Privacy Policy

What information we collect, why we collect it, who we share it with, and how you can ask us to change or delete it. Written to be readable, not to hide behind legalese.

Risk ABC LLC · Effective May 1, 2026 · Version 1.0

Contents

1. Who we are

This Privacy Policy is published by **Risk ABC LLC**, a limited liability company organized under the laws of the State of Georgia, United States ("RiskABC", "we", "us", "our").

Our products — the RiskABC ISO/SOC 2/TISAX platform and RiskABC Gov (CMMC, NIST 800-171, HIPAA) — are delivered as software-as-a-service. Our marketing website lives at **risk-abc.com**.

2. Scope of this policy

This policy covers personal information we collect or process in two places:

- **Our marketing website** (risk-abc.com) — anyone who visits the site.
- **Our product applications** (sso.risk-abc.com, risk.risk-abc.com, gov.risk-abc.com, onboard.risk-abc.com) — users with accounts, and the customer-organization data they put into the platform.

3. Our role & yours

For data put **into** our applications by a customer organization — risk registers, asset inventories, evidence files, control libraries, audit logs, and similar compliance records — RiskABC acts as a **data processor**. The customer organization is the **data controller**: they decide what is uploaded, who has access, and how long it is kept (subject to the limits in this policy).

For information about the marketing website's visitors, account holders' login details, billing data, and analytics on our own sites, RiskABC acts as the **data controller**. Those collections are described below.

4. Information we collect

4.1 Marketing website visitors

When you visit our marketing website we automatically receive standard request metadata: your **IP address**, your **browser and operating system** (from the User-Agent header), your screen size, the page you requested, the page you came from (referrer, when present), and the time of the request. We use this to operate the site and to compile aggregate usage statistics — see Section 6.

If you fill out the **Schedule a Demo** form, you provide us your name, work email, company, and any free-text message. We use that solely to reply to your request and to schedule a demonstration. We do not add you to a marketing list.

4.2 Product accounts

When a user account is created (by their organization's administrator or via a self-service onboarding flow), we store: full name, work email, hashed password (we use bcrypt — we never see plaintext), notification email if different, your role within your organization, your MFA enrollment status, optional avatar image, the timestamp of your last login, and an audit trail of authentication events for security monitoring.

4.3 Customer-organization data inside the apps

While your organization uses the platform, we host the data they choose to put into it: control assessments, risk and threat records, asset inventories, business-impact-analysis processes, policy and evidence files (encrypted at rest), tasks, corrective-action records, and the resulting audit trail. This may include personal data the customer chooses to enter (for example, names of asset owners or evidence reviewers). We process this data on the customer's instructions only.

4.4 Email we send

We send transactional email — welcome emails, password resets, MFA codes, task notifications, and security alerts. These are necessary for you to use the service. We do not send marketing email.

5. How we use information

We use the information described above for the following purposes:

- **Operate the service.** Authenticate you, route you to your workspace, store the records you create, and back them up.

- **Keep the service secure.** Detect abusive sign-in patterns, rate-limit, prevent fraud, investigate incidents, and produce audit logs that you can review.
- **Communicate with you.** Answer support tickets, respond to demo requests, send transactional notifications.
- **Understand how the product is used.** Aggregate analytics about which pages are visited, how long sessions last, and which features are used. We use this to prioritize improvements and identify issues. Details below.
- **Comply with legal obligations.** Tax records, lawful requests from authorities, dispute defense.

We do **not** sell personal information. We do not use customer data to train machine-learning models. We do not use account or analytics data to power third-party advertising.

6. Analytics on our websites

We run a small, self-hosted analytics layer. It is first-party — events go to our own servers, never to a third-party analytics company — and it does not use cookies or fingerprinting.

6.1 What it captures

- The site you visited (e.g. our marketing site, the SSO portal).
- The page or section you are on (URL path, and on long single-page documents the section anchor you have scrolled to).
- The approximate time you spent on each page or section.
- Your IP address (used for the next bullet, and otherwise visible only to system administrators).
- An **approximate location** derived from your IP — country, region, and city. This is approximate by design (city-centroid level, not GPS coordinates).
- Your browser, browser version, operating system, OS version, and a coarse device type (desktop / mobile / tablet) — read from the User-Agent string the browser already sends with every request.
- Your screen size in CSS pixels.
- The referring page, when one was sent.
- If you are signed in to one of our applications, your **account identifier and email** on events fired from that authenticated session — so administrators can see how individual signed-in users move through the product.

6.2 What it deliberately does NOT capture

- No cookies are set. A short-lived session identifier is held in your browser's sessionStorage and is deleted automatically when you close the tab.
- No browser fingerprinting (no canvas, no audio context, no font enumeration, no WebGL probe).
- No third-party analytics SDKs, no advertising pixels, no cross-site tracking.

6.3 Why we collect it

Aggregate, internal product and marketing analysis only: which pages and sections of our marketing site engage prospects, which features inside the product are most used, where in the world our users are, and which browsers we should test in. This helps us prioritize improvements and run a sustainable business. We do not use it to build profiles for advertising.

6.4 Lawful basis

For visitors in the European Economic Area or the United Kingdom: we rely on **legitimate interests** (Article 6(1)(f) GDPR) — operating, securing, and improving our own websites and software. The processing is limited, proportionate, and uses no cookies or fingerprinting. You can object at any time using the contact details in Section 16; on receipt we will delete events tied to your IP and decline to record further events from it.

6.5 Note on the Do Not Track and Global Privacy Control signals

DNT and GPC are anti-third-party-tracking signals. Because our analytics is first-party and stays on our own infrastructure, it does not transmit to advertisers, brokers, or third-party networks. We therefore do **not** automatically suppress collection on the basis of DNT or GPC headers; we publish this notice instead. If you want us to stop, write to us — see Section 16.

7. Cookies & tracking technologies

We use a single **essential** cookie for the SSO portal: an HttpOnly, Secure, SameSite=Lax session-refresh cookie. Without it you cannot stay logged in. We do not use any cookies for analytics, advertising, or tracking.

Inside the apps we also use your browser's sessionStorage and localStorage for short-lived UI state (selected workspace, open menus, theme). These never leave your browser.

8. Sharing & sub-processors

We share personal information only with vendors who help us operate the service. Each of them is bound by a written agreement that limits their use of the data to the purpose we engage them for. As of the effective date above, our sub-processors are:

Sub-processor	Purpose	Location
Hetzner Online GmbH	Primary application hosting (servers, network)	Helsinki, Finland (EU)
Amazon Web Services (S3)	Encrypted off-site backups	Frankfurt, Germany (EU)
Postmark (ActiveCampaign)	Transactional email delivery (welcome, MFA, alerts)	United States
ipapi.co (Kloudend, Inc.)	IP-to-approximate-geo lookup for analytics; queried per unique visitor IP, results cached 24 h	United States
Google Cloud DNS	Authoritative DNS for risk-abc.com	Global anycast
Let's Encrypt (ISRG)	TLS certificate issuance	United States

Sub-processor	Purpose	Location
Axiom	Application log storage (no personal data is logged by design; metadata only)	EU Central 1 (Frankfurt)

We will update this list before we add a new sub-processor or change one. Customers under contract receive advance notice when material changes affect data they entrust to us.

We also disclose information when required by law, by valid legal process, or to protect the rights, property, or safety of ourselves or our users.

9. Where data is stored

Application data is stored in the **European Union**: primary hosting in Finland, encrypted backups in Germany. Some sub-processors (transactional email, IP geo, log storage) operate in the United States — see the table above. When personal data of EU/UK residents is transferred to those US sub-processors we rely on the **EU-U.S. Data Privacy Framework** (where the recipient is certified) and on the **European Commission's Standard Contractual Clauses** together with appropriate supplementary measures.

10. How long we keep data

- **Customer data inside the apps** — kept for the lifetime of the subscription. After cancellation, customer data is retained for **30 calendar days** to allow export, then permanently deleted from active systems. Encrypted backups are deleted under our normal backup-rotation schedule (daily 14 d · monthly 3 m · yearly 1 y).
- **Account records** — deleted within 30 days of account closure.
- **Audit logs** — retained for the same lifetime as the customer's tenant; required for compliance evidence (ISO 27001, SOC 2, CMMC).
- **Analytics events** — retained for **13 months** rolling, then deleted automatically. This window lets us compare year-on-year patterns; it is not extended.
- **Demo-form submissions** — retained for 24 months from last contact, then deleted unless the contact has become a customer.
- **Server logs** — retained for 90 days.
- **Records we are legally required to keep** (tax, accounting, lawful-process responses) — retained for the period required by law.

11. Your rights

Depending on where you live, the law gives you some or all of the following rights over your personal data:

- **Right of access** — request a copy of the personal data we hold about you.
- **Right of rectification** — correct inaccurate or incomplete data.
- **Right of erasure** ("right to be forgotten") — ask us to delete your data, subject to legal retention obligations.

- **Right to restrict processing** — pause our processing while a dispute is resolved.
- **Right to data portability** — receive your data in a structured, machine-readable format.
- **Right to object** — object to processing based on legitimate interests, including the analytics described in Section 6.
- **Right to withdraw consent** where consent is the basis for a particular processing activity.
- **Right to lodge a complaint** with your local supervisory authority (e.g. an EU/EEA Data Protection Authority, the UK ICO).

If you are a user of one of our customers' workspaces, please direct rights requests in the first instance to that customer organization; they are the controller of the data they put into the platform. We will assist them in responding.

12. Making a request

Email privacy@risk-abc.com from the address associated with your account or, if no account exists, from the address you used to contact us. We will respond within 30 days. We may ask for verification information before fulfilling a deletion or access request, to make sure we are responding to the right person.

13. Security

Security details are described in full on our Security page. In summary: TLS in transit, AES-256 encryption for backups and uploaded files, bcrypt-hashed passwords, RS256-signed access tokens with 15-minute expiry, optional and admin-mandatory TOTP MFA, role-based access control, strict least-privilege data isolation between customer organizations, and a per-organization audit log of every privileged action.

14. Children's data

RiskABC is a B2B compliance product. We do not knowingly collect personal information from anyone under 16 years of age. If you believe a child has provided us with personal information, please contact us and we will delete it.

15. Changes to this policy

We may update this policy. The effective date at the top of the page reflects the most recent version. If we make changes that materially affect how we use your personal data, we will notify customers in advance by email and post a prominent notice on our website. We keep a public changelog of versions on request.

16. Contact

For privacy questions, complaints, or rights requests:

- Email: privacy@risk-abc.com
- For security disclosures specifically: security@risk-abc.com

We try to write privacy policies the way we would want to read them. If something here is unclear or you think we got something wrong, please tell us — we will fix it.