause 10.2.