

GDPR Compliance Chart - GateKeeper Enterprise

Article 32 Compliance Description: Data security measures should, at a minimum, allow:

1. Pseudonymizing or encrypting personal data.	2. Maintaining ongoing confidentiality, integrity, availability, access, and resilience of processing systems and services.	3. Restoring the availability of and access to personal data, in the event of a physical or technical security breach.	4. Testing and evaluating the effectiveness of technical and organization measures.
--	---	--	---

Article 32 Compliance Methods by GateKeeper:

Requirement	Description	Article Number	GateKeeper
Change Management	Monitors, logs, and reports changes. Shows compliance auditors that changes to the actions can be traced.	32	GateKeeper is a proximity-based identification and authentication solution using a physical token. A user must be physically present to access a workstation. Audit logs of physical access using GateKeeper are stored indefinitely on the GateKeeper Enterprise server. Additionally, GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. These audit logs are retained indefinitely. GateKeeper can connect to a syslog server and integrate with an enterprise security architecture. Authorized admins have the ability to export audit logs to further enable audit review, analysis, and reporting processes.
Data Masking	Anonymizes data via encryption/hashing, generalization, perturbation, etc. Pseudonymizes data by replacing sensitive data with realistic fictional data that maintains operational and statistical accuracy.	32	GateKeeper uses military-grade AES-256 to store and transmit passwords, PIN logins are obscured, and all authentication information is obscured.
User Rights Management	Identifies excessive, inappropriate, and unused privileges.	32	GateKeeper Enterprise provides proximity-based authentication and authorization to workstations. Using GateKeeper Enterprise, an organization can granularly assign access permissions to individuals/groups on a per workstation basis. This helps enforce the concept of least privilege on a system level.

User Tracking	Maps end user to the system or data accessed.	32	GateKeeper Enterprise provides robust auditing capabilities that identifies when an individual user was in proximity to a workstation and successfully locked/unlocked it. These audit logs are retained indefinitely.
---------------	---	----	--