DATA PROCESSING AGREEMENT

Between the Controller and MOBIROX LLP

Effective Date: March 6, 2026

Last Updated: March 2026 | Version 1.0

MOBIROX LLP
Stoney Works, 8 Stoney Lane
London, SE1 9BD
United Kingdom

1. PARTIES

Data Controller (“Controller”):
The entity identified in the applicable Service Agreement that uses the Services provided by the Processor.

Data Processor (“Processor”):
MOBIROX LLP, a limited liability partnership registered in England and Wales, with registered address at Stoney Works, 8 Stoney Lane, London, United Kingdom, SE1 9BD, operating the platform at mobileproxy.space (“Services”).

This Data Processing Agreement (“DPA”) forms part of the Service Agreement between the Controller and the Processor and shall take precedence over conflicting terms in the Service Agreement with respect to data protection matters.

---

2. DEFINITIONS

“Personal Data” means any information relating to an identified or identifiable natural person, as defined in Article 4(1) of the GDPR.

“Processing” means any operation performed on Personal Data, as defined in Article 4(2) of the GDPR.

“GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).

“UK GDPR” means the GDPR as incorporated into United Kingdom law by virtue of the Data Protection Act 2018 and the European Union (Withdrawal) Act 2018.

“CCPA” means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (CPRA).

“Data Protection Laws” means the GDPR, the UK GDPR, the CCPA, and any other applicable data protection and privacy legislation in force from time to time in any relevant jurisdiction.

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

“Sub-processor” means any third party appointed by the Processor to process Personal Data on behalf of the Controller.

“Services” means the mobile and server proxy services, browser extensions, API access, and related tools provided by the Processor via the mobileproxy.space platform.

“Standard Contractual Clauses” or “SCCs” means the standard contractual clauses approved by the European Commission for the transfer of Personal Data to third countries.

---

3. SCOPE AND PURPOSE OF PROCESSING

3.1 Subject Matter

The Processor provides mobile and static proxy infrastructure services. In the course of providing these Services, the Processor processes certain Personal Data on behalf of the Controller.

3.2 Purpose of Processing

Personal Data is processed solely for the purpose of providing the Services to the Controller, including:

- Routing network traffic through proxy channels assigned to the Controller;
- Authenticating the Controller's access to proxy services;
- Maintaining connection logs for service quality, troubleshooting, and security purposes;
- Providing technical support related to the Services;
- Billing and payment processing.

3.3 Duration of Processing

Processing shall continue for the duration of the Service Agreement between the parties, plus any retention period specified in Section 8 of this DPA.

---

4. CATEGORIES OF DATA AND DATA SUBJECTS

4.1 Categories of Personal Data Processed

Category	Description	Legal Basis
Client IP addresses	IP addresses used for proxy authentication (IP-based authorisation)	Contractual necessity
Connection logs	Timestamps, session duration, assigned proxy IP, connection metadata	Legitimate interest (security, service quality)
Proxy credentials	Login and password pairs generated for proxy access	Contractual necessity
Account data	Email address, payment information, billing records	Contractual necessity

4.2 Categories of Data Subjects

- Employees, contractors, and agents of the Controller who use the Services;
- Any natural person whose Personal Data is transmitted through the proxy infrastructure by the Controller.

4.3 Data the Processor Does NOT Collect

The Processor does not inspect, store, or log the content of traffic routed through the proxy channels. The Processor acts as a conduit for network traffic and does not access payload data.

---

5. OBLIGATIONS OF THE PROCESSOR

5.1 Lawful Processing

(a) The Processor shall process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country, unless required to do so by applicable law.

(b) The Processor shall immediately inform the Controller if, in the Processor's opinion, an instruction from the Controller infringes Data Protection Laws.

5.2 Confidentiality

(a) 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.

(b) The Processor shall limit access to Personal Data to personnel who require such access for the performance of the Services.

5.3 Security Measures

The Processor shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:

- (a) Encryption of Personal Data in transit using TLS/SSL;
- (b) Access controls and authentication mechanisms for systems storing Personal Data;
- (c) Regular security assessments and vulnerability testing;
- (d) Logging of administrative access to systems containing Personal Data;
- (e) Procedures for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures;
- (f) Physical security measures for server and modem farm infrastructure.

A summary of current technical and organisational measures is set out in Annex B.

5.4 Sub-processing

(a) The Controller provides general authorisation for the Processor to engage Sub-processors, subject to the conditions in this Section.

(b) The Processor shall maintain an up-to-date list of Sub-processors, available upon request and published at Annex C of this DPA.

(c) The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Sub-processors, giving the Controller at least **30 days** to object.

(d) If the Controller objects to a new Sub-processor on reasonable grounds relating to data protection, the parties shall discuss the objection in good faith. If the matter cannot be resolved within 30 days, the Controller may terminate the affected Services without penalty.

(e) The Processor shall impose data protection obligations on each Sub-processor by way of a contract that provides at least the same level of protection as this DPA.

(f) The Processor remains fully liable to the Controller for the performance of each Sub-processor's obligations.

5.5 Data Subject Rights

(a) The Processor shall assist the Controller in fulfilling its obligations to respond to requests from data subjects exercising their rights under Chapter III of the GDPR, including the rights of access, rectification, erasure, restriction, portability, and objection.

(b) The Processor shall promptly notify the Controller if it receives a request from a data subject directly, and shall not respond to such request without the Controller's instructions, unless required by law.

5.6 Data Protection Impact Assessments

The Processor shall provide reasonable assistance to the Controller with data protection impact assessments and prior consultations with supervisory authorities, where required under Articles 35 and 36 of the GDPR.

---

6. DATA BREACH NOTIFICATION

6.1 Notification to Controller

(a) The Processor shall notify the Controller without undue delay, and in any event within **48 hours** of becoming aware of a Data Breach affecting the Controller's Personal Data.

(b) Such notification shall include, to the extent available:

- A description of the nature of the Data Breach, including approximate categories and number of data subjects and records concerned;
- The name and contact details of the Processor's contact point for further information;
- A description of the likely consequences of the Data Breach;
- A description of the measures taken or proposed to address the Data Breach and mitigate its effects.

6.2 Cooperation

The Processor shall cooperate with the Controller and take reasonable steps to assist in the investigation, mitigation, and remediation of each Data Breach.

6.3 Record-Keeping

The Processor shall maintain a record of all Data Breaches, including the facts relating to the breach, its effects, and the remedial action taken.

---

7. INTERNATIONAL DATA TRANSFERS

7.1 Transfer Mechanisms

(a) The Processor operates infrastructure across multiple jurisdictions. Where Personal Data is transferred outside the UK or EEA, the Processor shall ensure that appropriate safeguards are in place in accordance with Chapter V of the GDPR, including:

- Standard Contractual Clauses (SCCs) as approved by the European Commission;

- The UK International Data Transfer Agreement (IDTA) or UK Addendum to the EU SCCs, as applicable;
- Any other lawful transfer mechanism recognised under Data Protection Laws.

(b) The Processor shall, upon request, provide the Controller with information regarding the specific transfer mechanisms in place for each relevant jurisdiction.

7.2 Disclosure Requests from Public Authorities

(a) The Processor shall promptly notify the Controller of any legally binding request from a public authority for disclosure of Personal Data, unless otherwise prohibited by law.

(b) If the Processor receives a request from a law enforcement or government authority regarding the Controller's data, the Processor shall:

- Redirect the authority to the Controller where possible;
- Provide only the minimum amount of data required by law;
- Notify the Controller as soon as legally permitted.

(c) The Processor shall maintain transparency regarding its practices for responding to government data requests.

---

8. DATA RETENTION AND DELETION

8.1 Retention Periods

Data Category	Retention Period	Justification
Connection logs (timestamps, session data, assigned IPs)	**12 months** from date of creation	Security, fraud prevention, service quality, legal obligations
Client IP addresses (authentication records)	Duration of Service Agreement + 30 days	Contractual necessity
Proxy credentials (login/password)	Duration of Service Agreement + 30 days	Contractual necessity
Account data (email, billing)	Duration of Service Agreement + **24 months**	Legal and tax obligations

8.2 Deletion Upon Termination

(a) Upon termination or expiry of the Service Agreement, the Processor shall, at the Controller's written request, either:

- Delete all Personal Data processed on behalf of the Controller; or
- Return all Personal Data to the Controller in a commonly used, machine-readable format.

(b) The Processor shall complete deletion or return within **60 days** of receiving such request.

(c) The Processor may retain Personal Data to the extent required by applicable law (including tax and accounting regulations), provided that such data is archived securely and not actively

processed.

8.3 Certification of Deletion

Upon request, the Processor shall provide written confirmation that Personal Data has been deleted in accordance with this Section.

---

9. AUDIT RIGHTS

9.1 Information and Audit

(a) The Processor shall make available to the Controller all information necessary to demonstrate compliance with this DPA and Data Protection Laws.

(b) The Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or an independent auditor mandated by the Controller, subject to reasonable advance notice of at least **30 days**.

(c) Audits shall be conducted during normal business hours, no more than once per calendar year, and shall not unreasonably interfere with the Processor's operations.

9.2 Costs

The Controller shall bear its own costs of any audit. If an audit reveals a material breach of this DPA by the Processor, the Processor shall bear the reasonable costs of the audit.

---

10. OBLIGATIONS OF THE CONTROLLER

The Controller warrants and represents that:

(a) It has a lawful basis for processing Personal Data and for instructing the Processor to process Personal Data on its behalf;

(b) It has provided all necessary notices to, and obtained all necessary consents from, data subjects as required by Data Protection Laws;

(c) It shall comply with Data Protection Laws in its use of the Services;

(d) It shall not use the Services in a manner that would cause the Processor to violate Data Protection Laws;

(e) Its processing instructions to the Processor shall comply with Data Protection Laws.

---

11. LIABILITY

11.1 Limitation

Each party's liability under this DPA shall be subject to the limitations and exclusions of liability set out in the Service Agreement.

11.2 Indemnification

Each party shall indemnify the other against all costs, claims, damages, and expenses incurred as a result of any breach of this DPA or Data Protection Laws by the indemnifying party.

---

12. TERM AND TERMINATION

12.1 Term

This DPA shall come into effect on the date of signature and shall continue in force for the duration of the Service Agreement.

12.2 Survival

Sections 6 (Data Breach Notification), 8 (Data Retention and Deletion), 9 (Audit Rights), and 11 (Liability) shall survive termination of this DPA.

---

13. GOVERNING LAW AND JURISDICTION

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

Any dispute arising out of or in connection with this DPA shall be subject to the exclusive jurisdiction of the courts of **England and Wales**.

---

14. CONTACT DETAILS

Processor Contact for Data Protection Matters:

Name: Mikhail Zaitsev
Email: law@mobileproxy.space
Address: MOBIROX LLP, Stoney Works, 8 Stoney Lane, London, SE1 9BD, United Kingdom

---

15. SIGNATURES

	Controller	Processor
Name:		
Title:		
Date:		
Signature:		

ANNEX A — Details of Processing

Subject matter	Provision of mobile and static proxy infrastructure services
Duration	Duration of the Service Agreement
Nature of processing	Routing of network traffic, authentication, connection logging, billing
Purpose	Delivery of proxy services as described in the Service Agreement
Categories of data subjects	Controller's employees, contractors, agents; natural persons whose data transits the proxy infrastructure
Categories of personal data	Client IP addresses, connection logs (timestamps, session duration), proxy credentials (login/password), account data (email, payment information)
Special categories of data	None intentionally processed. The Processor does not inspect traffic content.

ANNEX B — Technical and Organisational Measures

The Processor implements the following measures to protect Personal Data:

B.1 Encryption

- All proxy connections support SSL/TLS encryption
- Data in transit between client and proxy infrastructure is encrypted
- Administrative access to systems uses encrypted channels (SSH, HTTPS)

B.2 Access Control

- Role-based access control for internal systems
- Two-factor authentication for administrative access
- Individual user accounts for all personnel with access to Personal Data
- Principle of least privilege applied

B.3 Network Security

- Firewall protection on all servers
- Intrusion detection and monitoring
- Segregation of client proxy channels (one user per channel — no shared access)

B.4 Data Storage

- Connection logs stored in partitioned database tables (monthly partitioning)
- Automated purging of logs exceeding retention period
- Database backups encrypted and access-controlled

B.5 Physical Security

- Server infrastructure hosted in professional data centres with physical access controls
- Modem farm locations secured by farm operators according to Processor's requirements

B.6 Personnel

- All personnel with access to Personal Data bound by confidentiality obligations
- Regular security awareness training

B.7 Incident Response

- Documented incident response procedure
- Breach detection and notification process (48-hour notification to Controller)
- Regular review and testing of incident response plans

B.8 Business Continuity

- 99.9% uptime SLA
- Redundant infrastructure across multiple jurisdictions
- Regular backup procedures

ANNEX C — List of Sub-processors

Sub-processor	Purpose	Location	Data Processed
Third-party modem farm operators	Hosting and operating physical modem equipment connected to the platform	Various locations across 52 countries	Connection metadata (assigned proxy IP, session timestamps)
Dedicated server providers	Server infrastructure hosting	Multiple jurisdictions (EU, US, Asia-Pacific, and others)	Connection logs, account data
FKWallet	Payment processing	EU	Payment data, transaction records
Capitalist	Payment processing	EU	Payment data, transaction records
Volet	Payment processing	EU	Payment data, transaction records

The Controller will be notified of changes to this list at least 30 days in advance via email.

---

16. CHANGES TO THIS DPA

The Processor may update this DPA from time to time to reflect changes in legal requirements, Sub-processors, or processing activities. Material changes will be communicated to the Controller via email at least **30 days** prior to taking effect. Continued use of the Services after such notice constitutes acceptance of the updated DPA.

Last updated: March 2026 | Version 1.0