

Data Processing Terms

Last updated: October 24, 2026

These Data Processing Terms form part of the Terms of Service and apply to every plan, including Free and trial plans, whenever Compliance Platform processes Customer Personal Data on behalf of a customer organization.

1. Parties and scope · GDPR Art. 28(1)

The customer organization is the controller and the legal entity operating Compliance Platform is the processor. These Terms apply to Customer Personal Data submitted to or generated through the service. A separately signed data processing agreement prevails to the extent of any conflict.

Where the customer acts as a processor for another controller, for example when the customer delivers the service to its own regulated clients, the processor acts as a subprocessor. The customer warrants that it is authorized by that controller to engage the processor and to give the instructions issued under these Terms, and remains responsible for passing on that controller's instructions and requests. These Terms then apply between the customer as processor and the processor as subprocessor, and the processor owes no direct obligations to that controller beyond those set out here.

2. Processing details · Annex I · GDPR Art. 28(3)

Processing supports screening, monitoring, case management, reporting, API access and related support for the service term and applicable retention period. It may include collection, storage, organization, search, comparison, disclosure to authorized users, export and deletion. Data subjects may include users, employees, customers, counterparties, beneficial owners and screened persons. Data may include names, aliases, contact details, dates of birth, nationality, identifiers, document numbers, addresses, professional relationships and case or report data.

3. Instructions and customer responsibilities · GDPR Art. 28(3)(a), 29

The processor acts only on documented customer instructions, including use and configuration of the service, unless applicable law requires otherwise. The processor will notify the customer of an unlawful instruction unless prohibited by law. The customer is responsible for lawful collection, notices, legal bases, data minimization and responding to data subjects as controller.

4. Confidentiality and security · Annex II · GDPR Art. 28(3)(b), 32

Persons authorized to process Customer Personal Data are bound by confidentiality. The processor maintains appropriate technical and organizational measures, including access control, authentication, tenant separation, encryption in transit, operational logging, backup and resilience controls. The customer remains responsible for user permissions, credentials and secure use of exports and integrations.

Technical and organizational measures currently in place include: tenant isolation enforced by row-level security in the database; authenticated access through scoped, revocable API keys with per-capability authorization; encryption of data in transit over TLS and encryption at rest by the managed database provider; automated database backups operated by that provider; operational logging and an auditable history of screening activity kept under plan-specific retention periods; and confidentiality obligations for every person with access to Customer Personal Data. Infrastructure is operated through the providers listed in the subprocessor register.

Norvext personnel do not enter a customer organization's workspace on their own initiative. Access for support takes place only after an owner of the customer organization has enabled it in the product for a limited period of at most 30 days, and the customer can revoke it at any time. Such access is read-only, does not occupy a user seat, and every grant, revocation and support session is recorded in the organization's activity log, which the customer can see. Outside this, personnel access Customer Personal Data only to the extent strictly necessary to operate and secure the service, investigate an incident, carry out the customer's documented instructions or comply with the law.

5. Subprocessors and transfers · Annex III · GDPR Art. 28(2), 28(3)(d)

The customer gives general authorization to use subprocessors needed to operate the service. Current categories and providers are described in the Privacy Policy or security materials. The processor imposes equivalent data-protection duties, gives notice of material new subprocessors and considers reasonable objections. International transfers use safeguards required by GDPR Chapter V.

The current subprocessor register, naming each provider and its role, is published at compliance-mcp.com/subprocessors.

Where a subprocessor is located outside the European Economic Area, the transfer is covered by an adequacy decision or by the European Commission's Standard Contractual Clauses concluded with that subprocessor. Documentation of the mechanism relied on for a given subprocessor is available to the customer on request.

We give at least 30 days' notice before a new subprocessor starts processing Customer Personal Data. Notice is given by updating the register at compliance-mcp.com/subprocessors and by email to the owners of the affected workspaces. Where a subprocessor has to be replaced urgently, for example because of a security incident, a provider outage or the discontinuation of a provider's service, we give notice as soon as we reasonably can instead. Within the notice period the customer may object on reasonable data-protection grounds; we will work in good faith towards an alternative, and where none is available the customer may terminate the affected part of the service without penalty and receive a refund of prepaid fees for the unused period.

6. Assistance and incidents · GDPR Art. 28(3)(e)-(f), 33, 35, 36

Taking account of the processing, the processor assists with data-subject requests, security obligations, personal-data-breach notifications, impact assessments and prior consultations. The processor notifies the customer without undue delay after becoming aware of a breach affecting Customer Personal Data and provides available information needed for the customer response.

Security incidents and vulnerability reports concerning the service can be sent to security@norvext.com. Reports received at that address are assessed without undue delay, and the customer is notified of any personal data breach affecting Customer Personal Data.

The processor notifies the customer without undue delay after confirming awareness of a personal data breach affecting Customer Personal Data. The initial notice contains the information then available and does not wait for the investigation to finish; material updates follow in phases. No fixed 72-hour processor deadline applies under these Terms. The customer remains responsible for its own regulatory notification deadlines, and the processor provides reasonable cooperation and available information for that purpose.

7. Return, deletion and retention · GDPR Art. 28(3)(g)

At the end of the service, the processor deletes or returns Customer Personal Data at the customer's choice, unless law requires retention. Residual backup copies are protected and expire through normal backup cycles. The customer should export required records before closing the workspace; plan-specific retention periods continue to apply during service use.

Deletion follows a documented procedure. After a confirmed instruction from a person authorized to act for the customer, the processor completes deletion of Customer Personal Data from production systems within 30 days, unless applicable law requires retention or a shorter period is expressly agreed in writing. Residual copies in protected backups are isolated from ordinary use, are not restored except for disaster recovery, and expire under the infrastructure provider's normal documented backup cycle; if a backup is restored, the deletion instruction is reapplied. The processor may retain a deletion record that identifies the workspace, date and scope but contains no Customer Personal Data. Invoices and payment records remain only where accounting, tax or other law requires retention. The retention period stated for a plan is a floor, not a scheduled deletion date: it is the minimum time already-stored data is kept, and moving to a plan with a shorter stated period does not shorten the retention already applied to data collected under a longer one. Closing an organization deletes its data across the service on the same 30-day timeline described above.

8. Evidence, audits and priority · GDPR Art. 28(3)(h)

The processor provides information reasonably necessary to demonstrate compliance and supports proportionate audits subject to confidentiality, security and operational safeguards. Audits should normally occur no more than once a year unless an incident, authority or material concern requires otherwise. These Terms prevail over the Terms of Service for processor obligations concerning Customer Personal Data.

Where the customer acts as a processor for another controller, information and audit rights are exercised through the customer as a single point of contact, and not separately by each underlying controller.