Data Processing Agreement

Sentinel Edge Networks LTD · Registered in England & Wales 17150600 · Version 1.3 · 2 September 2026 · canonical copy at maskbreak.com/dpa

This Data Processing Agreement (**"DPA"**) forms part of, and is incorporated by reference into, the agreement between the customer (**"Customer"**) and Sentinel Edge Networks LTD (**"Maskbreak"**) under which Maskbreak provides its fraud-detection API and related services (the **"Services"**, and that agreement, the **"Agreement"**, being Maskbreak's Terms of Service or a signed Master Services Agreement). It governs Maskbreak's processing of Customer Personal Data and reflects the parties' obligations under UK GDPR and EU GDPR Article 28.

How to put this in force. This DPA is pre-approved by Maskbreak and takes effect automatically upon your acceptance of the Agreement — no signature is required for it to bind both parties. If your organisation needs a countersigned copy for its records, complete the signature block in Section 16, sign, and return the PDF to support@maskbreak.com; we will countersign and return it. A Standard Contractual Clauses / UK IDTA package for international transfers is available on the same request.

Contents

1. Definitions

Capitalised terms not defined here have the meaning given in the Agreement. **"Data Protection Law"** means all laws applicable to the processing of personal data under the Agreement, including the UK GDPR (as defined in the Data Protection Act 2018), the EU General Data Protection Regulation 2016/679 (**"EU GDPR"**), and any successor or implementing legislation. **"Controller"**, **"Processor"**, **"Data Subject"**, **"Personal Data"**, **"Processing"**, **"Personal Data Breach"**, and **"Supervisory Authority"** have the meanings given in the Data Protection Law. **"Customer Personal Data"** means Personal Data that Maskbreak processes on the Customer's behalf in providing the Services, as described in Annex A. **"Sub-processor"** means any third party engaged by Maskbreak to process Customer Personal Data.

2. Roles & scope of processing

For the Customer Personal Data described in Annex A, the Customer is the Controller (or a Processor acting on behalf of its own Controller) and Maskbreak is the Processor. Where the Customer is itself a Processor, the Customer warrants that it has the necessary authority from the relevant Controller to engage Maskbreak as a Sub-processor on these terms.

Maskbreak is an independent Controller for the limited personal data it collects to operate its business — Customer account data and website/security telemetry — which is governed by Maskbreak's Privacy Policy, not by this DPA. This DPA governs only the end-user data the Customer submits to the Services for evaluation.

The subject matter, duration, nature and purpose of the Processing, the types of Personal Data, and the categories of Data Subjects are set out in Annex A.

3. Customer instructions

Maskbreak shall process Customer Personal Data only on the Customer's documented instructions, including with regard to international transfers, unless required to do otherwise by law — in which case Maskbreak shall inform the Customer of that legal requirement before processing, unless the law prohibits such notice on important grounds of public interest. The Agreement, this DPA, and the Customer's configuration and use of the Services (for example the signals it submits and the rules and exceptions it configures) constitute the Customer's complete documented instructions. Maskbreak shall inform the Customer if, in its opinion, an instruction infringes Data Protection Law.

The Customer is responsible for the lawfulness of the Personal Data it submits and of its instructions, including having a valid lawful basis and providing any notices required to Data Subjects. The Customer must not submit special-category data for evaluation, and Maskbreak does not require or use special-category data to produce risk scores.

4. Confidentiality

Maskbreak shall ensure that persons authorised to process Customer Personal Data are bound by an appropriate obligation of confidentiality (contractual or statutory) and process the data only as instructed. Access is limited to personnel who need it to provide, secure, or support the Services.

5. Security of processing

Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk to Data Subjects, Maskbreak shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as required by Article 32. The measures in force are summarised in Annex B and detailed in the current Security Whitepaper. Maskbreak may update its measures over time provided the level of security is not materially reduced.

6. Sub-processors

The Customer grants Maskbreak general authorisation to engage Sub-processors to process Customer Personal Data, subject to this Section. The current Sub-processors are listed at maskbreak.com/sub-processors and reproduced by reference in Annex C.

Maskbreak shall impose on each Sub-processor, by written contract, data-protection obligations no less protective than those in this DPA, and remains fully liable to the Customer for a Sub-processor's performance of those obligations. Maskbreak shall give the Customer at least **30 days'** prior notice of any intended addition or replacement of a Sub-processor that processes Customer Personal Data — by email where the Customer has subscribed to sub-processor change notices, and by updating the public list with a dated change-log entry. The Customer may object on reasonable data-protection grounds within that period; if the parties cannot resolve the objection, the Customer may terminate the affected Services as its exclusive remedy.

7. Assistance with data-subject rights

Taking into account the nature of the Processing, Maskbreak shall assist the Customer by appropriate technical and organisational measures, insofar as possible, in fulfilling the Customer's obligation to respond to requests from Data Subjects exercising their rights under Chapter III of the GDPR (access, rectification, erasure, restriction, portability, and objection). Because Maskbreak holds Customer Personal Data only in pseudonymised or short-lived form and cannot identify a Data Subject from it alone, the Customer will ordinarily action such requests directly through the Services; where Maskbreak's assistance is nonetheless required, it will be provided without undue delay. If a Data Subject contacts Maskbreak directly regarding Customer Personal Data, Maskbreak shall promptly forward the request to the Customer and not respond substantively except to confirm receipt or as legally required.

8. Personal data breaches

Maskbreak shall notify the Customer without undue delay, and in any case within **72 hours**, after becoming aware of a Personal Data Breach affecting Customer Personal Data. The notification shall describe, to the extent known, the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed to address it. Maskbreak shall reasonably assist the Customer in meeting the Customer's own breach-notification obligations to Supervisory Authorities and Data Subjects. Notification is not, and shall not be construed as, an acknowledgement of fault or liability.

9. DPIAs & prior consultation

Taking into account the nature of the Processing and the information available to Maskbreak, Maskbreak shall provide reasonable assistance to the Customer with any data-protection impact assessments and prior consultations with Supervisory Authorities that the Customer is required to carry out under Articles 35 and 36. The Security Whitepaper and this DPA are intended to supply much of the information a DPIA requires.

10. International transfers

Maskbreak shall not transfer Customer Personal Data outside the UK or the EEA except where an appropriate safeguard under the Data Protection Law is in place. Where Maskbreak or a Sub-processor processes Customer Personal Data in a third country, the transfer is made under one or more of: (a) an adequacy decision; (b) the EU Standard Contractual Clauses (2021/914) and, for UK transfers, the UK International Data Transfer Addendum, which the parties agree to enter into and which are incorporated by reference and available on request; or (c) another lawful transfer mechanism. Maskbreak's primary processing regions and its Sub-processors' locations are described in Annex C.

11. Deletion & return of data

On termination or expiry of the Agreement, Maskbreak shall, at the Customer's choice, delete or return all Customer Personal Data and delete existing copies, unless retention is required by law. Given the nature of the Services, Customer Personal Data is short-lived by design: raw identifiers such as IP addresses are one-way hashed within 7 days, evaluation records are deleted when the account is deleted, and remaining pseudonymous records expire on their documented schedules (see the Privacy Policy and Annex A). Data held in routine encrypted backups is not immediately accessible and is overwritten on the backup rotation cycle (currently 60 days), after which it is unrecoverable; backups are never used to restore data a Customer has deleted.

12. Audits & information

Maskbreak shall make available to the Customer all information reasonably necessary to demonstrate compliance with Article 28 and this DPA, and shall allow for and contribute to audits, including inspections, conducted by the Customer or an auditor it mandates. The parties agree that the current Security Whitepaper, sub-processor list, and responses to the Customer's security questionnaires ordinarily satisfy this obligation. Where the Customer reasonably requires a further audit, it shall be conducted on reasonable prior written notice, no more than once per twelve months (except following a Personal Data Breach or where required by a Supervisory Authority), during business hours, in a manner that does not disrupt the Services, and subject to confidentiality.

13. Liability & precedence

Each party's liability arising out of or related to this DPA is subject to the limitations and exclusions of liability set out in the Agreement, and any reference to a party's liability means the aggregate liability of that party and its affiliates under the Agreement and this DPA together. In the event of any conflict between this DPA and the Agreement in relation to the Processing of Customer Personal Data, this DPA prevails; in the event of a conflict between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses prevail.

14. Term

This DPA takes effect on the effective date of the Agreement and remains in force for as long as Maskbreak processes Customer Personal Data, notwithstanding expiry or termination of the Agreement,

until all such data has been deleted or returned in accordance with Section 11.

15. Governing law

This DPA is governed by the laws of England and Wales, and the parties submit to the exclusive jurisdiction of the courts of England and Wales, except where the Data Protection Law requires otherwise for the protection of Data Subjects.

16. Signatures

This DPA binds the parties on acceptance of the Agreement without signature. The block below is provided only for Customers that require a countersigned copy for their records.

For the Customer (Controller)

SIGNATURE

NAME & TITLE

ORGANISATION

DATE

For Sentinel Edge Networks LTD (Processor)

Signed on behalf of Sentinel Edge Networks LTD, company number 17150600, registered address 134a West Hendon Broadway, London, NW9 7AA, United Kingdom, as the pre-approved standard form of this Data Processing Agreement. A countersigned copy is issued on request to support@maskbreak.com.

Annex A — Details of processing

Subject matter	Real-time evaluation of network and device signals to return a fraud-risk assessment (allow / review / block, a 0–100 risk score, and reason codes) for actions the Customer chooses to protect.
Duration	For the term of the Agreement; individual records are retained only for the periods stated below and in the Privacy Policy.
Nature & purpose	Collection, analysis, pseudonymisation, transient enrichment via sub-processors, and short-term storage of technical signals, solely to detect and prevent fraud and abuse on the Customer's behalf. No advertising, profiling for the Customer's marketing, or automated decision producing legal effects is performed by Maskbreak; the Customer determines and applies its own enforcement.
Types of Personal Data	End-user IP address; a pseudonymous device identifier (stored only as a one-way SHA-256 hash; the raw identifier is never stored); coarse client attributes (browser and OS name and major version, never a full user agent); network classification labels (e.g. VPN/proxy/datacenter/Tor); and, where the Customer chooses to submit them, a pseudonymous account reference (hashed) and an email address for a transient disposable-domain check (checked in memory and never stored — only the boolean result is retained).
Categories of Data Subjects	The Customer's own end users, applicants, and visitors whose interactions the Customer submits for evaluation (e.g. at signup, login, or checkout).
Retention	Raw IP addresses are one-way hashed within 7 days. Evaluation records persist for the life of the account and are deleted on account deletion. Pseudonymous device-sighting counters are deleted after 90 days of inactivity, and pseudonymous device-to-account links (the hashed account reference, where the Customer submits one) are likewise deleted after 90 days of inactivity. Attempts to deliver the Customer's configured webhooks are logged with the event type, HTTP outcome, and any error string only — never the payload and never end-user IP addresses — and delivery-log entries are deleted after 30 days or with the account. Transient inputs (submitted email, raw device identifier) are never stored. Encrypted backups roll off on a 60-day cycle.

Annex B — Technical & organisational measures

Maskbreak maintains the security measures summarised below; the authoritative and current description is the Security Whitepaper, which forms part of this Annex by reference.

- **Encryption** — TLS in transit (HTTPS-only, HSTS with preload); encryption at rest for the database and backups.

- **Data minimisation & pseudonymisation** — raw identifiers hashed within 7 days; device identifiers stored only as hashes; transient inputs never persisted.
- **Access control** — least-privilege access to production; authenticated console with optional two-factor authentication (TOTP with recovery codes, and passkeys), per-device session revocation, and an optional API-key IP allowlist.
- **Network & application security** — strict Content-Security-Policy, standard security headers, origin lockdown behind the CDN, per-key and per-IP rate limiting, and signed webhooks.
- **Resilience** — encrypted daily backups in the EU (Stockholm region) on a 60-day rolling schedule; health monitoring and alerting.
- **Governance** — an active responsible-disclosure programme (RFC 9116 `security.txt`), security-relevant account changes notified to the account holder, and an honest, dated statement of the attestations not yet held (Maskbreak is pre-audit for SOC 2 Type II and holds no SOC 2, ISO 27001, HIPAA, or PCI DSS certification today).

Annex C — Sub-processors

The following third parties may process Customer Personal Data. The authoritative, dated list is maintained at maskbreak.com/sub-processors; that list, including its change log, forms part of this Annex by reference.

SUB-PROCESSOR	PURPOSE	REGION
Network- & device-intelligence providers	Transient enrichment of network and device signals (VPN/proxy/Tor/datacenter classification and device intelligence); named to the Customer under this DPA.	Stated in the named provider list, available on request from support@maskbreak.com
Cloudflare	CDN, edge security, and DDoS protection.	Global edge
Railway	Application hosting.	EU / US
Turso	Managed database.	EU
Upstash	Rate-limit state (client IP addresses as short-TTL keys).	EU
Amazon Web Services (S3)	Encrypted database backups.	EU (Stockholm, eu-north-1)
Resend	Transactional and lifecycle email delivery.	US
Auth0 (Okta)	Emailed one-time sign-in link, where offered: verifies possession of the account holder's email address; receives that address only when the option is used.	EU / US (tenant region)

Where a Sub-processor is located outside the UK/EEA, transfers are made under the safeguards described in Section 10. The public list is definitive as to the current set of Sub-processors; their regions are as stated in this Annex.