TAX ROOM

LEGAL · TERMS & POLICIES

Data Security Policy

TaxRoom P/S · De Conincks Vej 13, 2840 Holte, Denmark
CVR: 37918911 · cko@taxroom.dk · https://taxroom.ai

1 Purpose and Scope

This Data Security Policy (the "Policy") describes the principles and controls TaxRoom applies to protect the data entrusted to the TaxRoom platform (the "Platform"). It applies to all data processed by the Platform and to all persons and systems with access to that data.

This Policy supplements, and shall be read together with, the TaxRoom Terms of Use, the Privacy Policy, and any Engagement Letter or Data Processing Agreement in force between TaxRoom and the Client. In the event of any conflict, the provisions of the Engagement Letter or Data Processing Agreement shall prevail.

2 Who We Are

TaxRoom P/S
CVR no. 37 91 89 11
De Coninckx Vej 13
2840 Holte

TaxRoom Komplementar ApS
CVR no. 37 91 85 71
De Coninckx Vej 13
2840 Holte

TaxRoom Tech ApS
CVR no. 37 91 92 68
De Coninckx Vej 13
2840 Holte

Collectively referred to as "TaxRoom"

3 Data Covered by This Policy

TaxRoom processes some of the most confidential information in private markets. For the purposes of this Policy, data on the Platform is classified as follows:

- **Client Data** — the substance of a due diligence engagement: uploaded fund documents, survey questions and responses, tax calculations and tax leakage analyses, structure charts, side letter provisions and negotiation records, and generated reports. Client Data is treated as strictly confidential at all times.
- **Personal Data** — information identifying Users, such as names, email addresses, organization membership, and authentication events, processed in accordance with the EU General Data Protection Regulation (GDPR) and the TaxRoom Privacy Policy.
- **Operational Data** — logs, audit records, and monitoring data generated by the operation of the Platform.

4 Hosting and Data Location

The Platform runs entirely on Microsoft Azure in the EU/EEA. All structured financial data is stored in an encrypted, fully managed database within the European Union, and uploaded documents are stored in Storage with private, non-public access in EU.

No Client Data is stored on local devices or endpoints; all processing occurs server-side. Test and production environments are fully separated, with independent databases, secret vaults, and configuration. Production data is never used for testing.

5 Encryption

- **At rest:** all stored data is encrypted using AES-256, managed by the Azure platform, covering the database, file storage, and secrets vault.
- **In transit:** all data in motion is encrypted using TLS — between the User's browser and the Platform, between the Platform and its database (SSL required on every connection), and between the Platform and any third-party service.
- **Secrets:** credentials and API keys are held in Secured Key Vault under role-based, identity-controlled access and are never stored in application code.

6 Access Control

Access to Client Data follows the principle of least privilege:

- **Authentication.** Every request to the Platform carries a cryptographically signed token that is verified before any data is accessed. Multi-factor authentication is supported and can be enforced at the organization level.
- **Organization membership.** Users must belong to a Client organization to access the Platform. Unaffiliated accounts cannot access any data.
- **Project-level roles.** Within each project, Users hold explicit roles (Admin, Viewer, and the working roles Contributor and Reviewer, assigned per workstream) that determine what they may see and do. Fund users must be explicitly invited to each project; there is no implicit access.
- **Internal access.** TaxRoom personnel access production systems only where necessary for operating and supporting the Platform, through identity-controlled, role-based mechanisms. Any kind of action on the infrastructure is logged with the personnel's personal identity.

7 Data Segregation

Each Client organization maps to exactly one tenant, and every query that retrieves business data is scoped to the requesting User's tenant. Within a project, data is shared only between the specific investor and fund parties linked to that project.

The Platform additionally enforces negotiation confidentiality between the two sides of a project: draft positions, staged decisions, internal review activity, and internal comments belonging to one party are withheld from the other party by the Platform's API until that party deliberately releases them by submitting its response. Nothing crosses between the parties except by an explicit, recorded action.

8 Third-Party Providers

TaxRoom engages a deliberately limited set of sub-processors: Microsoft Azure (hosting), Clerk (authentication), OpenAI (AI-assisted features), and Resend (transactional email). Only Azure and OpenAI process Client Data; data submitted to OpenAI through its API is not used to train OpenAI's models and is retained by OpenAI only for a limited abuse-monitoring period. Deterministic features, including tax leakage calculations, do not use AI and never leave TaxRoom's infrastructure.

The complete list, including data categories and processing locations, is set out in Annex A — Sub-processors to this Policy. New sub-processors are engaged only after due diligence on their security posture and data processing terms.

9 Auditability

Security-relevant actions on the Platform - invitations, membership and role changes, document access grants, side letter decisions and submissions - are recorded in an audit log that cannot be modified or deleted through the application. Each entry records the actor, organization, affected entity, before/after state, and timestamp. Audit records are retained for the life of the engagement. Application monitoring data is retained for 90 days and infrastructure logs for 30 days.

10 Backup and Recovery

The Platform's database is backed up automatically by a managed database service. Secret vault entries are protected by soft delete with a 7-day recovery window.

11 Data Retention and Deletion

Client Data is retained for as long as required to deliver the engagement and thereafter as required by law or agreed in the Engagement Letter. Upon termination and written request, TaxRoom will delete or return Client Data in accordance with the Data Processing Agreement.

12 Secure Development and Change Management

- All infrastructure is defined as code, version-controlled, and scanned by automated security tooling before any change reaches production.
- Deployments authenticate using short-lived tokens; no long-lived credentials are stored in the delivery pipeline.
- Changes must pass automated tests and the test environment before manual approval into production.
- Third-party dependencies are monitored continuously for known vulnerabilities, with updates proposed through reviewed pull requests.

13 Incident Response

TaxRoom monitors the Platform continuously for errors, anomalies, and availability. In the event of a security incident affecting Client Data, TaxRoom will:

- contain and investigate the incident without undue delay;
- notify affected Clients without undue delay, and in any event within the timeframe required by the GDPR and any applicable Data Processing Agreement;
- remediate the root cause and record the incident, its impact, and the corrective actions taken.

Suspected vulnerabilities can be reported to security@taxroom.ai TaxRoom asks that issues be reported privately and that reasonable time be allowed for investigation and remediation before any public disclosure.

14 Responsibilities of Users and Clients

Security of the engagement is shared. Clients are responsible for managing their own User accounts, assigning appropriate project roles, enforcing multi-factor authentication within their organization, and ensuring that Users access the Platform only for its intended purpose. Users must keep their credentials confidential and must not attempt to access data belonging to other tenants or projects.

15 Company Information

TaxRoom P/S
De Conincks Vej 13
2840 Holte, Denmark
CVR: 37918911
Email: cko@taxroom.dk
Website: https://taxroom.ai

ANNEX A

Sub-processors

TaxRoom engages a small, deliberately limited set of third-party service providers ("sub-processors") to deliver its services. This Annex lists the sub-processors we use, what they process, and where processing takes place.

What is a sub-processor?

When TaxRoom processes personal data on behalf of its customers, TaxRoom acts as a data processor under the EU General Data Protection Regulation (GDPR). Where TaxRoom engages a third-party service provider that has, or may have, access to that personal data, the GDPR refers to that provider as a sub-processor (Article 28 GDPR).

Every sub-processor listed below is bound by contract terms designed to ensure that personal data is processed only for the purpose of providing services to TaxRoom, and in accordance with our commitments to customers and applicable data protection law.

Due diligence

Before engaging any sub-processor, TaxRoom performs due diligence on the provider, including a review of its security posture, certifications, and data processing terms. Sub-processors are engaged only where the service they provide is necessary for delivering the TaxRoom platform.

List of sub-processors

SUB-PROCESSOR	PURPOSE	DATA CATEGORIES PROCESSED	LOCATION
Microsoft Azure (Microsoft Ireland Operations Ltd.)	Cloud hosting: application compute, PostgreSQL database, file (blob) storage, secret management, monitoring	All customer data stored on the platform, including financial documents, tax data, survey responses, and user account references	EU/EEA
Clerk (Clerk, Inc.)	Authentication and identity management	User identity data: name, email address, organization membership, authentication events. No financial data or documents.	EU/EEA
OpenAI (OpenAI, L.L.C.)	AI-assisted features: document evaluation, survey answer suggestions, structure chart extraction, report content generation	Uploaded documents and document content, extracted text, survey questions and answers, and project context submitted when AI features are used. Not used by OpenAI for model training; retained by OpenAI only for a limited abuse-monitoring period.	EU/EEA
Resend (Plus Five Five, Inc.)	Transactional email delivery (invitations, notifications)	Recipient email addresses, invitation details, notification content. No financial documents or survey data.	EU/EEA

No other third-party service provider receives customer data.

International data transfers

Where a sub-processor processes personal data outside the European Economic Area, TaxRoom ensures that appropriate safeguards are in place as required by Chapter V of the GDPR.

Changes to this list

Our business needs and service providers may change over time. We will update this Annex when we add, replace, or remove a sub-processor.