Cloud Privacy Notice

Website, configuration tools and enquiries

Version 3.0 | 24 October 2026

1. Controller, contact and scope

SHIKANOKO NETWORKS LTD, registered in England and Wales under company number 17131877, with its registered office at 128 City Road, London, United Kingdom, EC1V 2NX, trading as SKNK Cloud, is the controller for the website and enquiry processing described here. Contact admin@shikanoko-networks.com for privacy questions or rights requests.

This notice covers Cloud website visits, configuration and sharing tools, enquiries, support correspondence, complaints, rights requests and necessary delivery and security records. The Cloud website currently does not accept orders, payments or service activation. Selecting a configuration does not create a customer account, invoice, signature request or hosted workload. A separate service-specific notice and, where required, processing agreement must describe additional processing before a hosted service begins.

The main-site notice at /privacy covers shared site features and other services within its stated scope. RIPE application, identity, signing and resource-publication rules do not automatically apply to a Cloud visitor. This notice explains processing; it does not seek blanket consent or change an accepted contract.

2. Information we handle and where it comes from

Website requests: your device sends technical information needed to request and deliver a page, such as IP address, requested URL, request time, headers, browser or device information and, where supplied, a referrer. Delivery and security systems may generate response, error, threat or rate-limit information. A field passing through a system does not mean every layer stores it. We do not represent all website and supplier logs as containing no personal data.

Configuration tools: product selections are held in page state and may be reflected in the URL. Loading or sharing that URL can disclose those selections to the server, recipients of the link, browser history and relevant delivery systems. Copy controls write the selected link or configuration to your clipboard; your device controls how long it remains there. A product choice is not necessarily personal data on its own, but may become personal data when linked to a person or request. Keep personal information and secrets out of links.

Enquiries and reports: we receive the name, contact address, category, subject, message, relevant configuration and any material you choose to send. A shared contact form may also accept service, organisation, region and existing-resource information, and processes a security-verification token. Email correspondence can include its sender, recipients, headers, attachments and follow-up history. Delivery records may contain recipient, subject, status, time and provider identifiers; the fact that one application log masks a body does not erase the message in the mailbox or delivery service.

Sources are normally you and your device. We may receive relevant information from your authorised representative, another correspondent, a reporter or a delivery or security provider. We use third-party information only where necessary for the stated purpose and provide additional source and privacy information where the applicable law requires it. Do not send special-category information, identity documents, details about children or third-party personal data unless necessary and lawfully authorised.

3. Purposes and legal bases

We use necessary request and diagnostic information to deliver pages, maintain reliability, investigate faults, protect systems, prevent abuse and handle security incidents. Our legal basis is our legitimate interests in operating a secure and reliable website, subject to necessity, proportionality and your rights. We limit security information to what the risk and task reasonably require.

We use enquiry and correspondence information to answer you, assess a requested service, investigate an issue and manage appropriate follow-up. Where you personally request steps towards a contract, the basis may be those pre-contractual steps. For general questions, organisational contacts and authorised representatives, we normally rely on our legitimate interests in responding and managing the relationship, rather than treating every contact as personally party to a contract.

We handle rights requests, required disclosures and records under the legal duties that actually apply. Necessary complaints, evidence and claims processing may also rely on legitimate interests or a specific legal obligation. We identify the relevant duty rather than treating all records as subject to one unspecified retention law.

Where we rely on consent for an optional purpose, we explain that purpose and obtain the required choice before processing. An enquiry is not a marketing subscription; accepting terms or acknowledging a cookie notice is not general consent. You may withdraw consent without affecting the lawfulness of earlier processing. We do not sell personal data, and we do not use an enquiry as permission for unrelated advertising.

4. What you need to provide

You can read public product information without submitting a contact form. Technical requests are necessary to deliver pages, and blocking necessary request or security functions may prevent some features from working. You decide whether to contact us or share a configuration. A required reply address and enough information to understand a request are needed if you expect a response; without them we may be unable to reply, verify authority or resolve the issue.

Optional form fields and unnecessary attachments are not a condition of merely browsing. We ask for additional verification only when proportionate to a specific request. Do not send credentials or complete payment-card information. If sensitive evidence is necessary, request a suitable protected channel first.

5. Cookies, browser storage and measurement

NEXT_LOCALE is a first-party session cookie for language routing. The current website sets it for the site path with SameSite=Lax and Secure in production; it has no fixed application expiry beyond the session, although browser session-restoration behaviour can differ. The theme localStorage entry remembers appearance, and cookie_consent remembers acknowledgement of the notice. Those localStorage entries have no application expiry and remain until changed or removed in the browser. The acknowledgement entry is not an analytics or marketing opt-in.

Configuration state, configuration URLs, browser history and clipboard contents are separate from those preferences. You can clear site cookies and localStorage, remove history and replace or clear the clipboard through your browser or device. Clearing preferences may reset language or appearance. The current Cookie Settings control reopens the acknowledgement by clearing its stored flag; it does not by itself switch analytics on or off.

The public website uses Cloudflare delivery and security services, and Cloudflare performance measurement may be supplied through a beacon. Measurement remains a separate activity even where it uses no cookie. A script appearing in a page does not establish that every browser successfully ran it. We distinguish delivery and security processing from optional analytics. Where consent is required, optional browser analytics or marketing must not be activated until the required opt-in has been obtained; where an applicable law permits a specific exception, its transparency, purpose and objection conditions must be met. We do not treat continued browsing, closing a notice or an acknowledgement flag as that consent.

Necessary anti-bot verification may process browser and security signals under the applicable Cloudflare terms. Cookies for a separate payment, private order or admin workflow are explained in the notice for that workflow; browsing a Cloud page is not a request to start one. If a new optional tool is introduced, its purpose, provider, information and controls must be explained before activation. You may ask about measurement or object to discretionary processing through admin@shikanoko-networks.com, without losing the right to a more immediate choice required by law.

6. Who receives information

Access is limited to authorised company personnel and providers for their assigned tasks. The current website hosting provider is IONOS SE, a German service provider. It supplies the infrastructure on which website requests and necessary operational records are processed. Cloudflare supplies delivery, network security, anti-bot verification and relevant performance functions. Those functions process technical request or security information; our anti-bot verification request does not send the enquiry message fields merely to validate the token.

Brevo delivers shared contact-form notifications and transactional correspondence and receives the sender or reply-to details, recipients, subject, message and necessary delivery metadata for that task. The current email integration disables open and click tracking by default. Microsoft 365 receives and holds company correspondence in the company mailbox environment. Authorised personnel handling the relevant request can see the necessary message and attachments. Sending an email also involves the mail services selected by you and other correspondents.

DataRep receives information when a privacy or representative matter is sent or referred to it within its appointment. Where necessary, a limited disclosure may be made to professional legal or accounting

advisers, insurers, competent authorities or a lawful successor for the particular purpose and subject to confidentiality and legal safeguards. We do not make all records available to every provider or disclose private enquiries publicly by default.

Providers may act as processors for assigned tasks and may act as separate controllers for specific activities under their own terms. A software product name does not make its author a recipient. Stripe, DocuSeal, RIPE NCC or a VM-management platform is not made a recipient of a Cloud website visit merely because it supports another service. Company-controlled mail archives and protected recovery copies remain subject to the purpose, access and retention limits in this notice.

7. International processing and safeguards

The controller is a UK company. Hosting is supplied by IONOS SE, a German provider; company mail uses Microsoft 365, transactional delivery uses Brevo, and delivery and security use Cloudflare's international infrastructure. Authorised company personnel handle support and administration from China and Switzerland. A supplier's registered country or a proposed VPS location is not a statement that every record, backup, network request or remote access stays there. Provider support and subprocessors may operate in further countries, including the United States, as described in the applicable provider processing and subprocessor terms.

For each disclosure or access arrangement we assess whether it is a restricted transfer under the law that applies, including whether the recipient is a separate organisation. Work by personnel of the same legal controller is assessed separately from disclosure to an overseas contractor or other entity; confidentiality, necessity and security duties continue in either case. We do not treat access from China as covered by a European adequacy decision, or assume that a server location alone resolves transfer duties.

Where a restricted transfer requires protection, it must use an applicable adequacy arrangement or appropriate safeguards, such as the relevant EU Standard Contractual Clauses and UK transfer addendum or agreement, with the required assessment and supplementary measures. We do not rely on browsing the website as consent to routine restricted transfers. The safeguard must match the actual recipient, role and destination; there is no claim that one contract or certification covers every provider and access path.

Cloudflare's published customer DPA describes its EU SCC and UK-addendum arrangements for applicable restricted transfers. Microsoft publishes the Products and Services DPA for Microsoft 365; Brevo and IONOS publish their applicable processing and subprocessor information. The relevant arrangement must cover the actual service, role and destination we use. You can request information about the arrangement that applies to your records and a copy of relevant safeguards at admin@shikanoko-networks.com. We provide it subject only to proportionate redaction for other people's rights, security or protected commercial information; this request route does not replace the disclosures above.

8. Retention and deletion

We decide retention by record type and purpose, rather than applying one period to all website data. Browser preferences, configuration links, history and clipboard information follow the behaviour in section 5. Provider delivery, security and diagnostic records follow their assigned purpose and applicable service controls; we distinguish transient checks, operational metadata and copies kept as evidence.

Enquiry correspondence is retained while the matter is open and for a justified follow-up period. At closure we assess whether further correspondence, an unresolved complaint, a specific security investigation, a legal duty or an actual or reasonably anticipated claim requires particular records. We remove information that no longer has such a purpose, minimise unnecessary attachments and duplicates, and retain only the material needed for a separately justified duty or claim. A possible unspecified future use is not a reason for indefinite retention.

Security and delivery records are retained only for the period needed to investigate failures, enforce the relevant security window and resolve identified incidents, with longer evidence retention justified separately. A provider's maximum available history does not by itself justify keeping all records for that long. Closing an enquiry, cancelling renewal or expiring a token does not automatically erase every independent record, nor does it justify keeping it without review.

Specific legal holds restrict deletion only for their documented scope and duration. Protected backup or mailbox-recovery copies follow their applicable lifecycle and access restrictions; valid deletion decisions are carried forward if records are restored. A provider's deletion delay does not remove our duty to handle the request and explain any lawful limitation. We do not promise an unverified automatic deletion day or apply RIPE contract, tax, signing or recovery periods to every Cloud website record. If an enquiry becomes an actual service or accounting record, its applicable notice and documented legal basis determine the additional retention.

9. Security and automated checks

We use proportionate organisational and technical measures, including restricted access, authentication, protected communications, minimisation and appropriate recovery controls. The measures must reflect the data, purpose and risk; no system can promise absolute security. Report suspected exposure to admin@shikanoko-networks.com without sending additional secrets. Where a breach requires notification to an authority or affected people, we follow the applicable duties and deadlines.

Automated anti-bot checks, rate limits and security rules can reject or delay a request to protect the website. A failed check may prevent form submission; you can contact us by email for human assistance. We distinguish those controls from a solely automated decision producing legal or similarly significant effects. If such significant decision-making is introduced, we must first provide the required information about its use, relevant logic, consequences and available human intervention or challenge under the applicable law. Ordinary website use is not consent to such a decision.

10. Your rights and how to exercise them

Subject to the law that applies, you may request access and a copy, correction, erasure, restriction and, where the conditions are met, data portability. You may withdraw consent for processing based on consent.

Your right to object: You may object to processing based on legitimate interests for reasons relating to your situation. We then stop that processing unless the law permits us to continue on demonstrated overriding grounds or for legal claims. You may object to direct marketing at any time; that objection is not subject to an overriding-interest test.

Send a request to admin@shikanoko-networks.com, identifying the issue and enough information to locate your records. We ask only for proportionate additional identity or authority evidence where needed. You do

not need to buy a service, use a particular form or contact a representative first. Requests are normally free; a fee or refusal is used only where law permits it and is explained.

We respond without undue delay and within the applicable legal period, normally one calendar month for GDPR rights requests. Any lawful extension and its reason are communicated within the required initial period. A restriction, refusal or need to retain particular records is assessed individually and explained, with complaint or remedy information. A general retention schedule is not a reason to refuse every request.

11. Representatives and complaints

You may contact the company directly. DataRep is the appointed data-protection representative for SHIKANOKO NETWORKS LTD, trading as SKNK / SKNK Cloud / IPIP.one, within the EU/EEA, UK and Swiss written appointments. Privacy requests may be sent to datarequest@datarep.com or https://www.datarep.com/data-request, identifying the company and relevant service.

Representative postal contacts are: EU/EEA — DataRep, 77 Camden Street Lower, Dublin, D02 XE80, Ireland; United Kingdom — DataRep, 107-111 Fleet Street, London, EC4A 2AB, United Kingdom; Switzerland — DataRep, Leutschenbachstrasse 95, Zurich, 8050, Switzerland. Address correspondence to DataRep and identify SHIKANOKO NETWORKS LTD and SKNK Cloud in it. Current shared contact details are maintained at /privacy#data-protection-representatives.

DataRep is a representative, not a statement that we have appointed a DPO or received a general compliance certificate. Its DSA address, digitalrequest@datarep.com, is a separate channel and is not the privacy-request mailbox. DSA representative details are at /privacy#dsa-representative.

You may complain to the UK Information Commissioner through https://ico.org.uk/make-a-complaint/ or to another competent supervisory authority, including the authority for your habitual residence, workplace or alleged infringement where applicable. Swiss matters may also be raised with the Federal Data Protection and Information Commissioner at https://www.edoeb.admin.ch/. You retain applicable court and other remedies and do not have to contact us or DataRep before a regulator.

12. Changes and future services

This notice is version 3.0, dated 24 October 2026. We keep relevant prior versions and update the notice when purposes, recipients, tools or arrangements change. Material changes are communicated as required before the relevant new processing, and any required consent or other lawful basis is obtained. A website update does not retrospectively make earlier processing lawful or convert an enquiry into consent to a new purpose.

Before accounts, payments, contract signing or hosted workloads become available, the relevant service information must identify the additional data, purposes, roles, recipients, locations, safeguards, retention and exit arrangements. Processing personal data on a customer’s behalf requires the applicable processing agreement; this website notice does not replace it. Product specifications and another service’s processing history do not establish that those Cloud arrangements already operate.

The full Chinese translation accompanies the English notice. A translation or contract-language clause does not reduce a person’s mandatory privacy rights. Contact admin@shikanoko-networks.com if an explanation is unclear or you need an accessible version.