Data Processing Agreement

Version 1.0 · Effective 4 November 2026

Schedule 1 — Data Processing Agreement
Pursuant to Article 28 of Regulation (EU) 2016/679 (GDPR). Incorporated into and forming part of the Server Service Agreement between OTPBLUE SL and the Client.

This Data Processing Agreement (**"DPA"**) forms Schedule 1 to the Server Service Agreement (the **"Agreement"**) between **OTPBLUE SL, registration number B23828593**, with its registered address at Camino del Faro, nº 18, Planta 0, Puerta 23, BW, 03540 Alicante, Spain (**"Company"**, **"Processor"**) and the Client identified in the Agreement (**"Client"**, **"Controller"**). This DPA is effective from the Effective Date of the Agreement and is incorporated into it by reference.

In the event of any conflict between this DPA and the Agreement, the terms of this DPA shall prevail with respect to the processing of Personal Data.

1. Definitions

For the purposes of this DPA, the following terms shall have the meanings set out below. Capitalised terms not defined here have the meanings given in the Agreement.

Term	Definition
GDPR	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.
Personal Data	Any information relating to an identified or identifiable natural person (Data Subject), as defined in Article 4(1) GDPR.
Processing	Any operation or set of operations performed on Personal Data, as defined in Article 4(2) GDPR.
Controller	The Client, who determines the purposes and means of the processing of Personal Data.
Processor	The Company (OTPBLUE SL), who processes Personal Data on behalf of the Controller.
Sub-processor	Any third party engaged by the Processor to process Personal Data on behalf of the Controller.
Data Subject	The natural person to whom Personal Data relates (i.e., the end user whose phone number is submitted for verification).
Supervisory Authority	The competent data protection authority having jurisdiction over the Controller or Processor.
Security Incident	Any confirmed breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.
SCCs	Standard Contractual Clauses adopted by the European Commission pursuant to Article 46(2)(c) GDPR for the transfer of personal data to third countries.

2. Subject Matter and Roles

2.1 The Processor provides verification orchestration services to the Controller under the Agreement, which involves the processing of Personal Data (primarily telephone numbers of the Controller's end users) for the purpose of delivering one-time passcodes (OTPs) through the optimal available channel.

2.2 The Controller acts as data controller and determines the purposes and means of processing Personal Data submitted to the Services.

2.3 The Processor acts as data processor and processes Personal Data solely on behalf of and under the instructions of the Controller, in accordance with this DPA and the Agreement.

2.4 The details of the processing activities governed by this DPA are set out in Annex A (Details of Processing).

3. Processor Obligations

3.1 Processing on Instructions Only

The Processor shall process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to third countries, unless required to do so by applicable law. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless prohibited by law on grounds of public interest.

3.2 Confidentiality

The Processor shall ensure that persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.3 Security

The Processor shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate the measures referred to in Article 32(1) GDPR. The specific measures implemented are described in **Annex B** (Technical and Organisational Measures).

3.4 Sub-processing

3.4.1 The Processor shall not engage a Sub-processor without the prior written authorisation of the Controller, except as set out in this DPA.

3.4.2 The Controller hereby provides general written authorisation for the Processor to engage the Sub-processors listed in **Annex C**. The Processor shall notify the Controller of any intended changes to the list of Sub-processors (additions or replacements) by email to the Controller's designated contact at least **fourteen (14) days** before the change takes effect, giving the Controller the opportunity to object to such changes.

3.4.3 Where the Controller objects to a new Sub-processor on reasonable grounds related to data protection, the Processor shall use commercially reasonable efforts to make available a change to the Services to avoid the transfer of Personal Data to the objecting Sub-processor. If no such change is commercially feasible, either party may terminate the Agreement on thirty (30) days' written notice without penalty.

3.4.4 Where the Processor engages a Sub-processor, it shall impose data protection obligations on that Sub-processor equivalent to those set out in this DPA.

3.5 Data Subject Rights

The Processor shall, taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as possible, in fulfilling the Controller's obligation to respond to requests from Data Subjects exercising their rights under Chapter III of the GDPR (including rights of access, rectification, erasure, restriction, portability, and objection). The Processor shall forward any Data Subject request received directly to the Controller without undue delay.

3.6 Assistance with Compliance Obligations

The Processor shall assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR (security, breach notification, data protection impact assessments, and prior consultation), taking into account the nature of processing and the information available to the Processor.

3.7 Security Incident Notification

In the event of a Security Incident affecting Personal Data processed under this DPA, the Processor shall notify the Controller **without undue delay and in any event within 72 hours** of

becoming aware of the incident. Such notification shall include, to the extent available: (a) a description of the nature of the Security Incident; (b) the categories and approximate number of Data Subjects concerned; (c) the categories and approximate number of Personal Data records concerned; (d) the likely consequences of the Security Incident; and (e) the measures taken or proposed to address the Security Incident.

The Processor shall also cooperate with the Controller and take such reasonable steps as are directed by the Controller to assist in the investigation, mitigation, and remediation of the Security Incident.

3.8 Deletion or Return of Data

Upon termination or expiry of the Agreement, the Processor shall, at the choice of the Controller: (a) delete or destroy all Personal Data processed on behalf of the Controller; or (b) return all Personal Data to the Controller. The Processor shall delete or destroy existing copies unless storage is required by applicable law. Where an active billing dispute is outstanding at the time of termination, relevant metering and metadata records shall be retained until resolution of such dispute, and then deleted.

3.9 Audit and Demonstration of Compliance

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller. The Controller shall provide reasonable prior written notice of at least thirty (30) days for any audit and shall conduct audits no more than once per calendar year, except where a Security Incident has occurred. Audits shall be conducted at the Controller’s expense and shall not unreasonably disrupt the Processor’s business operations.

4. Controller Obligations

4.1 The Controller warrants that it has a valid legal basis under applicable data protection law for the collection and submission of Personal Data to the Services, including obtaining all necessary consents from end users where required.

4.2 The Controller is solely responsible for providing all required privacy notices to Data Subjects and for ensuring the accuracy and lawfulness of Personal Data submitted to the

Processor.

4.3 The Controller shall not submit to the Services any special categories of Personal Data as defined in Article 9 GDPR (including health data, biometric data, or data revealing racial or ethnic origin) unless expressly agreed in writing by the Processor.

4.4 The Controller shall ensure that instructions given to the Processor comply with applicable data protection laws.

5. International Data Transfers

5.1 Personal Data shall not be transferred to a country outside the European Economic Area (EEA) or a country without an adequacy decision from the European Commission, except where: (a) appropriate safeguards are in place pursuant to Article 46 GDPR; or (b) a derogation applies pursuant to Article 49 GDPR.

5.2 Where Personal Data is transferred outside the EEA in connection with the provision of the Services (including to Sub-processors), the Processor shall implement the applicable transfer mechanism set out in **Annex D** (Transfer Mechanisms).

5.3 The Processor shall promptly notify the Controller if it becomes aware that a transfer mechanism relied upon under this DPA is no longer valid or has been invalidated by a competent authority.

6. Data Protection Impact Assessments

Where the Controller is required to carry out a data protection impact assessment (DPIA) pursuant to Article 35 GDPR in relation to the processing activities governed by this DPA, the Processor shall provide reasonable cooperation and assistance upon request, including by making available relevant information about the technical and organisational measures implemented.

7. Liability

7.1 Each party's liability under this DPA shall be subject to the liability limitations and exclusions set out in the Agreement, to the maximum extent permitted by applicable law.

7.2 Nothing in this DPA shall limit or exclude either party's liability to the extent that it cannot be limited or excluded by applicable law, including under GDPR.

8. Term

This DPA shall enter into force on the Effective Date of the Agreement and shall remain in effect for as long as the Processor processes Personal Data on behalf of the Controller pursuant to the Agreement. Sections 3.8 (Deletion or Return of Data) and 3.9 (Audit) shall survive termination of this DPA.

9. Governing Law

This DPA shall be governed by the laws of England and Wales, consistent with the Agreement. Notwithstanding the foregoing, the parties acknowledge that GDPR applies to the processing activities described herein regardless of the governing law of this DPA, and nothing in this clause shall be construed to limit either party's obligations under GDPR.

Note: This is OTP Blue's standard Data Processing Agreement (Schedule 1), incorporated into OTP Blue customer agreements. The copy signed by the parties forms part of each contract.

Annex A — Details of Processing

Processing Details	
Subject matter	Provision of multi-channel OTP verification orchestration services via API, including phone number lookup, channel routing, and one-time passcode delivery.
Duration	For the duration of the Agreement and until all Personal Data is deleted or returned pursuant to Section 3.8.
Nature of processing	Collection, storage, use, disclosure (to Sub-processors/carriers), and deletion of Personal Data as required to deliver the Services.
Purpose of processing	Delivering one-time passcodes (OTPs) to end users via the optimal available channel (SMS, messaging applications, or other) on behalf of the Controller; fraud prevention; billing; service security.
Categories of Personal Data	Telephone numbers (including national and international format); message delivery metadata (timestamps, delivery status codes); IP addresses and API authentication logs (where technically necessary).
Categories of Data Subjects	Natural persons (end users of the Controller's digital products) whose telephone numbers are submitted to the Services for the purpose of identity verification or authentication.
Special categories of data	None. The Controller shall not submit special categories of Personal Data as defined in Article 9 GDPR.
Retention periods	Message metadata: up to 90 days from creation (extended for duration of any active billing dispute). Technical and security logs: up to 12 months. Billing data: as required by applicable law.

Annex B — Technical and Organisational Measures (TOMs)

OTPBLUE SL implements and maintains the following technical and organisational measures to ensure an appropriate level of security for the Personal Data processed under this DPA:

B.1 Access Control

- Role-based access controls (RBAC) limiting access to Personal Data to authorised personnel only.
- Multi-factor authentication (MFA) required for access to production systems.
- API key-based authentication for all client integrations; keys are hashed at rest.
- Quarterly access reviews to verify the principle of least privilege.

B.2 Encryption

- All Personal Data in transit encrypted using TLS 1.2 or higher.
- Personal Data at rest encrypted using AES-256 or equivalent standard.
- API keys and credentials stored using industry-standard secure hashing.

B.3 Network and Infrastructure Security

- Firewalls, intrusion detection, and rate-limiting applied to all production infrastructure.
- Network segmentation between production, staging, and internal systems.
- Regular vulnerability scanning and patching of infrastructure.

B.4 Physical Security

- Personal Data processed in data centres with physical access controls, CCTV, and environmental protections operated by certified cloud infrastructure providers (see Annex C).

B.5 Incident Management

- Security incident response procedure in place including detection, containment, investigation, notification, and post-incident review.
- Security Incidents affecting Personal Data reported to the Controller within 72 hours of detection.

B.6 Organisational Measures

- Confidentiality agreements in place with all personnel having access to Personal Data.
- Data protection training provided to relevant personnel.

- Data minimisation practices: only Personal Data strictly necessary for the Services is processed.

B.7 Availability and Business Continuity

- Redundant infrastructure and automated failover to maintain service availability.
- Regular backups of configuration and operational data.

Annex C — Approved Sub-processors

The Controller hereby provides general authorisation for the use of the following Sub-processors. The Processor shall notify the Controller of any changes (additions or replacements) at least **14 days** in advance pursuant to Section 3.4.2.

Sub-processor	Role	Location	Transfer Mechanism
Cloud infrastructure provider	Infrastructure hosting, data storage	EU (primary)	Adequacy / SCCs
Telecom carrier partners	SMS and voice delivery	Various (global)	SCCs / Adequacy
Messaging channel providers	OTT channel delivery	Various (global)	SCCs

Note: The specific identities of telecom carrier partners and messaging channel providers may vary by destination country and routing configuration. An up-to-date list of active Sub-processors is available upon written request to privacy@otpblue.es.

Annex D — Transfer Mechanisms

Where Personal Data is transferred outside the EEA in connection with the provision of the Services, the following transfer mechanisms apply:

Transfer scenario	Mechanism	Notes
Transfer to cloud infrastructure provider	EU adequacy / SCCs (Module 2: Controller to Processor)	Where infrastructure is hosted outside the EEA, SCCs are incorporated by reference.
Transfer to telecom carrier partners	SCCs (Module 2 or 3 as applicable) / Adequacy where available	Phone numbers are transmitted only to the extent necessary for routing and delivery.
Transfer to messaging platform providers	SCCs (Module 2)	Applicable where provider infrastructure is located outside EEA.

The Processor shall, upon the Controller's reasonable request, provide copies of or references to the applicable SCCs in place with Sub-processors for transfers outside the EEA. Where a previously relied-upon transfer mechanism is invalidated, the Processor shall notify the Controller without undue delay and cooperate to implement an alternative valid mechanism.

— End of Schedule 1 —