SWYTCH MOBILE LTD

DATA PROCESSING AGREEMENT

Version 2.3
Originally effective: 6 March 2023
Last updated: 3 February 2025

This Data Processing Agreement ("DPA") forms part of the agreement between Swytch Mobile Ltd. ("Swytch") and the customer entity entering into an agreement for the use of Swytch services ("Customer").

This DPA reflects the parties' agreement with respect to the processing of Personal Data in accordance with applicable Data Protection Laws, including the UK GDPR and, where applicable, the EU GDPR.

1. Parties

Swytch (Processor)

Legal name: Swytch Mobile Ltd
Incorporated: England and Wales (private limited company)
Company number: 08965691
Registered office: 47 Dean Street, London, W1D 5BE, United Kingdom
Privacy contact: privacy@swytch.com

Customer (Controller)

The entity using the Services and acting as Controller of Customer Personal Data to the extent applicable under Applicable Data Protection Laws.

2. Definitions

For the purposes of this DPA:

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.
"Processor" means the entity which Processes Personal Data on behalf of the Controller.

“Personal Data” means any information relating to an identified or identifiable natural person.

“Processing” means any operation performed on Personal Data, whether or not by automated means.

“Subprocessor” means any third party engaged by Swytch to Process Personal Data on behalf of the Customer.

“Services” means the telecommunications applications, dashboard, mobile services, and related functionality provided by Swytch.

“Applicable Data Protection Laws” means all laws and regulations applicable to the Processing of Personal Data under this DPA, including the UK GDPR, EU GDPR (where applicable), the UK Data Protection Act 2018, and the Privacy and Electronic Communications Regulations 2003 (PECR) as applicable.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

3. Scope and Roles

The parties acknowledge and agree that:

(a) to the extent Swytch Processes Personal Data on behalf of the Customer in connection with the Services, the Customer acts as Controller and Swytch acts as Processor for the purposes of Applicable Data Protection Laws; and

(b) Swytch may also act as an independent Controller for certain Processing activities required for the operation, security, maintenance, improvement, legal compliance, fraud prevention, accounting, billing, or protection of the Services.

4. Processing of Personal Data

Swytch shall:

(c) Process Customer Personal Data only on documented instructions from the Customer, unless otherwise required by applicable law;

(d) ensure that persons authorised to Process Personal Data are subject to appropriate confidentiality obligations;

(e) implement appropriate technical and organisational measures to protect Customer Personal Data, in accordance with Article 32 of the UK GDPR;

(f) assist the Customer, taking into account the nature of the Processing, in responding to requests from data subjects exercising their rights under Applicable Data Protection Laws;

(g) notify the Customer without undue delay, and in any event no later than 48 hours, after becoming aware of a reasonably suspected Personal Data Breach affecting Customer Personal Data, providing sufficient information to allow the Customer to meet its obligations under Applicable Data Protection Laws;

(h) make available information reasonably necessary to demonstrate compliance with this DPA; and

(i) assist the Customer in ensuring compliance with the obligations set out in Articles 32 to 36 of the UK GDPR, including in relation to security, breach notification, and, where requested, Data Protection Impact Assessments, taking into account the nature of Processing and the information available to Swytch.

5. Security Measures

Swytch implements appropriate technical and organisational measures, in accordance with Article 32 of the UK GDPR, designed to ensure a level of security appropriate to the risk. Such measures include, but are not limited to:

- Encryption of data in transit and at rest, leveraging the encryption capabilities provided by Swytch's cloud infrastructure provider (Amazon Web Services), which maintains its own independently certified encryption standards;
- Access controls and authentication measures applied to systems handling Customer Personal Data, with access restricted to authorised personnel on a need-to-know basis;
- Restricted access on a need-to-know basis, with access rights reviewed periodically;
- Authentication controls and session management procedures;
- Logging, monitoring, and alerting on system access and anomalous activity;
- Secure cloud hosting infrastructure provided by AWS, subject to AWS's own security certifications (including ISO 27001 and SOC 2);
- Vulnerability management procedures, including regular security patching and periodic penetration testing;
- Incident detection and response procedures;
- Backup and recovery processes with tested restoration procedures;
- Confidentiality obligations for all personnel with access to Customer Personal Data.

Swytch reviews and updates its security measures on a regular basis to account for changes in technology and the nature of risks.

6. Communications Data

6.1 Swytch does not access call content as part of the provision of the Services.

6.2 SMS content may be Processed only where technically necessary to provide the Services or to comply with applicable legal obligations, including obligations under PECR and the Investigatory Powers Act 2016.

6.3 Swytch may Process communications metadata, routing information, operational logs, and related telecommunications data as necessary for the provision, security, maintenance, fraud prevention, regulatory compliance, and lawful operation of the Services.

6.4 Where required by applicable law, including under the Data Retention and Acquisition Regulations 2018 (DRAR) or pursuant to a lawful authority notice under the Investigatory

Powers Act 2016, Swytch may retain or disclose communications data to competent law enforcement or regulatory authorities. Swytch will, to the extent permitted by law, inform the Customer of any such request.

7. Subprocessors

7.1 The Customer authorises Swytch to engage Subprocessors in connection with the provision of the Services.

7.2 Swytch shall ensure that any Subprocessor is subject to data protection obligations materially equivalent to those set out in this DPA.

7.3 Current Subprocessors and third-party service providers are listed below. Swytch may update or replace Subprocessors from time to time as reasonably necessary for the provision of the Services and will maintain an up-to-date list at privacy@swytch.com upon request.

Provider	Purpose
Amazon Web Services (AWS)	Cloud hosting and backend infrastructure
Cloudflare, Inc.	Network security and content delivery
Webflow, Inc.	Website hosting and management
Stripe, Inc. / Stripe Payments Europe Ltd.	Payment processing and fraud prevention
Paddle.com Market Limited	Subscription billing and payment services
Google Analytics (GA4)	Website analytics
Google Tag Manager	Website tag management
Meta/Facebook Pixel	Marketing analytics and advertising attribution
LinkedIn Insight Tag	Marketing analytics and advertising attribution
Hotjar Ltd.	Website usage analytics
Cybot A/S (Cookiebot)	Cookie consent management
Firebase Analytics	Mobile and application analytics
Firebase Crashlytics	Application crash reporting and diagnostics
Ziron Limited (a TelcoSwitch Group company)	Telecommunications infrastructure
Tango Networks UK Ltd.	Telecommunications infrastructure
X-Mobility Ltd	Telecommunications infrastructure
Hutchison 3G UK Limited (Three UK)	Telecommunications infrastructure
SMTP.com (j2 Global Canada, Inc.)	Transactional email infrastructure
Help Scout, Inc.	Customer support platform

8. International Data Transfers

8.1 Certain Customer Personal Data may be Processed outside the United Kingdom or European Economic Area by Swytch or its authorised Subprocessors.

8.2 Where Customer Personal Data is transferred outside the United Kingdom or EEA, Swytch shall implement appropriate safeguards in accordance with Applicable Data Protection Laws, which may include:

- adequacy regulations or adequacy decisions recognised by the ICO or European Commission;
- the UK International Data Transfer Addendum (IDTA) to the Standard Contractual Clauses;
- the European Commission Standard Contractual Clauses (SCCs); or
- such other lawful transfer mechanisms as are recognised under Applicable Data Protection Laws from time to time.

9. Retention and Deletion

9.1 Customer Personal Data will be retained for the duration of the provision of the Services.

9.2 Upon termination of the Services or following a valid deletion request, Swytch will delete or anonymise Customer Personal Data within 30 days, unless retention is required by applicable law or reasonably necessary for legitimate business purposes, including fraud prevention, security, dispute resolution, accounting, enforcement of agreements, or telecommunications regulatory compliance obligations (including obligations under the Data Retention and Acquisition Regulations 2018).

9.3 Backup copies of Customer Personal Data may remain in secure archival systems for up to 90 days following deletion or anonymisation of live data, until overwritten or expired in accordance with Swytch's backup retention procedures, after which they will be deleted.

10. Audit Rights

10.1 Upon reasonable written request, Swytch shall make available information reasonably necessary to demonstrate compliance with this DPA.

10.2 Any audit or inspection requested by the Customer shall:

(j) be subject to reasonable advance written notice of no less than 30 days;

(k) occur no more than once per calendar year, unless required by a supervisory authority or following a confirmed security incident;

(l) be conducted during normal business hours and in a manner that avoids unreasonable disruption to Swytch's operations; and

(m) remain subject to appropriate confidentiality obligations agreed in advance by the parties.

10.3 Where the Customer requires an audit to be conducted by a third-party auditor, such auditor must be approved in advance by Swytch, such approval not to be unreasonably withheld.

11. Automated Processing and Profiling

11.1 As part of the provision of the Services, Swytch may carry out automated processing activities including fraud detection, usage analysis, network routing optimisation, and communications metadata processing. These activities may involve profiling of usage patterns for the purposes of fraud prevention, security, service integrity, and operational management.

11.2 Where any automated processing activity carried out by Swytch as Processor produces a decision that has a legal or similarly significant effect on an identifiable individual (for example, suspension of access to the Services), Swytch shall, to the extent technically and operationally feasible, provide the Customer with sufficient information to allow the Customer to fulfil its obligations to affected data subjects under Article 22 of the UK GDPR, including the right to obtain human review of the decision.

11.3 The Customer, as Controller, remains responsible for ensuring that any automated decision-making carried out on its instruction, or using outputs derived from the Services, complies with Applicable Data Protection Laws, including the provision of appropriate notices to data subjects and, where required, the facilitation of data subject rights under Article 22 of the UK GDPR.

12. Customer Responsibilities

The Customer remains responsible for:

(n) ensuring that it has a lawful basis for the Processing of Personal Data under Applicable Data Protection Laws;

(o) providing appropriate privacy notices to data subjects;

(p) obtaining any required consents prior to instructing Swytch to Process Personal Data; and

(q) ensuring that its instructions to Swytch regarding the Processing of Personal Data comply with Applicable Data Protection Laws.

13. Governing Law

13.1 This DPA shall be governed by and construed in accordance with the laws of England and Wales.

13.2 The courts of England and Wales shall have exclusive jurisdiction over any dispute arising out of or in connection with this DPA.

ANNEX I – Categories of Data

Version 2.3 | Last updated: 3 February 2025

Categories of Data Subjects

- Customer employees and authorised users;
- customer contacts communicated with through the Services;
- billing and account contacts; and
- support contacts.

Categories of Personal Data

- names;
- email addresses;
- telephone numbers;
- account credentials and account identifiers;
- device information;
- billing and payment information;
- contact book information voluntarily synced by users;
- communications metadata and routing information;
- support communications; and
- fraud prevention and security information.

Nature and Purpose of Processing

Swytch Processes Personal Data for the purpose of providing telecommunications services, mobile applications, dashboard functionality, customer support, billing, fraud prevention, security, analytics, and operational maintenance, in accordance with this DPA and Applicable Data Protection Laws.

Duration of Processing

For the duration of the Services agreement, subject to Section 9 of this DPA.

ANNEX II – Technical and Organisational Security Measures

Version 2.3 | Last updated: 3 February 2025

The following measures represent Swytch's current technical and organisational security baseline, implemented in accordance with Article 32 of the UK GDPR. Measures are reviewed and updated on a regular basis.

1. Encryption

- Data in transit: encrypted using protocols provided and maintained by Swytch's cloud infrastructure (AWS), which supports current industry-standard transport encryption;
- Data at rest: encrypted using AWS infrastructure-level encryption, which is applied by default across Swytch's cloud storage and database services;
- Encryption key management maintained through AWS Key Management Service (KMS).

2. Access Controls

- Access controls applied across systems handling Customer Personal Data, with access granted to authorised personnel only and provisioned on a need-to-know basis;
- Authentication controls applied to system access, with stronger authentication measures planned for implementation across production and administrative systems;
- Access provisioned on a minimum-necessary (least privilege) basis;
- Access rights reviewed periodically and revoked promptly upon role change or departure.

3. Network and Infrastructure Security

- Hosted on Amazon Web Services (AWS) infrastructure, benefiting from AWS's ISO 27001, SOC 1, SOC 2, and SOC 3 certifications;
- Network traffic filtered through Cloudflare for DDoS protection and content delivery security;
- Firewall rules and network segmentation applied to limit exposure of internal systems;
- Intrusion detection and monitoring controls in place.

4. Vulnerability and Patch Management

- Security patches applied on a regular basis and tracked through a vulnerability management process;
- Periodic penetration testing conducted by qualified third parties;
- Internal security reviews conducted following significant infrastructure or application changes.

5. Monitoring and Logging

- System access, administrative actions, and anomalous activity are logged and monitored;

- Security alerts are triaged and responded to in accordance with Swytch's incident response procedures;
- Logs retained for a defined period in accordance with applicable legal and operational requirements.

6. Incident Response

- A documented incident response procedure is maintained and tested periodically;
- Confirmed or reasonably suspected Personal Data Breaches are escalated and notified in accordance with Section 4(e) of this DPA;
- Post-incident reviews are conducted to identify root cause and prevent recurrence.

7. Backup and Recovery

- Customer Personal Data is backed up on a regular basis;
- Backup restoration is tested periodically to validate recovery procedures;
- Backups are stored securely and subject to the same access controls as live data.

8. Personnel and Confidentiality

- All personnel with access to Customer Personal Data are subject to written confidentiality obligations;
- Staff receive data protection awareness training appropriate to their role;
- Third-party contractors with access to Customer Personal Data are subject to equivalent obligations.

Privacy Contact

Questions or requests regarding this DPA, data subject rights, or data protection matters should be directed to:

Email: privacy@swytch.com
Post: Swytch Mobile Ltd, 47 Dean Street, London, W1D 5BE, United Kingdom
Website: https://www.swytch.com

Swytch will acknowledge all valid data protection enquiries within 5 business days.