Syncura

Syncura Security and Compliance Overview

Purpose

This document provides an overview of Syncura's security posture, data handling practices, and compliance approach. It is intended to support customer security reviews, procurement diligence, and pre-sales discussions.

This document is **informational and non-contractual**. Binding security, privacy, and data protection obligations are governed by the SaaS Subscription Agreement, Data Processing Agreement (DPA), and any applicable addenda.

The Syncura platform is designed to support secure document processing while maintaining appropriate data retention capabilities required for search, audit, and operational workflows.

1. Security Governance

Syncura designs and operates its platform with security as a core architectural principle. Security responsibilities are shared across engineering, operations, and leadership, with oversight aligned to industry best practices.

Key principles include:

- least-privilege access controls,
- defense-in-depth architecture,
- separation of customer environments,
- continuous monitoring and improvement.

2. Data Handling and Processing Model

2.1 Data Flow Overview

Customer data is processed solely for the purpose of delivering the Syncura service. Data flows are designed to support reliable processing, searchability, monitoring, and auditability while maintaining strong security controls and minimizing unnecessary exposure.

2.2 Data Retention and Storage

Syncura retains Customer Data within the service environment as necessary to support core platform capabilities, including document search, auditability, workflow monitoring, and service reliability.

Customer Data and processing outputs may be stored within the service for the duration of the customer's subscription or for a defined retention period agreed during onboarding.

Retention practices are designed to balance operational functionality with data minimization principles. Where appropriate, customers may configure or request specific retention periods aligned with their internal governance or regulatory requirements.

Operational details, retention behavior, and configuration options may vary by deployment model and customer requirements and are documented as part of onboarding and security review.

2.3 Metadata and Logs

Syncura may retain limited non-content metadata required for:

- usage metering and billing,
- service reliability and performance monitoring,
- security detection and incident investigation.

Such metadata may include operational information related to processed documents and workflows but is retained solely for service delivery, monitoring, and security purposes.

2.4 Data Lifecycle Management

Syncura manages Customer Data through defined lifecycle practices including ingestion, processing, storage, retrieval, and deletion. Data retention and deletion policies are implemented through platform controls and operational procedures designed to support both customer operational needs and applicable regulatory expectations.

Upon termination of the applicable subscription, Customer Data may be deleted or returned to the customer in accordance with the SaaS Subscription Agreement and Data Processing Agreement.

3. Data Security Controls

3.1 Access Controls

- Role-based access control (RBAC)

- Multi-factor authentication for administrative access
- Access granted on a least-privilege basis

3.2 Encryption

- Encryption in transit using industry-standard protocols
- Encryption at rest for systems storing Customer Data and service outputs
- Secure key management practices

Encryption at rest is applied to systems storing Customer Data and service outputs using industry-standard encryption mechanisms.

3.3 Environment Isolation

- Logical isolation between customer environments
- Segmentation of processing, storage, and management systems

4. Incident Response

Syncura maintains incident response procedures designed to detect, respond to, and remediate security incidents.

- Continuous monitoring for suspicious activity
- Defined escalation and response processes
- Customer notification in accordance with contractual and legal obligations

5. Subprocessors and Third-Party Services

Syncura may rely on vetted third-party service providers (for example, cloud infrastructure providers) to deliver the service.

- Subprocessors are subject to contractual security and confidentiality obligations
- Syncura remains responsible for its subprocessors in accordance with applicable agreements

Syncura

6. Compliance Approach

Syncura's security and privacy program is designed to support customers operating in regulated industries and across multiple jurisdictions. Syncura does not provide blanket regulatory certifications unless formally audited; instead, it aligns its controls, processes, and contractual commitments to recognized regulatory and industry standards.

6.1 Industry Regulatory Alignment

Financial Services and Insurance

Syncura supports customer compliance with financial services and insurance regulations, including requirements related to safeguarding non-public personal information and sensitive financial records. Security practices are designed to align with expectations under regulations such as the U.S. Gramm–Leach–Bliley Act (GLBA) and insurance data security model laws, where applicable.

Healthcare

Syncura may support healthcare use cases involving protected health information (PHI) when acting as a Business Associate pursuant to a separately executed Business Associate Agreement (BAA). HIPAA obligations apply only to the scope and deployment defined in the BAA.

Logistics and Supply Chain

Syncura supports customers handling operationally sensitive trade, shipping, and logistics documentation by applying strong access controls, data minimization, and incident response practices aligned with industry expectations.

6.2 Privacy and Data Protection Laws

Syncura supports customer compliance with applicable privacy and data protection laws, including:

- **European Union:** General Data Protection Regulation (GDPR)
- **United Kingdom:** UK GDPR
- **Switzerland:** Swiss Federal Act on Data Protection (revFADP)
- **Canada:** PIPEDA and applicable provincial privacy legislation
- **United States:** Applicable federal and state privacy laws, including CCPA/CPRA

Data processing obligations are governed contractually through the Data Processing Agreement (DPA).

6.3 International Data Transfers

Where Personal Data is transferred across borders, Syncura implements appropriate safeguards consistent with Applicable Data Protection Laws, such as standard contractual clauses or equivalent mechanisms, as reflected in the DPA.

6.4 Security Framework Alignment

Syncura aligns its security program with recognized industry frameworks, including:

- SOC 2 Trust Services Criteria (security, availability, confidentiality)
- ISO/IEC 27001 principles
- NIST Cybersecurity Framework

Formal certifications may be pursued as the company matures.

7. Customer Responsibilities

Customers are responsible for:

- determining the suitability of the service for their use case,
- configuring workflows and validation controls,
- managing user access and credentials,
- retrieving and storing Outputs outside the service.

Customers are responsible for defining appropriate data retention and governance policies for documents processed through the service.

8. Continuous Improvement

Syncura continuously evaluates and enhances its security and compliance practices in response to evolving threats, customer feedback, and regulatory developments.

9. Questions and Reviews

Additional security documentation, questionnaires, or clarifications may be provided upon reasonable request during the sales or onboarding process.