



PhoenixX Data Retention & Evidence Preservation Policy

Document Reference: PHX-DREP-1.0



PhoenixX Data Retention & Evidence Preservation Policy

Reference: PHX-DREP-1.0

Document Version: 1.0

Effective Date: 1 November 2025

Governing Law: Swiss Substantive Law

Dispute Resolution: Zurich Arbitration (Swiss Rules)

Issued By: Agency PhoenixX LLC

Domain: PhoenixX.one

Document Classification

This document is a legally binding corporate retention and evidence governance policy. It defines mandatory retention periods, deletion controls, legal hold obligations and forensic evidence preservation rules for PhoenixX Systems.

Confidentiality Level: Internal – Legal Compliance Document

Applies To: PhoenixX Systems, Clients, Users, Suppliers, Subcontractors and Compliance Operations

Status: Approved by PhoenixX Compliance & Risk Management

1. Purpose and Legal Effect

This Data Retention & Evidence Preservation Policy ("Policy") establishes the binding framework for retention, preservation and lawful destruction of data processed by PhoenixX. This Policy ensures compliance with statutory retention periods, evidence preservation requirements, arbitration readiness, artificial intelligence model integrity and fraud enforcement. This Policy prevails over any contract term, data request or deletion demand that conflicts with legal retention obligations or security requirements.

2. Scope and Applicability

This Policy applies to all data processed, generated, received or stored within PhoenixX Systems, including operational logs, transactional records, AI training data, derived data, moderation data, audit trails, legal records, financial records and investigation records. This Policy applies to PhoenixX, Clients, Users, Suppliers, Subcontractors and third-party processors engaged by PhoenixX.



3. Data Categories Covered by This Policy

This Policy applies to all categories of data Processed by PhoenixX, including Operational Data, Transaction Data, Compliance Data, Audit Logs, Security Records, Client Submission Data, Supplier Data, Derived Data, Moderation Data, AI Training Data, Annotation Records, Payment Records, Contractual Records, Communication Archives and Legal Hold Records. This Policy also applies to Sensitive Data and Erotic Data under lawful Processing in accordance with PhoenixX Privacy Policy Annex B.

4. Legal Basis for Retention

PhoenixX retains data in accordance with Article 6(1)(b), (c) and (f) GDPR, Article 17(3) GDPR, Articles 25–27 of the Swiss FADP, U.S. Federal Evidence Rules, EU AML Directives, Swiss AMLA, FATF Recommendations, and PhoenixX Arbitration Rights. PhoenixX may retain data to comply with legal obligations, enforce contracts, prevent fraud, preserve evidence, defend legal claims, ensure AI model integrity and comply with AML/CTF requirements. PhoenixX shall not be compelled to erase data that is subject to contractual enforcement, fraud investigation, legal hold, arbitration evidence or legitimate business necessity.

5. Data Retention Schedule

PhoenixX applies category-based retention periods as follows:

Data Type	Retention Period
Business Contracts & Records	10 years (commercial law)
Transaction Logs & Payment Records	10 years (AML/Tax law)
Compliance & Verification (KYC/KYB/UBO)	10 years (AML/FINMA)
Audit Logs & Access Records	7–10 years
Enforcement Evidence & Blacklist Records	Retained indefinitely (RET3)
Derived Data & Risk Intelligence	Retained indefinitely
AI Training Data & Model Metadata	Retained indefinitely (AI-RET3)
Security Logs & System Traces	5–10 years
Legal Hold Records	Until Legal Hold is released

PhoenixX may apply extended retention where legal or business necessity exists, including fraud, security risk, litigation or arbitration.



6. Legal Hold & Evidence Preservation

PhoenixX may impose a Legal Hold to preserve records relevant to disputes, investigations, fraud reviews, compliance audits or arbitration. When Legal Hold applies, affected data shall not be deleted, altered or destroyed until formally released by PhoenixX Compliance & Risk Management. Legal Hold overrides any deletion request, data export request or privacy objection. Legal Hold enforcement applies to all Clients, Users, Suppliers and Subcontractors.

7. Data Deletion and Restriction Requests

PhoenixX may accept requests to delete or restrict data where legally permissible; however, PhoenixX is not obligated to delete data that must be retained under legal, regulatory, contractual or enforcement obligations. PhoenixX may decline deletion requests where retention is necessary for compliance with GDPR Article 17(3), Swiss FADP Article 32, AMLA, FATF, contractual enforcement, fraud monitoring or AI model integrity.

8. Exceptions to Deletion

PhoenixX shall not delete data where it is required for: (a) fraud prevention; (b) AML/CTF and sanctions compliance; (c) commercial dispute resolution; (d) arbitration or litigation; (e) contractual enforcement; (f) audit obligations; (g) AI system security; or (h) compliance reporting. PhoenixX rejects any misuse of data rights to avoid legal responsibility, system enforcement or fraud investigation.

9. Evidence Chain of Custody

PhoenixX maintains forensic chain of custody procedures for legal and arbitration evidence. PhoenixX may preserve system metadata, audit logs, communication records, AI interaction traces, files, annotations, risk alerts and internal review records. Evidence preservation includes hash verification and timestamp logging where applicable.

10. Storage Location and Security Controls

Data retained under this Policy may be stored securely in PhoenixX-controlled infrastructure located in approved jurisdictions, including Switzerland, the United States and the European Union. Storage is protected using encryption, access control, audit logging and risk monitoring consistent with PhoenixX Security Standards.

11. Third-Party Processor Retention Rules

PhoenixX sub-processors and storage partners must comply with this Policy and ensure data retention in accordance with legal retention schedules and Legal Hold obligations. PhoenixX may audit sub-processors for compliance.

12. Law Enforcement Cooperation and Arbitration Evidence

PhoenixX may preserve and provide retained data to competent authorities where legally required. PhoenixX cooperates with INTERPOL, EUROPOL, national FIUs, cybercrime units, NCMEC, OFAC and SECO in lawful investigations. Retention obligations survive termination of account or contract and remain enforceable for arbitration defense.

Approval and Enforcement





This Data Retention & Evidence Preservation Policy – PHX-DREP-1.0 is binding across all PhoenixX operations. Retention obligations apply to all Clients, Users, Suppliers and Subcontractors without exception.

Approved by: PhoenixX Compliance & Risk Management

Agency PhoenixX LLC

PhoenixX.one

legal@PhoenixX.one | compliance@PhoenixX.one

© 2025 Agency PhoenixX LLC – A Wyoming Limited Liability Company | All Rights Reserved Governing Law: Swiss Substantive Law | Dispute Resolution: Zurich Arbitration (Swiss Rules)



+1 307 302 4642
info@phoenixx.one
www.phoenixx.one

2106 House Ave Suite 226
Cheyenne 82001 WY / USA