

Data Processing Agreement

Sentinel Edge Networks LTD · Registered in England & Wales 17150600 · Version 1.13 · 18 October 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. Version 1.12 keeps this rule for those three additions.

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 Annex C no longer lists Auth0, whose emailed sign-in link was withdrawn on 5 October 2026 and whose tenant was deleted on 6 October 2026, and lists Widgo for legacy records only, as its chat was removed from the website on 30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 1.13 (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.

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

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. 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). 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 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 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), after which it is unrecoverable; backups are never used to restore data a Customer has deleted. 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).

Assurance clarification, 6 September 2026: the Security Whitepaper records pending implementation checks of backup expiry and restoration. 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)

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, enrichment by the network- and device-intelligence providers listed in Annex C (and, for the console’s email and phone check, by the email- and phone-intelligence provider 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; 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. 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.

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), and the people whose email address or phone number an account holder checks in the console.

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-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. 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 (submitted email, raw device identifier, a value checked with the console's email and phone check and its answer) are never stored. Encrypted backups are removed within 60 days (each copy currently 40 days after it is made); see Section 11 for the copies made up to 16 October 2026.

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, 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 an enrolled device; administrative access by Maskbreak staff is recorded in application logs, 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, origin lockdown behind the CDN, per-account and per-IP rate limiting, and signed webhooks.
- **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; 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 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 (kept 3 days). 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)
Cloudflare	CDN, edge security, and DDoS protection; since 17 October 2026 also R2 storage for the encrypted nightly database backups (disaster recovery; each copy removed after 40 days).	Global edge; backups: EU (R2 EU jurisdiction)
Railway	Application hosting and application logs (kept up to 30 days).	United States (US East)
Turso	Managed primary database (holds all stored Customer Personal Data).	United States (AWS us-east-1, Virginia)
Amazon Web Services (S3)	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)
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. Also runs scheduled monitoring checks that contain no customer records.	United States and other locations where GitHub-hosted runners operate

SUB-PROCESSOR	PURPOSE	REGION
Resend	Transactional and lifecycle email delivery.	United States
Widgo (Widgo, Inc.) — legacy records only	Former AI chat on public marketing pages, from 22 September 2026 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
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. 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
Crisp (Crisp IM SAS)	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; backups are stored in the EU. 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.

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 1.13, 18 October 2026. This is the canonical published copy; a countersigned PDF is available on request. Version 1.13 brings the Annexes up to date: the account network and the console’s email and phone check (Annex A), backups in Cloudflare R2 since 17 October 2026 (Annexes A to C, Section 11) and the email- and phone-intelligence provider (Annex C), which began processing without the 30 days’ notice of Section 6 (see Version 1.13). Version 1.12 corrects statements of fact in Annexes B and C (the console’s content-security policy is enforced, rate limits are per account and per IP address, Auth0 is no longer a Sub-processor, Widgo keeps legacy records only). 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.