

Privacy Policy

Last updated: August 22, 2026

This Privacy Policy explains how Compliance Platform handles personal data for the public website, account access, support, compliance checks, reports, API use, and organization workspaces.

Controller and privacy contact

Compliance Platform is operated by Norvext SIA, a limited liability company registered in Latvia under registration number 40203766785, with its registered address at Irbju iela 12, Jūrmala, LV-2011, Latvia. Norvext SIA is the controller for the personal data described in this policy.

Privacy requests can be sent through the Contact page or directly to privacy@norvext.com.

If a customer organization uses the platform for its own business data, that organization may act as an independent controller for the data it decides to enter into the platform. Compliance Platform may act as a processor for that customer data under the applicable customer agreement or data processing terms.

The standard Data Processing Terms are available on the DPA page and apply to every plan, including Free and paid plans, whenever the platform processes Customer Personal Data on behalf of an organization.

Norvext SIA acts as controller for the public website, account and workspace administration, billing, support, service security and our customer sanctions due diligence. When a customer organization submits counterparties, people, cases or other content for screening, monitoring, reporting or storage for its own purposes, that customer determines the purposes and means and Norvext SIA acts as its processor under the Data Processing Terms. The same information may be processed in different roles only where the purposes are genuinely different.

Data we process

We process account and profile data such as name, email address, authentication identifiers, organization membership, role, and workspace settings.

We process operational data entered into the platform, including TARIC/CN check inputs, countries, additional codes, entity screening subjects, saved case parameters, generated report metadata, support messages, invitations, API keys metadata, usage events, and audit-style logs needed to operate the service.

We also process technical data such as IP address, device/browser information, security events, request metadata, and error logs where needed for security, abuse prevention, troubleshooting, and service reliability.

Fields marked as required are needed to create and secure an account or workspace, provide the requested feature, or meet billing and customer-screening requirements. Without required account or authentication data we cannot create or provide access to the account. Without the legal name,

registration number, country and required billing address we cannot complete customer sanctions due diligence or activate a paid plan. Optional fields are identified as such.

Why we process data

We use personal data to provide the service, authenticate users, route users to the correct workspace, maintain organizations and access rights, generate reports, answer support requests, secure the platform, and meet legal or contractual obligations.

For B2B customers, some data may be processed on behalf of the customer organization. The customer remains responsible for deciding what business data is entered into the platform.

Legal bases under GDPR

We process account, authentication, workspace, support, and service-use data where processing is necessary to provide the service or take steps before entering into a service relationship (GDPR Article 6(1)(b)).

We process security logs, abuse-prevention data, error logs, product reliability data, and limited operational analytics where necessary for our legitimate interests in securing, maintaining, improving, and protecting the platform (GDPR Article 6(1)(f)).

We process billing, tax, accounting, legal, and compliance records where necessary to comply with legal obligations (GDPR Article 6(1)(c)).

Optional, non-essential processing relies on consent (GDPR Article 6(1)(a)) and can be withdrawn at any time. Today that includes consent-based website analytics and the separate public double-opt-in subscription to operational status notifications. Registered account holders receive routine incident and planned-maintenance service messages by default under the service and legitimate-interest bases described above and can switch them off in account settings. Mandatory security, legal, billing or contractual notices are managed separately. Status notifications are not marketing; any future marketing would require separate consent.

Matching scores, sanctions candidates, risk indicators and AI output support human work; they are not a final legal decision. Norvext SIA does not use solely automated processing to make decisions about an individual that produce legal effects or similarly significant effects. Potential customer sanctions matches require human review and are not automatically rejected. Customer organizations remain responsible for their own compliance decisions made with the service.

If you voluntarily subscribe to status notifications, we process your email address, language, selected incident or maintenance categories, confirmation and unsubscribe state, and limited delivery metadata on the basis of your consent. Double opt-in is required and every operational message includes an unsubscribe link; this subscription is not used for marketing. Unconfirmed requests are deleted after 7 days, an active subscription is kept until you unsubscribe, an unsubscribed address is deleted after 30 days, and delivery logs are kept for 90 days.

Service providers

We use infrastructure and service providers to run the application, store data, authenticate users, deliver email, protect the network, provide the built-in AI assistant and process payments. The providers currently in use or approved are Supabase (managed database, authentication and file storage), Render (screening

and compliance API), Vercel (web application), Cloudflare (DNS, content delivery, network protection and independent status notifications), Resend (transactional and notification email), Anthropic and OpenAI (model providers for the built-in AI assistant) and Stripe (subscription billing). The register published at compliance-mcp.com/subprocessors is the authoritative list and names each provider's role, status, the data involved and its location.

The built-in AI assistant is optional, and there are three different situations. When it runs on the platform's own key, the content you submit in that conversation is sent to the model provider identified as In use in our Subprocessor Register — today OpenAI, in the United States — to generate the reply; Anthropic is an approved alternative, and any switch to it would follow the 30 days' notice set out in the Data Processing Terms. When your organization configures its own provider and API key, that provider processes on your instructions under your own agreement with it, and it is not our subprocessor. When you drive the platform from your own AI client over the API or the MCP connector, we send nothing to any model provider at all. Under the commercial terms that apply to our own use of these services, submitted content is not used to train the provider's models, and screening, cases, reports and the API all work without the assistant.

The public website measures visits with Google Analytics 4, provided by Google Ireland Limited. It runs only where you have accepted the analytics category, so the legal basis is your consent (GDPR Article 6(1)(a)) and you can withdraw it at any time through the cookie banner. What is processed is a browser-level identifier, the pages viewed, the campaign or link that referred you and an approximate location derived from a shortened IP address; we do not send names, email addresses or anything you type into the platform. Google may transfer this data to the United States, relying on the European Commission's adequacy decision for the EU-US Data Privacy Framework. Advertising features and Google Signals are switched off, and the tag is not loaded in the platform application at all, so your screening work stays outside it.

We do not sell personal data. We do not intentionally use advertising profiles or marketing pixels on the public site at launch.

International transfers

The primary database and configured application workloads are hosted in EU regions, but EU hosting does not mean that all processing remains in the European Economic Area. Depending on the feature used, personal data may be processed outside the EEA or through global infrastructure by OpenAI for the optional platform-provided AI assistant, Stripe for billing, Cloudflare for network delivery and protection, and Supabase, Render, Vercel or Resend for support, account, operational or service-delivery data as described in their terms and DPAs. Consent-based Google Analytics may also involve a transfer to the United States. For these transfers we use the safeguards required by GDPR Chapter V, such as European Commission Standard Contractual Clauses, an applicable adequacy decision including the EU-US Data Privacy Framework where the recipient is certified, and supplementary contractual or technical measures. The current provider, role, status and location details are maintained at compliance-mcp.com/subprocessors.

Information about the European Commission Standard Contractual Clauses is available at https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

You may request information about, or a copy of, the transfer safeguard relevant to your data by writing to privacy@norvext.com. We may redact information where reasonably necessary to protect security, confidential information, trade secrets or third-party rights, while still providing a meaningful description of the safeguard.

Retention and security

We keep personal data only for as long as needed for the service, account administration, security, auditability, support, legal obligations, or the applicable customer agreement. The periods below apply from the platform side; a separately signed customer agreement may set different ones.

Screening records, cases and reports remain available in the workspace for the organization's plan retention period: 3 months on Free, 5 years on Starter and Team, 7 years on Professional and Business, and the period agreed in writing for Enterprise. These are service availability settings, not legal advice or a promise that they satisfy a customer's AML, accounting, evidentiary or sector-specific retention duties. The customer must determine its applicable duties and export or delete records accordingly. Deleting a case moves it to workspace trash, where it is permanently deleted after 30 days. Technical execution records are retained for 30 days. Account, billing and tax records are retained while needed for the account and thereafter for periods required by applicable accounting, tax or legal obligations.

We apply access controls, authentication, tenant separation, security checks, HTTPS, and operational logging to protect the platform. No system can be guaranteed perfectly secure, but we design the service with privacy and security as default operating assumptions.

Your rights

Depending on your location and relationship with the service, you may have rights to access, correct, delete, restrict, object to, or receive a copy of your personal data.

To exercise privacy rights, contact us through the Contact page and include the email address used for the platform. If your account belongs to an organization, we may coordinate the request with that organization where required.

If you are in Latvia or believe Latvian data protection law applies, you may lodge a complaint with Datu valsts inspekcija, the Latvian Data State Inspectorate. Website: <https://www.dvi.gov.lv/en>. Email listed by the authority: pasts@dvi.gov.lv.

Where the GDPR applies and its conditions are met, your rights include access, rectification, erasure, restriction, objection and data portability. Where processing relies on your consent, you may withdraw that consent at any time as easily as you gave it, without affecting processing already carried out lawfully before withdrawal. If a customer organization is the controller of the data, contact that organization first; we assist it as processor.

Privacy Policy · Last updated: August 22, 2026

Norvext SIA · 40203766785 · Irbju iela 12, Jūrmala, LV-2011, Latvia · VAT LV40203766785

<https://compliance-mcp.com/privacy>