Data Processing Agreement

Sentinel Edge Networks LTD · Registered in England & Wales 17150600 · Version 1.23 · 5 November 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.

When versions 1.10 and 1.11 apply. Version 1.11 applies from its publication on 28 September 2026, except that three additions first made in version 1.10 apply to a Customer whose account was created before 28 September 2026 only 14 days after Maskbreak notifies that Customer of them by email: the device-storage sentence in Section 3 (second paragraph); the restriction on decisions about individuals in Section 3 (third paragraph); and, in Section 6, the words "for the processing it carries out on Maskbreak's behalf" and the sentence on providers' own-purpose use. Until then the corresponding text of version 1.9 applies to that Customer. The other changes in version 1.10 correct statements of fact (processing regions, the GitHub backup job, the storage the browser SDK uses, the security-header wording and how sub-processor change notices are given) and apply at once. Version 1.11, published the same day, replaces the fixed start date that version 1.10 gave those three additions with this notice rule, uses the same account-creation cut-off as the Terms of Service, and gives sub-processor change notices through the dated change log on the public list. Later versions keep this rule for those three additions.

Version 1.23 (5 November 2026). This version records changes made on 5 November 2026 and corrects statements of fact; it applies at once and adds no obligation for the Customer. Section 11 and Annex C now say that each encrypted backup copy kept in Google Drive is moved to the trash after 25 days (after 30 days until 5 November 2026) and deleted by the provider 30 days later, by a cleanup the nightly backup job runs every night, also when its upload fails; Annex C also says where the backup copies are held (the copies in Cloudflare R2 in the EU, the encrypted copies in Google Drive in the United States and other Google locations), which version 1.18 left out of its closing note. Section 11 now says that, for a day after an account is deleted, a sweep repeated every hour removes any

record written under it while the deletion ran. Annex A now says that a login, second-factor check or password change the Customer has not reported as successful is kept in the account network as an attempt, which counts toward how many of the Customer's accounts a device or a network address tried but is not a device or address the account used; that Maskbreak's server looks up the DNS records of a script address the Customer adds through Cloudflare's public DNS resolver (1.1.1.1), which receives only those names and no end-user data; and how a deleted account's script address is removed. Annex C says that the daily count of email and phone checks also holds how many unanswered checks were given back that day, and lists the DNS resolver under Cloudflare, already a Sub-processor. Annex B adds the per-account limits on the codes entered to change the second factor, the binding of Google and GitHub redirect sign-ins to the browser that started them, and the password check before an organization invites a member or makes one an admin. Version 1.22 is under Version history with the notes of earlier versions.

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
2. Roles & scope of processing
3. Customer instructions
4. Confidentiality
5. Security of processing
6. Sub-processors
7. Assistance with data-subject rights
8. Personal data breaches
9. DPIAs & prior consultation
10. International transfers
11. Deletion & return of data
12. Audits & information
13. Liability & precedence
14. Term
15. Governing law
16. Signatures

Annex A — Details of processing
Annex B — Security measures
Annex C — Sub-processors
Version history

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, website/security telemetry, and the pseudonymous service-wide device-sighting counter it keeps from the device identifier of each evaluation (a one-way hash with how many times and since when that device has been seen across all customers, with no site, account, IP address or user agent attached, used to return `times_seen` and `first_seen`) — 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. This includes deciding whether rules on storing or accessing information on an end user's device (for example regulation 6 of the UK Privacy and Electronic Communications

Regulations or Article 5(3) of the ePrivacy Directive) require consent before the Maskbreak browser SDK runs on the Customer's own sites, and obtaining it where they do; the storage the SDK uses is listed at maskbreak.com/integrations#sdk-storage. (For a Customer whose account was created before 28 September 2026, this applies only 14 days after Maskbreak notifies it by email; see When versions 1.10 and 1.11 apply.) The Customer must not submit special-category data for evaluation, and Maskbreak does not require or use special-category data to produce risk scores.

The Customer shall not use the Services, alone or as a material factor, to decide an individual's creditworthiness, employment eligibility, financial status, tenancy or insurability, or as the basis of any other decision with legal or similarly significant effects on an individual, except where that use complies with Data Protection Law and other applicable law, including any requirement for human review. (For a Customer whose account was created before 28 September 2026, this applies only 14 days after Maskbreak notifies it by email; see When versions 1.10 and 1.11 apply.)

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 for the processing it carries out on Maskbreak's behalf, and remains fully liable to the Customer for a Sub-processor's performance of those obligations. Annex C describes where a provider's own standard terms may also permit it to use data it collects for its own purposes; for that use the provider acts under its own terms, not on Maskbreak's behalf. (For a Customer whose account was created before 28 September 2026, this applies only 14 days after Maskbreak notifies it by email; see When versions 1.10 and 1.11

apply.) 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 a dated entry in the change log on the public list at maskbreak.com/sub-processors. 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.

Where Annex C lists a Sub-processor by category rather than by name, Maskbreak shall give the Customer that Sub-processor's legal name, address and processing location on request, as confidential information under the Agreement.

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). Maskbreak holds most Customer Personal Data in pseudonymised or short-lived form, and an account reference the Customer sends is kept encrypted for that Customer's console (Annex A). The Customer can find and export the records about a Data Subject through the Services (the console's event search and CSV export); Maskbreak deletes individual records on the Customer's documented request, and provides any other assistance required, 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 IP addresses in evaluation records are replaced with a keyed one-way hash after 7 days by a cleanup that runs every six hours, evaluation records are deleted when the account is deleted (and, for a day after the deletion, a sweep repeated every hour removes any record written under that account while the deletion ran), 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 removed on the backup cycle, within 60 days (each copy is currently removed 40 days after it is made; since 22 October 2026 a second copy, encrypted with a key only Maskbreak holds, is kept in Google Drive, where each copy is moved to the trash after 25 days (after 30 days until 5 November 2026) and deleted by the provider 30 days later), after which it is unrecoverable; backups are never used to restore data a Customer has deleted. The primary database also keeps its provider's point-in-time history (Cloudflare D1 Time Travel) for 30 days; it is used only to recover from a failure of the database itself, and deletions made after the point restored are carried out again. The copies made up to 16 October 2026 are held by Maskbreak's former backup provider, where a rule set to delete them within the 60-day limit was in place when that account was suspended; Maskbreak can no longer check or delete those copies itself (Annex C). On 19 October 2026 Maskbreak deleted the database it kept with the former database provider and closed its accounts with that provider and with the former email provider; copies they may still hold in their own backups follow their retention terms. The application logs kept by the former hosting provider are deleted by it within 30 days of 20 October 2026.

Assurance clarification, 6 September 2026: the Security Whitepaper records the daily backup-expiry audit and the open restoration item. This disclosure does not amend or extend the deletion and retention obligations in this DPA.

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)	For Sentinel Edge Networks LTD (Processor)
_____ Signature _____ Name & title _____ Organisation _____ Date	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, enrichment by the network- and device-intelligence providers listed in Annex C (and, for the console's email and phone check and, for a Customer that has email and phone intelligence on, for the email addresses and phone numbers it sends with its visitor checks, by the email- and phone-intelligence provider listed there; and, for a Customer whose server reports login attempts or account events, account-takeover scoring of its login attempts and the recording of the account events it reports by Sift, listed there), and storage of technical signals for the periods below, 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	**Collected in the end user's browser and processed to produce the assessment:** the IP address and connection characteristics; browser and device characteristics read by the network and device checks (for example user agent, languages, time zone, screen and window size, processor count, rendering (canvas/WebGL) characteristics, and automation, tampering, private-mode, emulator and virtual-machine indicators); and a pseudonymous device identifier. **Stored by Maskbreak:** the 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 reason codes; per-customer device-visit history (hashed event and device identifiers with timestamps, and a customer-specific keyed hash of the account reference where the Customer submits one); where the Customer enables the optional GPU evidence beta, 128 numeric GPU-execution features per device, stored encrypted and compared only within that Customer; where the Customer uses the optional browser-consistency check, keyed one-way hashes of canvas readings and of the machine type they describe, per Customer; where the Customer chooses to submit it, an account reference (`accountId`), kept as a keyed hash for that Customer and, since 18 October 2026, encrypted with a key of that Customer's own so that Customer's console can show it, together with the devices (the same one-way device hash) and the network addresses (a keyed one-way hash for that Customer, never kept for a shared exit such as a VPN, proxy, datacenter address, Tor exit, Apple's iCloud Private Relay or a mobile carrier's shared address) the account was checked from, and the stored evaluations that carried it (since 5 November 2026 a login, second-factor check or password change the Customer has not reported as successful is kept with the same hashes but marked as an attempt, which counts toward how many of the Customer's accounts a device or an address tried and is not counted as a device or an address the account used); an email address for a transient disposable-domain check (checked

in memory and never stored — only the boolean result is retained); and, when an account holder uses the console's email and phone check, the one email address or phone number typed into it, which is sent to the email- and phone-intelligence provider in Annex C and, like the answer, not stored by Maskbreak. **Sent to Sift, for a Customer whose server reports a login attempt or an account event (since 23 October 2026; login protection is on for every Customer, processes nothing until then, and can be turned off in the Customer's Settings):** for each login attempt the Customer reports as a login, keyed one-way hashes of the Customer's account reference, of its session identifier (or of Maskbreak's device key where none is sent) and of Maskbreak's device key, made with a key that differs for every Customer; whether the password was right; the end user's IP address and browser user-agent string; the end user's email address where the Customer sends one; the Customer's website domain; and Maskbreak's own result for the visit (the decision and risk score, network and browser flags, the VPN service's name and the IP address's country). One Sift account serves every Customer that uses login protection, so the scores for one Customer's logins draw on the logins of all of them. The account events the Customer reports for an account (a signup, a password change, a verification, a logout, an account-detail change) are sent to Sift as that event with the same data, and Sift returns no score for them. Of Sift's answer to a login Maskbreak keeps, on the stored evaluation record: the account-takeover score, the names of Sift's reasons (never their values), Sift's pseudonymous user identifier for the account (the keyed hash above) and the Customer's own report of the login as the real user or a takeover, which Maskbreak sends to Sift as a label on that pseudonymous user; a high score also leaves the reason code `account_takeover_risk`. **Sent to the email- and phone-intelligence provider, for a Customer that has email and phone intelligence on (since 23 October 2026; on for accounts created on or after that day, off for older accounts until they turn it on in their Settings, and any account can turn it off there):** the email addresses and phone numbers the Customer sends with its visitor checks, and nothing else about the

end user; the provider returns a risk score, its reason names and a few facts (whether the address accepts mail, when its domain was registered, on how many sites it was seen, in how many known data breaches it appears; a number's validity, line type and carrier), which Maskbreak keeps on the stored evaluation record together with, on a high score, the reason code `email_high_risk` or `phone_high_risk`; the address and the number are never stored or logged. Also stored for the Customer's console: the two-letter country code of the IP address; the address lookups the Customer runs (`/v1/lookup` and the MCP `lookup_ip` tool), stored like evaluations; and false-positive reports, a copy of one evaluation's technical details with the Customer's note. Where the Customer puts its public site ID in the script tag (since 17 October 2026), each page view that loads the script sends that ID, and the end user's browser adds the page's origin; Maskbreak stores only the first and latest origin seen and their times, per account, and nothing about the end user. Where the Customer adds its own script address (a subdomain of its site, since 20 October 2026), end users' browsers load the script and send that report through that name, carrying the same request data as through maskbreak.com; Maskbreak stores only the name, its set-up state, when it was added and first worked and, since 5 November 2026, when its TXT record was found, per account, while it is in use; since 5 November 2026, when the Customer adds a name and while it waits for its TXT record, Maskbreak's server looks up the name's DNS records and the TXT record `_maskbreak.` followed by the name through Cloudflare's public DNS resolver (1.1.1.1), which receives only those names. The console's page check (since 20 October 2026) processes no end-user data: a browser run by Cloudflare opens, once, the page address an account holder enters, and Maskbreak keeps neither the address nor the result.

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), the people whose email address or phone number an account holder checks in the console, and, where the Customer has email and phone intelligence on, the end users whose email address or phone number the Customer sends with a visitor check.

Retention	Raw IP addresses in evaluation records (including an address recorded because it matched a Customer exception) are replaced with a keyed one-way hash after 7 days, by a cleanup that runs every six hours. Evaluation records persist for the life of the account and are deleted on account deletion. Pseudonymous device-to-account links (the hashed account reference, where the Customer submits one) are deleted after 90 days of inactivity. (The service-wide device-sighting counter is Maskbreak's own data, Section 2; it is deleted after 90 days without a sighting.) Account-network records (the encrypted account reference, its device and address links and the list of its stored evaluations) are deleted 90 days after the account was last checked, and the account reference on a stored evaluation record is cleared 90 days after that evaluation; browser-consistency hashes are kept for 30 days from the last sighting. 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. Per-customer device-visit history is kept for a rolling 90 days and GPU-evidence features for up to 30 days after the last sample; both are deleted with the account, and GPU-evidence data also when the Customer disables that beta. Transient inputs (a submitted email address or phone number, the raw device identifier, a value checked with the console's email and phone check and its answer) are never stored. Of the providers' answers, the scores, reason names and facts listed under Types of Personal Data (Sift's account-takeover score and reasons with the Customer's own report; the email- and phone-intelligence provider's scores, reasons and facts) are kept on the evaluation record for the life of the account; Sift and the email- and phone-intelligence provider keep what they receive under their agreements with Maskbreak and their own terms. The IP address in a false-positive report is hashed on the same 7-day schedule, and reports are deleted with the account. The primary database's own point-in-time history (Cloudflare D1 Time Travel) keeps earlier states of the database for 30 days. Encrypted backups are removed

within 60 days (each copy in Cloudflare R2 currently 40 days after it is made; each copy in Google Drive moved to the trash after 25 days and deleted by the provider 30 days later); see Section 11 for the copies made up to 16 October 2026. A Customer's script address is removed from Cloudflare when the account is deleted; if Cloudflare does not confirm the removal at once, a job that runs every hour asks again until it does, and until then only the name and Cloudflare's reference for it are kept.

Annex B — Technical & organisational measures

Maskbreak maintains the security measures summarised below. Section 2 ("Technical controls in place today") of the current Security Whitepaper forms part of this Annex by reference; the rest of the whitepaper is explanatory.

- **Encryption** — TLS in transit (HTTPS-only; HSTS for one year including subdomains, sent with the preload directive — the domain is not yet on browsers' built-in preload lists); encryption at rest for the database and backups.
- **Data minimisation & pseudonymisation** — raw IP addresses in evaluation records replaced with a keyed one-way hash after 7 days; device identifiers stored only as hashes; an account reference the Customer submits is kept as a keyed hash for linking and, encrypted with a key per Customer, only for display in that Customer's console; transient inputs never persisted. Exception entries the Customer configures keep the value the Customer entered until the Customer removes them.
- **Access control** — least-privilege access to production; authenticated console with optional two-factor authentication (TOTP with recovery codes, and passkeys), per-account limits on failed sign-in and two-factor attempts and, since 5 November 2026, on the codes entered to change the second factor; Google and GitHub redirect sign-ins bound to the browser that started them (PKCE, since 5 November 2026); a password check, or a recent Google or GitHub sign-in, before sensitive account changes, including, since 5 November 2026, an organization inviting a member or making one an admin; per-device session revocation, console sessions held in an HttpOnly cookie, and an optional API-key IP allowlist; administrative sign-in requires a phishing-resistant passkey through a single-sign-on provider and passes an access gateway that admits only Maskbreak's operator; administrative access by Maskbreak staff is recorded in application logs and, since 20 October 2026, in an audit table kept for one year, and key rotations, two-factor removal, forced sign-outs and reinstatements an operator makes to an account are emailed to the account holder.
- **Network & application security** — Content-Security-Policy with host allowlists and violation reporting on every page (a strict first-party policy without inline script is enforced on the

internal admin console; a hash-based policy without inline script is enforced on the customer console), standard security headers, per-account and per-IP rate limiting, and signed webhooks. The application server has no public address of its own: since 20 October 2026 it runs in a Cloudflare container that only Maskbreak's gateway Worker can reach, and it reaches the database only through a Worker that requires a secret (the nightly backup job holds a separate secret that permits reading only). A Customer's own script address answers only for the script, its network-check redirect and its site report (and a `robots.txt` served by the gateway).

- ✓ **Resilience** — encrypted daily backups in the EU (Cloudflare R2, EU jurisdiction, since 17 October 2026; each copy removed 40 days after it is made, within a 60-day commitment that a daily audit checks), created by a scheduled job on GitHub-hosted infrastructure that writes through a receiver accepting only that job's signed identity and only new copies, and that, since 19 October 2026, loads each copy into a temporary in-memory database to check its row counts and integrity; since 22 October 2026 a second copy, encrypted on the backup runner with a key only Maskbreak holds, in Google Drive, where the same job moves each copy to the trash after 25 days; the primary database's own 30-day point-in-time history (Cloudflare D1 Time Travel), used only to recover from a failure of the database, after which deletions made after the point restored are carried out again; health monitoring and alerting, including an outside check every five minutes that emails Maskbreak when the website or the API fails, without depending on the application server or the database; a new application version takes over only once it answers its readiness check.
- ✓ **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 and regions, forms part of this Annex by reference.

Sub-processor	Purpose	Region
Network-intelligence provider and device-intelligence provider	Network and device checks: their scripts run in the end user's browser and, with the requests Maskbreak's server makes to them, process the IP address, an encrypted network token, browser and device characteristics, pseudonymous device identifiers and security signals to return VPN/proxy/Tor/datacenter classifications and device intelligence. Their standard terms may also allow them to use signals collected through their scripts for their own purposes (for example to maintain and improve their services, for security, or in de-identified and aggregated form); for that use they act under their own terms, not on Maskbreak's behalf. Listed by category; each provider's name, address and processing location are given to the Customer on request under Section 6, as confidential information, from support@maskbreak.com.	United States (transfers under Section 10)

Sub-processor	Purpose	Region
Email- and phone-intelligence provider	The console's email and phone check, since 18 October 2026: when an account holder types one email address or one phone number, Maskbreak's server sends that value to this provider and shows a summary of the answer, with a daily limit of checks per account. The provider receives only the typed value, never account, API-key, evaluation or visitor records, and Maskbreak stores neither the value nor the answer, only how many checks the account made that day and, since 5 November 2026, how many unanswered checks were given back to it that day (kept 3 days). Email and phone intelligence on visitor checks, since 23 October 2026 (on for a Customer account created on or after that day, off for an older account until it turns it on in its Settings; any account can turn it off there): the email addresses and phone numbers a Customer that has it on sends with its visitor checks go to this provider too, which returns a risk score, its reason names and the facts listed in Annex A; Maskbreak keeps those on the evaluation record, never the address or the number, and each check counts toward the same daily number. Its standard terms may also allow it to use the values it is asked about for its own purposes, such as the fraud history it keeps across its customers; for that use it acts under its own terms, not on Maskbreak's behalf. Listed by category; its name, address and processing location are given to the Customer on request under Section 6, as confidential information.	United States (transfers under Section 10)

Sub-processor	Purpose	Region
Sift (Sift Science, Inc.)	Login protection, since 23 October 2026, on for every Customer account (the Customer can turn it off in its Settings; nothing is sent until the Customer's server reports a login attempt or an account event with the Customer's own account reference, which is its instruction to use it): for each login attempt that Customer reports as a login, Maskbreak's server sends Sift the data listed in Annex A (keyed one-way hashes of the account and session identifiers and of the device key, never the identifiers themselves; whether the password was right; the end user's IP address and browser user-agent string; the email address where the Customer sends one; the Customer's website domain; Maskbreak's own result for the visit) and returns Sift's account-takeover score with its answer; the account events that Customer reports (a signup, a password change, a verification, a logout, an account-detail change) are sent to Sift as that event, with the same data and no score in return. One Sift account serves every Customer that uses login protection, so its scores learn from the logins of all of them. Sift's service privacy notice says it also uses the data it receives to improve its services, including the models behind its scores; for that use it acts under its own terms, not on Maskbreak's behalf.	United States (transfers under Section 10)

Sub-processor	Purpose	Region
Cloudflare	CDN, edge security, and DDoS protection, and Workers (among them the gateway in front of the application server, the Worker through which the application reaches the database, the email relay, the receiver that writes the backups, and an uptime check); since 17 October 2026 also R2 storage for the encrypted nightly database backups (disaster recovery; each copy removed after 40 days); since 19 October 2026 also D1, the primary database (holds all stored Customer Personal Data, encrypted at rest), and Email Service, which delivers Maskbreak's email; since 20 October 2026 also Containers, which run the application server and keep its application logs for 7 days (since 22 October 2026 R2, in its EU jurisdiction, also keeps a copy of those logs for 30 days), Browser Run for the console's page check (no end-user data), and custom hostnames, which serve the script from a Customer's own subdomain; since 5 November 2026 also its public DNS resolver (1.1.1.1), which Maskbreak's server asks for the DNS records of a script address a Customer adds and which receives only those names (no end-user data).	Global edge; application server and database: United States (Eastern North America); backups and the 30-day log copy: EU (R2 EU jurisdiction)

Sub-processor	Purpose	Region
GitHub (GitHub, Inc.)	GitHub Actions runs the nightly backup job: for a few minutes each night a GitHub-hosted runner reads the full database, compresses it and uploads it to Cloudflare R2 (to AWS S3 until 16 October 2026), where it is encrypted at rest, and since 22 October 2026 also, encrypted with a key only Maskbreak holds, to Google Drive. Also runs scheduled monitoring checks that contain no customer records.	United States and other locations where GitHub-hosted runners operate
Google (Google LLC)	Google Drive, in Maskbreak's Google Workspace: since 22 October 2026 stores a second copy of each nightly database backup, encrypted on the backup runner before upload with a key Google does not hold; each copy is moved to the trash after 25 days (after 30 days until 5 November 2026), by a cleanup the nightly backup job runs every night, and Google deletes it 30 days later.	United States and other Google locations

Sub-processor	Purpose	Region
PostHog (PostHog, Inc.)	Product analytics and session recordings for Maskbreak's own website (public pages, `/signup`) and the dashboard, loaded from page load without a consent prompt and skipped under Global Privacy Control, Do Not Track and Save-Data. Pages viewed, clicks, browser/device metadata, IP address, a random browser identifier and session recordings in which form fields, the visitor's own network readouts and all dashboard text are masked in the browser; since 17 October 2026 also page-speed measurements and, on public pages and `/signup`, clicks that changed nothing and the page's own script errors, with addresses, emails and key-like strings removed. Not supplied with customer API/evaluation records; listed for transparency about our own website service.	EU (PostHog EU Cloud, Frankfurt, Germany); PostHog's DPA permits processing outside the EEA, including the US

Sub-processor	Purpose	Region
Sentry (Functional Software, Inc.)	Error reports from Maskbreak's own server software, sent when it hits an unexpected error: error type, message and stack trace, runtime and release details, the request method and path with IP addresses, email addresses, identifiers (UUIDs, account and record numbers, long hexadecimal strings) and token-like segments replaced by placeholders, and, for up to 30 recent outgoing calls, only the method, status code and origin (scheme, host name and port; no path or query), so a Customer's webhook host name can appear. Request headers, cookies, bodies, query strings, IP addresses, email addresses, the user/account profile, API keys, secrets and tokens are removed before sending, including from error messages; this removal is pattern-based, a strong safeguard rather than a guarantee. Errors only: no tracing, profiling, log forwarding or browser SDK. In Sentry, IP-address storage is turned off, the server-side data scrubber is on as a second layer, and generative AI features (including Seer) are off, so error data is not sent to Sentry's AI sub-processors. Retention: 30 days on Sentry's free Developer plan; up to 90 days on paid plans and during a trial. Designed not to receive Customer Personal Data; listed for transparency.	EU (Sentry EU region, Frankfurt, Germany); Sentry's DPA permits processing in the US and other countries where it or its sub-processors operate

Former Sub-processors

Maskbreak no longer sends these providers any Customer Personal Data. Each may still hold data from the time it was used, as described.

Sub-processor	What it did and what it may still hold	Region
Railway — former	Former application hosting and application logs, until 20 October 2026, when Maskbreak shut its service there down (Cloudflare Containers since); the logs it kept are deleted by Railway within 30 days.	United States (US East)
Turso — former	Former managed primary database, until 19 October 2026 (Cloudflare D1 since); the database was deleted and Maskbreak's account closed the same night, and copies Turso may still hold in its own backups follow its retention terms.	United States (AWS us-east-1, Virginia)
Resend — former	Former transactional and lifecycle email delivery, until 19 October 2026 (Cloudflare Email Service since); the account was closed the same night, and copies Resend may still hold in its own backups follow its retention terms.	United States
Amazon Web Services (S3) — former	Former backup store: the encrypted database backups made up to 16 October 2026 (no new copies since). A rule set to delete them within the 60-day limit was in place when the account was suspended; Maskbreak is not restoring access to it and can no longer check or delete these copies itself.	EU (Stockholm, eu-north-1)

Sub-processor	What it did and what it may still hold	Region
Widgo (Widgo, Inc.) — legacy records only	Former AI chat on public marketing pages, from 8 September 2026 (opened by a click until 22 September) until its removal on 30 September 2026; no page loads it now. Holds the chat content, volunteered contact details and visit/device metadata it received while loaded. Never supplied with customer API/evaluation records; listed for transparency about our own website service.	US, EU and other locations described in Widgo's privacy policy
Crisp (Crisp IM SAS) — legacy records only	Historical support conversations only following replacement on 8 September 2026. The switch does not delete existing records; access and deletion requests remain available.	EU (France)

Where a Sub-processor is located outside the UK/EEA, transfers are made under the safeguards described in Section 10. The primary database and application hosting are in the United States, so stored Customer Personal Data is held and processed there; the backups in Cloudflare R2 are stored in the EU, and the second, encrypted copy in Google Drive in the United States and other Google locations. The public list is definitive as to the current set of Sub-processors; their regions are as stated in this Annex and on that list and, for providers listed by category, in the details supplied on request under Section 6.

Version history

Version 1.22 (2 November 2026). This version records a change to Annex B and applies at once; it adds no obligation for the Customer. Since 26 October 2026 the access gateway in front of administrative sign-in no longer checks that the operator's device is enrolled; it admits only Maskbreak's operator, who still signs in with a phishing-resistant passkey through a single-sign-on provider, and administrative access is still recorded as before. Version 1.21 is under Version history with the notes of earlier versions.

Version 1.21 (23 October 2026). This version, published the same day as version 1.20, records the default settings of the two features that version described and applies at once; it adds no obligation for the Customer. Annex A and Annex C now say that login protection

is on for every Customer account: it processes nothing until the Customer's server sends Maskbreak a login attempt or an account event with the Customer's own account reference, which is the Customer's instruction under Section 3 to use it, and the Customer can turn it off in its Settings; and that email and phone intelligence is on for Customer accounts created on or after 23 October 2026 and off for accounts created before, which can turn it on in their Settings (any account can turn it off there), and sends nothing until an email address or a phone number arrives with a visitor check. A Customer whose server sends no login attempt, account event, email address or phone number is not affected. The Customer may object on reasonable data-protection grounds until 22 November 2026, as under version 1.20. Version 1.20 is under Version history with the notes of earlier versions.

Version 1.20 (23 October 2026). This version records changes to the processing of two existing Sub-processors and applies at once; it adds no obligation for the Customer. Annex A and Annex C now say that, since 23 October 2026, for a Customer that turns on email and phone intelligence in its Settings, the email addresses and phone numbers that Customer sends with its visitor checks are sent to the email- and phone-intelligence provider (already listed in Annex C for the console's email and phone check), which returns a risk score, its reason names and a few facts that Maskbreak keeps on the evaluation record (never the address or the number); and that, for a Customer that has turned on login protection, the account events it reports (a signup, a password change, a verification, a logout, an account-detail change) are sent to Sift as that event, with the same data as a login and no score in return. Annex A also states what Maskbreak keeps of Sift's answer to a login (the score, the names of Sift's reasons, Sift's pseudonymous user identifier for the account and the Customer's own report of the login as the real user or a takeover), which version 1.19 described as not stored; that changed the same day, for the Customer's console. Each provider processes a Customer's Personal Data for these purposes only after that Customer turns the feature on, which is its instruction under Section 3 to use it; a Customer that does not turn it on is not affected. The Customer may object on reasonable data-protection grounds until 22 November 2026. Version 1.19 is under Version history with the notes of earlier versions.

Version 1.19 (23 October 2026). This version adds a Sub-processor and applies at once; it adds no obligation for the Customer. Annex C now lists Sift (Sift Science, Inc., United States), which since 23 October 2026 scores login attempts for account takeover for a Customer that turns on login protection in its Settings. Annex A says what Sift receives for each such login (keyed one-way hashes of the Customer's account and session identifiers and of Maskbreak's device key, made with a key that differs for every Customer; whether the password was right; the end user's IP address and browser user-agent string; the end

user's email address where the Customer sends one; the Customer's website domain; and Maskbreak's own result for the visit) and that one Sift account serves every Customer that uses login protection, so the scores for one Customer's logins draw on the logins of all of them. Sift processes a Customer's Personal Data only after that Customer turns login protection on, which is its instruction under Section 3 to use it; a Customer that does not turn it on is not affected. The Customer may object on reasonable data-protection grounds until 22 November 2026.

Version 1.18 (22 October 2026). This version adds a Sub-processor and applies at once; it adds no obligation for the Customer. Annex C now lists Google (Google Drive, in Maskbreak's Google Workspace), which since 22 October 2026 stores a second copy of each nightly database backup, encrypted on the backup runner before upload with a key Google does not hold, so that the backups do not depend on one provider; each copy is moved to the trash after 30 days and Google deletes it 30 days later, within the 60-day commitment of Section 11. It began processing on 22 October 2026, the day its entry was published in the change log on the public list, so the 30 days' notice in Section 6 was not given for it; the Customer may object on reasonable data-protection grounds until 21 November 2026.

Version 1.17 (22 October 2026). This version records a change to the processing of an existing Sub-processor and applies at once; it adds no obligation for the Customer. Annex C now says that since 22 October 2026 Cloudflare, already a Sub-processor, also keeps a copy of Maskbreak's application logs for 30 days in R2, in its EU jurisdiction, with keys, tokens and Maskbreak's own secrets removed from each line first; the hosting provider's own log still keeps them for 7 days. The change was published in the change log on the public list on the day it took effect.

Version 1.16 (21 October 2026). This version corrects a statement of fact and applies at once; it adds no obligation for the Customer. Section 2 now names the pseudonymous service-wide device-sighting counter (a hashed device's visit count and first and last sighting across all customers, which returns `times_seen` and `first_seen`) among the data Maskbreak keeps as an independent Controller, as its Privacy Policy already says, and Annex A no longer lists it among the Customer Personal Data it processes.

Version 1.15 (21 October 2026). This version corrects statements of fact and applies at once; it adds no obligation for the Customer. Section 7 now says that an account reference

the Customer sends is kept encrypted for its console and that Maskbreak deletes individual records on the Customer's documented request. Section 11 and Annexes A and B describe the primary database's own 30-day point-in-time history (Cloudflare D1 Time Travel), used only to recover from a failure of the database, after which deletions made after the point restored are carried out again; Annex B also describes the audit table that records administrative access and the nightly check of each backup copy. Annex A names three stored records it left out (the IP address's country code, address lookups and false-positive reports). Annex C lists former Sub-processors in a table of their own, as the public list does, and corrects the dates of the former chat provider.

Version 1.14 (20 October 2026). This version corrects statements of fact and applies at once; it adds no obligation for the Customer. On 19 and 20 October 2026 Cloudflare, already a Sub-processor, took over the primary database (Cloudflare D1), email delivery (Cloudflare Email Service) and application hosting (Cloudflare Containers) from Turso, Resend and Railway; the database and the application server are in the United States (Eastern North America), as before. Annex C lists the three as former providers and says what became of the data they held. Each change was published in the change log on the public list on the day it took effect, as a change to the processing of an existing Sub-processor, so it was not announced 30 days in advance; the Customer may object on reasonable data-protection grounds until 18 November 2026 (database and email) and 19 November 2026 (hosting), as under Section 6. Annexes A and C also describe two console features of 20 October 2026: the page check, in which a browser run by Cloudflare opens a page address an account holder enters, and the Customer's own script address, a subdomain of its site from which end users' browsers load Maskbreak's script. Annex B describes how the application server and the database are reached and the outside check that alerts Maskbreak when the Services fail.

Version 1.13 (18 October 2026). This version brings the Annexes up to date and applies at once. Annex A adds the account network (where the Customer sends an account reference, Maskbreak now also keeps it encrypted, with a key of that Customer's own, so that Customer's console can show which of its accounts share a device or a network address) and the console's email and phone check. Annexes A, B and C and Section 11 describe the backups, which moved from Amazon Web Services to Cloudflare R2 (EU jurisdiction) on 17 October 2026. Annex C adds the email- and phone-intelligence provider used by that check. It began processing on 18 October 2026, the day its entry was published in the change log on the public list, so the 30 days' notice in Section 6 was not given for it. The check runs only when an account holder types an email address or a phone number into it,

so a Customer that does not want this provider to process its data can leave the check unused, and the Customer's right to object under Section 6 is unchanged.

Version 1.12 (11 October 2026). This version corrects statements of fact and applies at once; it adds no obligation for the Customer. Annex B now says that the strict content-security policy is enforced on the customer console (since 6 October 2026) and that rate limits apply per account and per IP address. Annex C no longer lists Auth0, whose emailed sign-in link was withdrawn on 5 October 2026 and whose tenant was deleted on 6 October 2026, and lists Widgo for legacy records only, as its chat was removed from the website on 30 September 2026.

Version 1.10 corrects the processing regions in Annex C, adds GitHub (nightly backup job) to Annex C, describes the network- and device-intelligence providers' data and their own use under their terms, states how sub-processor change notices are given, completes Annexes A and B, and adds the Customer obligations in Section 3 and the own-purpose wording in Section 6. Version 1.11, the same day, makes those additions apply to a Customer whose account was created before 28 September 2026 only 14 days after Maskbreak notifies it by email, and gives sub-processor change notices through the change log; see the dated change log at maskbreak.com/sub-processors.

Sentinel Edge Networks LTD · Registered in England & Wales, company number 17150600 · 134a West Hendon Broadway, London NW9 7AA, United Kingdom · Data-protection contact: support@maskbreak.com · Version 1.23, 5 November 2026. This is the canonical published copy; a countersigned PDF is available on request. What each version changed is under Version history; sub-processor changes are in the dated change log at maskbreak.com/sub-processors.