Privacy Policy

SanctionCheck.io — operated by Double A Data

Effective date: June 11, 2026

> **Plain-English summary:** You upload names; we screen them; we throw the names away. Screening data (names and match results) is automatically and permanently deleted within 24 hours of job completion. Names are never written to long-term storage. What we keep forever is *metadata only* — when a run happened, how many rows it had, which watchlist versions and engine version were used, and who ran it — so you have an audit trail without us holding your data. **You are the data controller for every name you submit.** You are responsible for having the legal right to screen those names and for your own compliance program. We are a screening tool, not your compliance department.

1. Who We Are

SanctionCheck.io ("the Service") is a sanctions-screening platform operated by Double A Data ("we," "us," "our"). The Service compares names you submit against published government and intergovernmental sanctions watchlists (including OFAC SDN, OFAC Consolidated, UN Security Council Consolidated, UK OFSI, EU CFSP, and US CSL) and returns match-confidence scores.

Contact: support@doubleadata.dev

2. Roles: You Are the Controller, We Are the Processor

This is the most important section of this policy.

When you submit names for screening — individually, by CSV batch, or via API — **you (the customer) are the data controller** of that personal data. **We act solely as a data processor** (or "service provider" under US state privacy laws), processing the names only to perform the screening you requested.

As controller, **you are responsible for:**

- Having a lawful basis to screen each name you submit (under GDPR, UK GDPR, or other applicable law);
- Providing any required notices to the individuals whose names you screen;
- Ensuring the data you upload is accurate, relevant, and limited to what is needed for screening (a full name; do not upload extraneous personal data in passthrough columns unless you need it);

- Responding to data-subject rights requests from the individuals you screen;
- Downloading your results within the 24-hour window — after that, they are unrecoverable by design;
- Determining whether the watchlists you select, your match threshold, and your review process satisfy your legal and regulatory obligations. **We do not determine, warrant, or advise that the Service satisfies your sanctions-compliance obligations.** You select which lists apply and you remain responsible for your compliance program, including human review of matches before taking any adverse action.

We will never use the names you submit to build profiles, train models, market services, or for any purpose other than executing your screening request.

3. What We Collect and Why

3.1 Screening data (submitted by you, deleted within 24 hours)

- **Names** you submit for screening, and any passthrough columns in your CSV.
- **Match results**, including confidence scores and per-judge attribution.

Processing purpose: to run the screening you requested and make results available for download. **Retention:** names are processed in memory and short-term working storage only and are **never persisted to long-term storage**. Match results and downloadable result files are **automatically and permanently purged no later than 24 hours after job completion.** Deletion is irreversible; we cannot recover results after the window closes.

3.2 Run metadata (retained)

For every screening run we record an audit attestation containing: date and time, number of names screened, job status, the watchlist identifiers and versions screened against, the screening engine version, your configured match threshold, and the account/team member who ran it. **This metadata never includes the names themselves or the match results.**

Processing purpose: audit trail, billing, abuse prevention, and service integrity. Attestations are tamper-resistant so that you can demonstrate when a screening occurred and against exactly which list versions. **Retention:** retained for the life of your account and as required for legal and audit purposes thereafter.

3.3 Account and team data (retained while your account is active)

- Name, email address, and login credentials for you and any teammates you invite;
- Team invitations (invitee email and invite token);
- API key names, scopes, environment, and hashed key material (we store only a hash — we cannot recover a lost key);
- Settings such as selected watchlists and match threshold;

- Billing and credit-balance information.

Processing purpose: providing and securing your account, authentication, team management, billing. **Retention:** for the duration of your account plus 30 days after closure, except where longer retention is legally required.

3.4 Technical and usage data

Standard server logs (IP address, timestamps, user agent, request paths) and security telemetry, used for security, debugging, and abuse prevention. Logs do not contain submitted names. Retained for 30 days.

3.5 What we do *not* collect

We do not store submitted names beyond active processing. We do not sell personal data. We do not use submitted screening data for advertising, profiling, analytics, or model training.

4. Retention Summary

Data	Stored?	Retention
Names submitted for screening	In-memory / short-term processing only	Never persisted; purged on completion
Match results & result downloads	Yes, temporarily	Auto-purged ≤ 24 hours after completion
Audit metadata (date, counts, status, list versions, engine version, user)	Yes	Life of account + legal retention
Account, team, API key (hashed), settings, billing	Yes	Life of account + 30 days
Server/security logs (no names)	Yes	30 days

5. Disclosures

We may disclose information where required by law, regulation, legal process, or enforceable governmental request, or to protect the rights, safety, or property of our users or the public. Given the 24-hour purge, in most cases we will hold no screening data responsive to such a request — only run metadata.

We do not sell or share personal data for cross-context behavioral advertising.

6. Security

- All data is encrypted in transit (TLS) and at rest during the temporary processing window.
- API keys are stored as cryptographic hashes only.
- Access to production systems is restricted, logged, and role-based.
- Audit attestations are tamper-resistant.
- Our strongest security control is architectural: **we minimize what exists to be breached.** Names are not retained, so a compromise of stored data cannot expose the individuals you have screened.

No system is perfectly secure; you are responsible for safeguarding your login credentials and API keys.

7. International Transfers

The Service is operated from the United States. If you submit personal data from the EEA, UK, or other jurisdictions with transfer restrictions, you (as controller) are responsible for ensuring a lawful transfer mechanism. We offer a Data Processing Agreement incorporating Standard Contractual Clauses on request at support@doubleadata.dev.

8. Data-Subject Rights

For individuals whose names were screened by one of our customers: the customer who submitted your name is the data controller. Please direct access, correction, deletion, or objection requests to them. Because names are purged within 24 hours and never retained, in nearly all cases we hold no personal data about you by the time a request reaches us; where we do (an in-flight job), we will refer your request to the relevant customer and assist them as processor.

For account holders: you may access, correct, export, or delete your account data at any time via Settings or by contacting [email]. Deleting your account removes account data per Section 3.3; audit metadata may be retained as described above.

Residents of California, Colorado, Virginia, and other US states with privacy statutes, and of the EEA/UK, may have additional statutory rights. We honor verified requests as required by applicable law and will not discriminate against you for exercising them.

9. Sanctions Screening Is Not Automated Decision-Making by Us

The Service produces match-confidence scores; it does not make decisions about any individual. **You must not treat a match score as a determination that a person is a**

sanctioned party. Matches require human review by your team before any action is taken. You are responsible for any decisions made using Service output.

10. Children

The Service is a business tool and is not directed at children under 16. We do not knowingly collect personal data from children as account holders.

11. Cookies

We use only cookies strictly necessary for authentication and session management.

12. Changes to This Policy

We may update this policy from time to time. Material changes will be announced via the dashboard or email to account owners at least [30] days before taking effect. The "Last updated" date above reflects the current version.

13. Contact

Questions, requests, or complaints: support@doubleadata.dev individuals may also lodge a complaint with their supervisory authority.

This document describes how the Service handles data. It does not constitute legal advice to customers, and use of the Service does not create an advisory relationship regarding your sanctions-compliance obligations.