Synthetic Users Compliance Policy

Version: 1.0

Effective Date: 25 March 2026

Last Reviewed: 25 March 2026

Owner: CTO & CISO — Artur Ventura

Approved by: CEO — Kwame Ferreira

Review Frequency: Annually

Classification: Internal — Confidential

CRA Reference: 23.1.1

---

1. Purpose

This policy establishes Synthetic Users' commitment to complying with all applicable laws, regulations, industry standards, and contractual obligations relevant to our operations, data processing, and service delivery.

---

2. Scope

This policy applies to all Synthetic Users employees, contractors, and third parties who access company systems or data. It covers all business operations, products, and services, including the AI-powered synthetic user research platform.

---

3. Regulatory & Legal Compliance

Synthetic Users complies with the following regulatory frameworks:

3.1 Data Protection & Privacy

- **General Data Protection Regulation (GDPR)** — As a company with operations in Portugal (EU) and customers globally, Synthetic Users complies with GDPR requirements for data processing, data subject rights, cross-border transfers, and breach notification.
- **California Consumer Privacy Act (CCPA)** — Applicable to California-based customers and users.
- **Data Processing Addendums (DPAs)** — Maintained with all subprocessors and enterprise clients, including provisions for data handling, retention, deletion, and breach notification.

3.2 Information Security Standards

- **SOC 2 Type II** — Synthetic Users maintains SOC 2 Type II certification, with annual audits conducted by an independent third-party auditor. The most recent report covers the Trust Services Criteria: Security, Availability, and Confidentiality.
- **ISO 27001** — Security controls are aligned with ISO 27001 requirements through our Information Security Management System (ISMS).

3.3 Industry-Specific Compliance

- **Financial Services (JPMC SCA)** — For engagements with regulated financial institutions, Synthetic Users complies with applicable Supplier Cybersecurity Assessment (SCA) requirements, including AI/GenAI-specific controls.
- **AI/GenAI Governance** — AI systems are governed by documented policies covering algorithm design, data flow, model validation, change management, incident response, and decommissioning.

4. Contractual Compliance

Synthetic Users maintains compliance with all contractual obligations, including:

- **Service Level Agreements (SLAs)** — Monitored through observability and monitoring tools. SLA performance tracked and reported.
- **Client-Specific Requirements** — Enterprise client security and compliance requirements are tracked, assessed, and incorporated into operational controls.
- **Subprocessor Agreements** — All third-party providers operate under DPAs with defined security, privacy, and data handling requirements. Third-party risk is assessed and tiered (High/Medium/Low) per the Third-Party Risk Management Policy.
- **Incident Notification** — Contractual incident notification obligations (e.g., JPMC 72-hour notification) are documented in the Incident Response Plan and tracked during exercises.

5. Internal Compliance Controls

5.1 Policies & Procedures

Synthetic Users maintains a comprehensive set of security, privacy, and operational policies. All policies are:

- Reviewed at least annually
- Approved by the CTO or CEO
- Communicated to all employees during onboarding and through annual awareness training
- Stored centrally and accessible to all authorized personnel

5.2 Employee Training & Awareness

- All employees complete mandatory annual Security Awareness Training, which includes compliance obligations, data protection, acceptable use, and AI/GenAI

security.

- Training completion is tracked via Google Forms and monitored by the Security Lead / CTO.
- New employees receive compliance training as part of onboarding.

5.3 Access Control & Segregation

- Role-based access control (RBAC) and least-privilege principles are enforced across all systems.
- Privileged access is separated from day-to-day accounts.
- Access is reviewed semi-annually per the Access Rights Review Policy.

5.4 Change Management

- All changes to production systems, including AI/GenAI components, follow the documented Change Management Policy.
- Changes are authorized, tested, and logged before deployment.

---

6. Monitoring & Audit

6.1 Continuous Monitoring

- Security controls are continuously monitored through Sprinto (compliance automation), centralized logging (PaperTrail, Axiom), and infrastructure monitoring.
- Compliance status is tracked in Sprinto with automated evidence collection.

6.2 Internal Audits

- Internal compliance audits are conducted annually, covering security controls, access management, data handling, and policy adherence.
- Findings are documented, risk-rated, and tracked to remediation.

6.3 External Audits

- SOC 2 Type II audits are conducted annually by an independent auditor.
- Penetration testing is conducted at least annually by an independent third party (most recent: Bulletproof/Worknest, 2025).

---

7. Non-Compliance & Remediation

- Non-compliance findings from audits, assessments, or monitoring are documented and assigned to a responsible owner.
- Remediation plans are established with target dates and tracked to closure.
- Material non-compliance is escalated to the CTO and, where required, to the CEO and affected clients.
- Employees who violate compliance policies are subject to disciplinary action per the Employee Code of Conduct.

---

8. Anti-Bribery & Anti-Corruption

Synthetic Users maintains a zero-tolerance policy for bribery and corruption. All employees and third parties must comply with the standalone Anti-Bribery & Anti-Corruption Policy, which prohibits facilitation payments, improper gifts, and conflicts of interest.

---

9. Related Documents

- SOC 2 Type II Report
- Anti-Bribery & Anti-Corruption Policy
- Privacy Policy
- Data Processing Addendum

- Incident Response Plan
- Third-Party Risk Management Policy
- Change Management Policy
- Access Rights Review Policy
- User Awareness Training Program
- Employee Code of Conduct

---

10. Review Schedule

This policy is reviewed annually or upon material changes to regulatory requirements, business operations, or client obligations. Next scheduled review: **March 2027**.