This Data Processing Agreement ("DPA") forms part of the Terms of Use (or other similarly titled written or electronic agreement addressing the same subject matter) ("**Agreement**") between Customer (as defined in the Agreement) and "**OTPless**" under which the Processor provides the Controller with the software and services (the **"Services"**). The Controller and the Processor are individually referred to as a **"Party"** and collectively as the **"Parties"**.

The Parties seek to implement this DPA to comply with the requirements of EU GDPR (defined hereunder) in relation to Processor's processing of Personal Data (as defined under the EU GDPR) as part of its obligations under the Agreement.

This DPA shall apply to Processor's processing of Personal Data, provided by the Controller as part of Processor's obligations under the Agreement.

Except as modified below, the terms of the Agreement shall remain in full force and effect.

1. **Definitions**

   Terms not otherwise defined herein shall have the meaning given to them in the EU GDPR or the Agreement. The following terms shall have the corresponding meanings assigned to them below:

   1.1. "**Data Transfer**" means a transfer of the Personal Data from the Controller to the Processor, or between two establishments of the Processor, or with a Sub-processor by the Processor.

   1.2. "**EU GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

   1.3. "**Standard Contractual Clauses**" means the contractual clauses attached hereto as Schedule 1 pursuant to the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of data protection.

   1.4. "**Controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

   1.5. **"Processor"** means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

1.6. "**Sub-processor**" means a processor/ sub-contractor appointed by the Processor for the provision of all or parts of the Services and Processes the Personal Data as provided by the Controller.

2. **Purpose of this Agreement**

This DPA sets out various obligations of the Processor in relation to the Processing of Personal Data and shall be limited to the Processor's obligations under the Agreement. If there is a conflict between the provisions of the Agreement and this DPA, the provisions of this DPA shall prevail.

3. **Categories of Personal Data and Data Subjects**

The Controller authorizes permission to the Processor to process the Personal Data to the extent of which is determined and regulated by the Controller. The current nature of the Personal Data is specified in Annex I to Schedule 1 to this DPA.

4. **Purpose of Processing**

The objective of Processing of Personal Data by the Processor shall be limited to the Processor's provision of the Services to the Controller and or its Client, pursuant to the Agreement.

5. **Duration of Processing**

The Processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing by the Controller.

6. **Data Controller's Obligations**

6.1. The Data Controller shall warrant that it has all necessary rights to provide the Personal Data to the Data Processor for the Processing to be performed in relation to the agreed services. To the extent required by Data Privacy Laws, Data Controller is responsible for ensuring that it provides such Personal Data to Data Processor based on an appropriate legal basis allowing lawful processing activities, including any necessary Data Subject consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. Should such consent be revoked by the Data Subject, the Data Controller is responsible for communicating the fact of such revocation to the Data Processor.

6.2. The Data Controller shall provide all natural persons from whom it collects Personal Data with the relevant privacy notice.

6.3. The Data Controller shall request the Data Processor to purge Personal Data when required by the Data Controller or any Data Subject whom it collects Personal Data unless the Data Processor is otherwise required to retain the Personal Data by applicable law.

6.4. The Data Controller shall immediately advise the Data Processor in writing if it receives or learns of any:

6.4.1. Complaint or allegation indicating a violation of Data Privacy Laws regarding Personal Data;

6.4.2. Request from one or more individuals seeking to access, correct, or delete Personal Data;

6.4.3. Inquiry or complaint from one or more individuals relating to the collection, processing, use, or transfer of Personal Data; and

6.4.4. Any regulatory request, search warrant, or other legal, regulatory, administrative, or governmental process seeking Personal Data

7. **Data Processor's Obligations**

7.1. The Processor will follow written and documented instructions received, including email, from the Controller, its affiliate, agents, or personnel, with respect to the Processing of Personal Data (each, an "**Instruction**").

7.2. The Processing described in the Agreement and the relating documentation shall be considered as Instruction from the Controller.

7.3. At the Data Controller's request, the Data Processor will provide reasonable assistance to the Data Controller in responding to/ complying with requests/ directions by Data Subject in exercising their rights or of the applicable regulatory authorities regarding Data Processor's Processing of Personal Data.

7.4. In relation to the Personal Data, Data Processor shall obtain consent (where necessary) and/or provide notice to the Data Subject in accordance with Data Protection Laws to enable shared Personal Data to be provided to, and used by, the other Party as contemplated by this Agreement.

7.5. Where shared Personal Data is transferred outside the Data Processor's territorial boundaries, the transferor shall ensure that the recipient of such data is under contractual obligations to protect such Personal Data to the same or higher standards as those imposed under this Addendum and the Data Protection Laws.

7.6. The processor shall inform the controller if, in its opinion, a processing instruction infringes applicable legislation or regulation.

7.7. As A Data Processor ,taking into account the nature of the processing and the information available to the Data Processor, the Data Processor shall assist the data controller in conducting any necessary Data Protection Impact Assessments (DPIAs), as required under GDPR.

8. **Data Secrecy**

8.1. To Process the Personal Data, the Processor will use personnel who are

8.1.1. Informed of the confidential nature of the Personal Data, and

8.1.2. Perform the Services in accordance with the Agreement.

8.2. The Processor will regularly train individuals having access to Personal Data in data security and data privacy in accordance with accepted industry practice and shall ensure that all the Personal Data is kept strictly confidential.

8.3. The Processor will maintain appropriate technical and organizational measures for protection of the security, confidentiality, and integrity of the Personal Data as per the specifications as per the standards mutually agreed in writing by the Parties.

9. **Audit Rights**

9.1. Upon Controller's reasonable request, the Processor will make available to the Controller, information as is reasonably necessary to demonstrate Processor's compliance with its obligations under the EU GDPR or other applicable laws in respect of its Processing of the Personal Data.

9.2. When the Controller wishes to conduct the audit (by itself or through a representative) at Processor's site, it shall provide at least fifteen (15) days' prior written notice to the Processor; the Processor will provide reasonable cooperation and assistance in relation to audits, including inspections, conducted by the Controller or its representative.

9.3. The Controller shall bear the expense of such an audit.

10. **Mechanism of Data Transfers**

Any Data Transfer for the purpose of Processing by the Processor in a country outside the European Economic Area (the "***EEA***") shall only take place in compliance as detailed in Schedule 1 to the DPA. Where such model clauses have not been executed at the same time as this DPA, the Processor shall not unduly withhold the execution of such template model clauses, where the transfer of Personal Data outside of the EEA is required for the performance of the Agreement.

11. **Sub-processors**

11.1. The Controller acknowledges and agrees that the Processor, may engage a third-party Sub-processor(s) in connection with the performance of the Services, provided such Sub-processor(s) take technical and organizational measures to ensure confidentiality of Personal Data shared with them; The current Sub-processors engaged by the Processors and approved by the Controller are listed in Annex III of Schedule 1 hereto. The processor shall notify the controller at least thirty (30) calendar days in advance of any intended changes or additions to its Sub-processors listed in Annex III by emailing notice of the intended change to Customer. In accordance with Article 28(4) of the GDPR, the Processor shall remain liable to

Controller for any failure on behalf of a Sub-processor to fulfil its data protection obligations under the DPA in connection with the performance of the Services.

11.2. If the Controller has a concern that the Sub-processor(s) Processing of Personal Data is reasonably likely to cause the Controller to breach its data protection obligations under the GDPR, the Controller may object to Processor's use of such Sub-processor and the Processor and Controller shall confer in good faith to address such concern.

12. **Personal Data Breach Notification**

12.1. The Processor shall maintain defined procedures in case of a Personal Data Breach (as defined under the GDPR) and shall without undue delay notify Controller if it becomes aware of any Personal Data Breach unless such Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons.

12.2. The Processor shall provide the Controller with all reasonable assistance to comply with the notification of Personal Data Breach to Supervisory Authority and/or the Data Subject, to identify the cause of such Data Breach and take such commercially reasonable steps as reasonably required to mitigate and remedy such Data Breach.

12.3. No Acknowledgement of Fault by Processor. Processor's notification of or response to a Personal Data Breach under this DPA will not be construed as an acknowledgement by Processor of any fault or liability with respect to the data incident.

13. **Return and Deletion of Personal Data**

13.1. The Processor shall at least thirty (30) days from the end of the Agreement or cessation of the Processor's Services under the Agreement, whichever occurs earlier, shall return to the Controller all the Personal Data, or if the Controller so instructs, the Processor shall have the Personal Data deleted. The Processor shall return such Personal Data in a commonly used format or in the current format in which it was stored at discretion of the Controller, soon as reasonably practicable following receipt of Controller's notification.

13.2. In any case, the Processor shall delete Personal Data including all the copies of it as soon as reasonably practicable following the end of the Agreement.

14. **Technical and Organizational Measures**

Having regard to the state of technological development and the cost of implementing any measures, the Processor will take appropriate technical and organizational measures against the unauthorized or unlawful processing of Personal Data and against the accidental loss or destruction of, or damage to, Personal Data to ensure a level of security appropriate to: (a) the harm that might result from

unauthorized or unlawful processing or accidental loss, destruction or damage; and (b) the nature of the data to be protected [including the measures stated in Annex II of Schedule 1]

SCHEDULE 1

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name : **Customer (As set forth in the relevant Order Form).**

Address: **As set forth in the relevant Order Form.**

Contact person's name, position, and contact details: **As set forth in the relevant Order Form.**

Activities relevant to the data transferred under these Clauses: **Recipient of the Services provided by OTPless in accordance with the Agreement.**

Signature and date: **Signature and date are set out in the Agreement.**

Role Controller/ Processor): ***Controller***

Data importer(s):

Name: ***OTPless***

Address:1101, Rajhans Bonista, Old Ghod Dod Rd, Ram Chowk, Adarsh Society, Athwa, Surat, Gujarat 395001

Contact person's name, position, and contact details: *help@otpless.com*

Activities relevant to the data transferred under these Clauses: **Provision of the Services to the Customer in accordance with the Agreement.**

Signature and date: **Signature and date are set out in the Agreement.**

Role (controller/processor): ***Processor.***

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customer's authorized users of the Services.

Categories of personal data transferred

Email, Phone, Username.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No sensitive data collected.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

Continuous basis

Nature of the processing
Collection, storage, organization, structuring, use, access, transmission, hosting, and deletion of personal data in order to provide the Services

Purpose(s) of the data transfer and further processing

The purpose of the transfer is to facilitate the performance of the Services more fully described in the Agreement and accompanying order forms.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The period for which the Customer Personal Data will be retained is more fully described in the Agreement, Addendum, and accompanying order forms.

For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing

The subject matter, nature, and duration of the Processing more fully described in the Agreement, Addendum, and accompanying order forms.

C.COMPETENT SUPERVISORY AUTHORITY

Data exporter is established in an EEA country.

The competent supervisory authority is ***as determined by application of Clause 13 of the EU SCCs.***

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational security measures implemented by OTPless as the data processor/data importer to ensure an appropriate level of security, taking into account the nature, scope, context, and purpose of the processing, and the risks for the rights and freedoms of natural persons.

- **Security**

  - **Security Management System**.
    - **Organization**. OTPless designates qualified security personnel whose responsibilities include development, implementation, and ongoing maintenance of the Information Security Program.
    - **Policies**. Management reviews and supports all security related policies to ensure the security, availability, integrity and confidentiality of Customer Personal Data. These policies are updated at least once annually.
    - **Assessments**. OTPless engages a reputable independent third-party to perform risk assessments of all systems containing Customer Personal Data at least once annually.
    - **Risk Treatment**. OTPless maintains a formal and effective risk treatment program that includes penetration testing, vulnerability management and patch management to identify and protect against potential threats to the security, integrity or confidentiality of Customer Personal Data.
    - **Vendor Management**. OTPless maintains an effective vendor management program
    - **Incident Management**. OTPless reviews security incidents regularly, including effective determination of root cause and corrective action.
    - **Standards**. OTPless operates an information security management system that complies with the requirements of ISO/IEC 27001:2022 standard.
  - **Personnel Security.**
    - OTPless personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. OTPless conducts reasonably appropriate background checks on any employees who will have access to client data under this Agreement, including in relation to employment history and criminal records, to the extent legally permissible and in accordance with applicable local labor law, customary practice and statutory regulations.
    - Personnel are required to execute a confidentiality agreement in writing at the time of hire and to protect Customer Personal Data at all times. Personnel must acknowledge receipt of, and compliance with, OTPless's confidentiality, privacy and security policies. Personnel are provided with privacy and security training on how to implement and comply with the Information Security Program. Personnel handling Customer Personal Data are required to complete additional

requirements appropriate to their role (e.g., certifications). OTPless's personnel will not process Customer Personal Data without authorization.

- **Access Controls**
  - **Access Management**. OTPless maintains a formal access management process for the request, review, approval and provisioning of all personnel with access to Customer Personal Data to limit access to Customer Personal Data and systems storing, accessing or transmitting Customer Personal Data to properly authorized persons having a need for such access. Access reviews are conducted periodically to ensure that only those personnel with access to Customer Personal Data still require it.
  - **Infrastructure Security Personnel**. OTPless has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. OTPless's infrastructure security personnel are responsible for the ongoing monitoring of OTPless's security infrastructure, the review of the Services, and for responding to security incidents.
  - **Access Control and Privilege Management**. OTPless's and Customer's administrators and end users must authenticate themselves via a Multi-Factor authentication system or via a single sign on system in order to use the Services
  - **Internal Data Access Processes and Policies – Access Policy**. OTPless's internal data access processes and policies are designed to protect against unauthorized access, use, disclosure, alteration or destruction of Customer Personal Data. OTPless designs its systems to only allow authorized persons to access data they are authorized to access based on principles of "least privileged" and "need to know", and to prevent others who should not have access from obtaining access. OTPless requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; a need to know basis; and must be in accordance with OTPless's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies follow industry standard practices. These standards include password complexity, password expiry, password lockout, restrictions on password reuse and re-prompt for password after a period of inactivity
- **Data Center and Network Security**
  - **Data Centers.**
    - **Infrastructure.** OTPless has AWS as its data center.
    - **Resiliency.** Multi Availability Zones are enabled on AWS and OTPless conducts Backup Restoration Testing on regular basis to ensure resiliency.
    - **Server Operating Systems.** OTPless's servers are customized for the application environment and the servers have been hardened for the security of the Services. OTPless employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

- **Disaster Recovery**. OTPless replicates data over multiple systems to help to protect against accidental destruction or loss. OTPless has designed and regularly plans and tests its disaster recovery programs.
- **Security Logs.** OTPless's systems have logging enabled to their respective system log facility in order to support the security audits, and monitor and detect actual and attempted attacks on, or intrusions into, OTPless's systems.
- **Vulnerability Management.** OTPless performs regular vulnerability scans on all infrastructure components of its production and development environment. Vulnerabilities are remediated on a risk basis, with Critical, High and Medium security patches for all components installed as soon as commercially possible.

- **Networks and Transmission.**
  - **Data Transmission**. Transmissions on production environment are transmitted via Internet standard protocols.
  - **External Attack Surface**. AWS Security Group which is equivalent to virtual firewall is in place for Production environment on AWS.
  - **Incident Response**. OTPless maintains incident management policies and procedures, including detailed security incident escalation procedures. OTPless monitors a variety of communication channels for security incidents, and OTPless's security personnel will react promptly to suspected or known incidents, mitigate harmful effects of such security incidents, and document such security incidents and their outcomes.
  - **Encryption Technologies**. OTPless makes HTTPS encryption (also referred to as SSL or TLS) available for data in transit.
- **Data Storage, Isolation, Authentication, and Destruction.** OTPless stores data in a multi-tenant environment on AWS servers. Data, the Services database and file system architecture are replicated between multiple availability zones on AWS. OTPless logically isolates the data of different customers. A central authentication system is used across all Services to increase uniform security of data. OTPless ensures secure disposal of Client Data through the use of a series of data destruction processes.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorized the use of the following sub-processors:

Name of Sub- Processor	Description of Processing	Location of Other Processor
Amazon Web Services	Hosting the Production Environment	Mumbai
Sentry	Monitoring (Self hosted)	Hosted in aws in our vpc (Mumbai)
Sendgrid	Email	United States

Version	1.0
Effective Date	16-dec-2025
Last Updated	16-dec-2025