CONTROL MAPPING DOCUMENT

Line-by-Line Control Mapping Across Frameworks

A full control-by-control mapping across SOC 2, ISO 27001, GDPR, CCPA, and the EU AI Act — with the ZoikoTime implementation and the evidence generated for each mapped control.

SOC 2 Type II | ISO 27001 | GDPR | CCPA | EU AI Act

ZoikoTime™ · **Workforce Truth Infrastructure**

Version 2026.1 · August 17, 2026 · **Confidential**

SCOPE & METHOD

How to read this mapping

Each control domain lists the corresponding SOC 2 criterion, ISO 27001 Annex A reference, and applicable GDPR article, followed by how ZoikoTime implements the control and the evidence it produces. References indicate alignment; they are not a claim of certification for any specific customer environment.

CONTROL DOMAIN	SOC 2	ISO 27001	GDPR	IMPLEMENTATION IN ZOIKOTIME	EVIDENCE GENERATED
Access Control	CC6.1	A.9	Art. 32	Role-based access control, SSO/SAML, and session-identity validation enforced at the platform level.	Access logs, RBAC role assignments, session identity records.
Data Protection	CC6.7	A.8	Art. 5, 32	AES-256 encryption in transit and at rest; data-minimization enforced by policy.	Encryption configuration, data-inventory, minimization policy version.
Audit Logging	CC7.2	A.12	Art. 30	Immutable, append-only audit logs and a processing-activity register.	Tamper-evident log exports, records of processing (RoPA).
Continuous Monitoring	CC7.1	A.12	—	Real-time anomaly detection and risk-indicator monitoring with escalation.	Anomaly events, alert history, escalation trail.
Data Subject Rights	—	A.18	Art. 15–22	Rights-execution workflows (access, rectification, erasure, portability) with request tracking.	DSAR request register, fulfilment timestamps, outcome records.
Incident & Breach Mgmt	CC7.3	A.16	Art. 33	Automated breach detection with a 72-hour notification workflow and case tracking.	Incident timeline, notification records, post-incident review.
Human Oversight (AI)	CC7.1	A.5	EU AI Act §14	Assistive AI is bounded and non-decisional; humans confirm consequential outcomes.	Human-review flags, decision-authority audit, model-scope statement.
Retention & Deletion	CC6.5	A.8	Art. 5(1)(e)	Configurable retention and deletion by data type within governed limits.	Retention policy version, deletion job logs.

Evidence linkage. Every control above is linked to structured, timestamped records generated during normal operation, so the mapping can be demonstrated rather than asserted.

Per-framework alignment summary

SOC 2 Type II

Controls span the Security, Availability, Confidentiality, and Processing-Integrity criteria and are designed to operate continuously so they can be examined over a period rather than at a point in time.

ISO 27001

Controls align to Annex A domains including access control (A.9), operations security (A.12), supplier and incident management (A.15/A.16), and compliance (A.18).

GDPR & CCPA/CPRA

Lawful-basis handling, data-subject/consumer rights workflows, records of processing, and breach-notification timelines are supported and evidenced.

EU AI Act

ZoikoTime's AI is assistive and non-decisional. Transparency and human-oversight controls are documented; the system never determines misconduct, pay, or discipline.

> **Limitations.** Control references indicate design alignment. Applicability, scope boundaries, and certification status depend on the specific deployment and are confirmed through the governed review process. This document is not legal advice.