Privacy Attestation

- **Issuer:** draw.io Ltd
- **Product:** diagrams.net
- **Version:** 2.4.1
- **Published:** 28 November 2026
- **Status:** Published
- **URL:** https://www.drawio.com/trust/privacy-attestation
- **Author:** David Benson

Purpose

This attestation is published by draw.io Ltd as a formal statement of the privacy and data-handling position of diagrams.net. It exists so that organizations evaluating diagrams.net can rely on a single, versioned document rather than negotiating individual contracts. It is a living document; material changes will be published as a new version at the same canonical URL.

The version number and publication date above identify the version of the commitments in force. Organizations relying on this attestation should record the version number they relied on.

Issuer

draw.io Ltd is a UK private limited company.

draw.io Ltd
Artisans' House, 7 Queensbridge
Northampton NN4 7BF
United Kingdom

The named security and privacy contact is David Benson.

1. Scope of Data Handled

diagrams.net does not ask users for personally identifiable information and does not store it, apart from what an organization types into the admin console described below. It does not store user-created content on draw.io Ltd infrastructure, apart from the short-lived collaboration cache described below.

Diagrams are created and edited entirely within the user's browser. Diagrams are saved to the storage the user or institution chooses (the user's local device, Google Drive, Microsoft OneDrive, Confluence, Jira, GitHub, GitLab, Nextcloud, and similar). draw.io Ltd has no access to that storage and does not receive a copy.

Diagram content leaves the user's browser only when the user uses one of these functions:

- **PDF and image export**, where the browser cannot produce the file itself, sends the diagram to a serverless conversion service on Cloudflare for rendering. The payload is not logged, not stored, and not retained after the response is returned.
- **Real-time collaboration**, for diagrams stored in Google Drive or Microsoft OneDrive. While a diagram is open in more than one place, changes are encrypted in the browser and passed between the open copies

through draw.io Ltd's collaboration service, which can hold them in memory, in a cache, for at most 5 minutes. draw.io Ltd does not hold the encryption keys. The cache is not logged or backed up, and entries are deleted automatically.

- **AI features.** A request to create or change a diagram, and any diagram included with it, passes through draw.io Ltd's AI service to Anthropic's Claude models, which Amazon Web Services runs in the European Union (Amazon Bedrock), or to a model that Cloudflare runs, which produces the result. draw.io Ltd does not store or log requests or results. Amazon Web Services keeps no copy of them and does not use them to train models, and Anthropic does not receive them.
- **Import from a web address.** draw.io Ltd's proxy service fetches the file and passes it to the browser without storing it.

Web server logs contain standard request metadata (resource requested, user agent) and are kept for 30 days. They do not contain IP addresses (filtered at the CDN), diagram data, or PII. The web application also reports usage counts that carry no user identifier: the version in use and the kind of storage a diagram is opened from. In a random sample of about 1% of sessions at app.diagrams.net, it also counts clicks on its menus and buttons, to show which functions are used. It sends the fixed name of each menu item and button, how often it was clicked, and the version in use. Any other label, such as a file, page or layer name, is counted as "other" and is not sent. Embedded use and the viewer are not counted. The click counts carry no user identifier, IP address or diagram content. They are stored with the host name and the time they were received, and are deleted after three months.

For Google Drive users at app.diagrams.net, draw.io Ltd counts the users of each organization who open or save a diagram or sign in, each user once a month, for licensing per organization and to count the organizations that use diagrams.net. The browser sends the user's Google ID token the first time each month that it opens and saves a diagram, and the sign-in service passes the token on at each Google sign-in and token renewal. The server reads only the organization's domain (the Google Workspace domain; personal accounts, including Google accounts made with a company address but without Google Workspace, are not counted, and nor are schools, colleges and universities) and the Google account ID from it, and discards the token. Only the number of users per domain and month is stored, with no user identifier, for 24 months. For a domain with one user, the number still relates to that person. So that each user is counted once, the server keeps a HyperLogLog sketch for the running month only, fed with a keyed hash of the account ID. It holds no identifiers and is deleted when the month ends. A hidden file in the user's own Google Drive app data folder records the last month in which the browser reported the user, so that it reports each user once a month. Each count also adds to a daily total of how the token's Google Workspace domain compares with the domain of the user's address: numbers only, with no domains or users, kept for 90 days. To tell education domains apart, draw.io Ltd uses the domain's name and a list of universities, and otherwise reads the domain's public homepage and asks an AI model that Cloudflare runs; it stores only the verdict for the domain. The browser also sends the ID token to get any settings the organization chose. An older licence check, retired in October 2026, recorded the domain only; its records are kept for 24 months.

Organizations that use the admin console at admin.diagrams.net store, on draw.io Ltd infrastructure: the organization's name, domains and settings; each administrator's passkey, as a public key that does not identify its holder; optional names the organization gives its passkeys, which may be a person's name; an audit log of sign-ins and changes, kept for two years; and pending invitations, with the invited email address kept only as a keyed hash until the invitation is used or expires after 7 days. Administrators sign in with a Google account in one of the organization's domains. The ID token and sessions are not stored.

2. Use Restrictions

draw.io Ltd does not, and will not:

- Use any user data for advertising or behavioral targeting.
- Sell, rent, or trade any user data.
- Use any user data, including diagram content, to train AI or machine-learning models.
- Build personal profiles of users.
- Use diagram content, or any data that identifies a user, for product improvement, analytics, or research. The only usage data draw.io Ltd keeps is the usage counts and click counts described in section 1, which carry no user identifier.

These commitments are technically reinforced by the fact that draw.io Ltd does not have the data in the first place.

3. Sub-processors

The following sub-processors are used:

- **Cloudflare, Inc.** - delivers the web application to users, processing their IP addresses to do so and to limit abuse; it is the only sub-processor that sees users' IP addresses. It runs the conversion service for PDF and image export (in Germany), the real-time collaboration relay and its cache (in the EU; the cache can hold encrypted diagram changes in memory for at most 5 minutes), and the web-address proxy, the AI service and the AI models it runs itself (in the Cloudflare data centre nearest the user). It also runs the sign-in service used when connecting cloud storage, which passes access tokens through without storing them and, for Google Drive sign-ins on app.diagrams.net, passes the ID token to the count described in section 1. None of these store or log diagram content. It stores the Google Drive user counts and the admin console records described in section 1 in Western Europe. It also stores the click counts described in section 1.
- **Google Cloud (GCP)** - receives the web application's error reports and usage counts, in Germany (Frankfurt), and keeps them in its logs for 30 days. They contain no IP addresses, diagram data or PII. It also hosts the server that delivers the web application, whose web server logs described in section 1 are kept in the United States. The older licence check's records described in section 1 hold the domain only and are kept in the United Kingdom for 24 months.
- **Amazon Web Services** - runs the AI models used by the AI features (Anthropic's Claude, on Amazon Bedrock), processing requests in the European Union. It stores no requests or results and does not use them to train models. The data does not leave the European Union, and the AWS GDPR Data Processing Addendum applies.

Each sub-processor's own data-protection terms apply to its processing.

draw.io Ltd will update this attestation when sub-processors are added, removed, or changed.

4. Security Controls

draw.io Ltd operates an Information Security Management System (ISMS). Relevant policies include the Information Security Policy, Change Management Policy, Breach Notification Policy, and Risk Management Policy.

- All data in transit is encrypted using current industry-standard cryptography.
- No diagram content is stored at rest on draw.io Ltd infrastructure: the collaboration cache holds data in memory only. The usage counts and admin console records described in section 1 are stored in Cloudflare D1, which encrypts them at rest with AES-256. The click counts are stored in Cloudflare Analytics Engine.
- Access to draw.io Ltd production systems is controlled under the principle of least privilege, with strong authentication.
- A public bug bounty program is operated via Bugcrowd. Findings and historical penetration test reports are tracked internally and remediated through the change management process.
- draw.io Ltd is **working toward SOC 2** certification. This attestation will be updated when that work reaches a reportable milestone. Specific framework certifications (ISO 27001, SOC 2 Type I/II, NIST) are not currently held by draw.io Ltd.

5. Breach Notification

In the event of a security breach affecting draw.io Ltd systems, draw.io Ltd will:

- Notify the UK Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach, where the breach is notifiable under UK GDPR.
- Publish a public advisory describing the breach and its impact at the canonical product communications channels.

Because draw.io Ltd keeps no contact records for end users or their organizations (no accounts, no email addresses), notification to affected organizations is by published advisory rather than direct per-customer notification. Organizations relying on this attestation should subscribe to or monitor the published product communications channels accordingly.

6. Data Return, Deletion, and Termination

Apart from the collaboration cache entries described in section 1, which are deleted automatically within 5 minutes, draw.io Ltd holds only the usage counts described in section 1, which carry no user identifier and are deleted after 24 months, with the running month's sketches, the click counts described in section 1, which are deleted after three months, and the admin console records of organizations that use it. An organization can ask draw.io Ltd to delete its admin console records: its passkeys and their names, its settings, its invitations and its audit log. Otherwise, termination of use of the product has no data-handling consequences on the draw.io Ltd side.

Data held by the user's chosen storage provider (Google Drive, OneDrive, Confluence, Jira, GitHub, GitLab, etc.) is the responsibility of that provider and the organization that contracts with it.

7. Insurance

draw.io Ltd carries cyber liability insurance underwritten by Hiscox Insurance Company Limited, with a limit of indemnity of GBP 1,000,000 in the aggregate and worldwide geographical limits. Cover is held on a continuing basis and renews annually. Evidence of cover is available on request.

8. Governing Law and Jurisdiction

This attestation, and any commitments made within it, are governed by the laws of England and Wales. draw.io Ltd is a UK company and does not accept the jurisdiction of any non-UK court for matters arising from this attestation.

9. Changes to This Attestation

draw.io Ltd will publish material changes to this attestation as new versions, with an updated version number and publication date. The version number and publication date at the top of this document identify the in-force version. Organizations relying on this attestation should record the version number they relied on.

Changes from Version 2.4

- Section 3: Google Cloud keeps the web application's error reports and usage counts in Germany (Frankfurt) instead of the United States. The entry also states that the web server logs are kept in the United States.

Changes from Version 2.3.2

- Sections 1 and 3: the AI features use Anthropic's Claude models run by Amazon Web Services in the European Union (Amazon Bedrock), which keeps no copy of requests, in place of Anthropic and OpenAI in the United States. Amazon Web Services is a new sub-processor; Anthropic and OpenAI are no longer sub-processors for diagrams.net.