NAERON LEGAL & CYBERSECURITY ASSURANCE

DATA SECURITY, PROTECTION & RETENTION POLICY

A Comprehensive Guide to Cloud Data Protection, Multi-Tenancy Isolation, Regulatory Archiving & Destruction Protocols

Document Reference: NAER-POL-2026-V1	**Regulatory Alignments: GDPR, KVKK, SHGM, EASA**
Effective Date: August 22, 2026	**Target Audience: Aviation Academies, Flight Instructors, Students**
Policy Owner: Data Protection Committee	**Last Updated: November 25, 2025**

1. Background and Purpose

Naeron Flight School Management System is a specialized aviation software-as-a-service (SaaS) platform built to digitize and manage complex operations of flight academies and aviation universities. Since its launch in 2015, Naeron has accumulated a robust digital memory, successfully managing over **1,194,255 flight hours**, **859,214 sorties**, 12 active aviation institutions, and 16,826 registered student pilots.

The aviation sector demands unparalleled precision, traceability, and confidentiality. In accordance with Turkish Personal Data Protection Law (**KVKK No. 6698**), the European Union General Data Protection Regulation (**GDPR**), and civil aviation authorities (**SHGM, EASA**), Naeron enforces strict data governance, cryptographic isolation, and rigorous retention rules to safeguard critical pilot logbooks, personnel records, and maintenance logs.

2. Data Categorization & Classification

Naeron collects and processes multiple categories of operational and personal data to deliver seamless pilot training administration and ensure legal compliance with aviation regulations. All data categories are rigorously mapped and restricted:

Veri Kategorisi / Data Category	Core Elements	Legal Base (GDPR/KVKK)	Access Restriction Level
Identity Data (Kimlik Bilgileri)	Full name, National ID / T.C. Kimlik No, passport number, birth date.	Legitimate Interest & Contract Fulfilment	RESTRICTED (HR & School Admin Only)
Contact Data (■leti■im Bilgileri)	Email address, phone number, physical home/billing address.	Contract Fulfilment (Art. 6 GDPR)	RESTRICTED (Instructors & Admin)
Aviation & Training Records	Student logs (logbook), flight hours, sorties, flight instructor assessments, theoretical exam scores.	Legal Obligation (SHGM/EASA Compliance)	INTERNAL (Assigned Instructors, Quality Dept, ATO)
Medical Certificates & Licenses	FAA/EASA Medical Class Class-1/Class-2 documents, license categories, expiry dates.	Legal Obligation & Consent	HIGHLY CONFIDENTIAL (Chief Flight Instructor & HR)
Technical Logs	IP addresses, browser finger-printing, device identifiers, audit logs.	Legitimate Interest (Security Monitoring)	CONFIDENTIAL (Naeron Security & Ops)

Data Minimization Principle:

Naeron operates strictly under the **Data Minimization Principle**. Only data strictly required for flight roster execution, licensing checks, quality management, and regulatory SHGM/EASA filing is collected and maintained. Unnecessary personal data, such as general social media accounts or private communication records, is never processed.

3. Technical Data Protection & Security Controls

To guarantee the confidentiality, availability, and resilience of aviation information, Naeron enforces standard-compliant defenses across application, database, and infrastructure layers:

Layer	Technical Implementation	Siber Güvenlik Faydas■ / Benefit
Cloud Hosting	Hosted on **Google Cloud Platform (GCP)**. Redundant database clustering and private container virtualization.	Protects physical assets and guarantees 99.9% application uptime.
Data Encryption	Encryption at rest (**AES-256**) and in transit via TLS v1.3. Direct database communication is protected via SSL certificates.	Neutralizes risk of raw data sniffing and raw database exposure.
Hashing (Parola)	All system credentials and passwords are compiled using the **bcrypt** algorithm with high iteration factor.	Renders password brute-forcing mathematically unfeasible.
Multi-Tenant Isolation	Each flight academy's schema is isolated logically via database tenant middleware.	Absolute protection against cross-school BOLA/IDOR data leakages.
Session Defense	Asymmetric **RSA-3072** JWTs are verified cryptographically. Session revocation is executed via Redis.	Improves security against session Hijacking and brute-forced tokens.
Disaster Recovery	**Co■rafi Yedekleme (Geographical Redundancy)** with real-time replication across multiple GCP European datacenters.	Eliminates single points of failure, ensuring data preservation during disasters.

Security Audits:

Naeron conducts regular, third-party security audits of its API endpoints and cloud configurations. Any detected minor optimizations are addressed instantly through continuous deployment pipelines, guaranteeing zero-vulnerability operational stability.

4. Data Retention & Archiving Periods

Aviation training organizations operate under stringent legal archiving structures. Records cannot be deleted prematurely, as they must remain accessible for regular SHGM (Turkish Civil Aviation) and EASA audits. Below are the legally approved retention periods:

Record Category	Retention Period	Regulatory Justification	Destruction Trigger
Pilot Logbooks & Flight Records (Sorti)	10 Years (or Permanent)	SHGM SHT-1A / EASA Part-FCL audit requirements.	Archived to secondary read-only cold storage after 10 years.
Student Progress Reports	5 Years	Required by EASA/SHGM to prove training curriculum completion.	Purged completely or anonymized 5 years after student graduation.
Theoretical Exams	5 Years	Required to verify course completions and safety exam success.	Securely purged from active Postgres database tables after 5 years.
Inactive Accounts (Pasif Hesaplar)	2 Years	GDPR/KVKK storage limitation rules.	Deleted after 2 years of complete inactivity, following warning email.
Financial Records (Billing & Contracts)	10 Years	Turkish Commercial Code & Tax Regulations.	Physically and digitally purged 10 years after final billing statement.
System Audit Logs	1 Year	Security monitoring and log preservation legislation.	Overwritten automatically on a rolling 365-day basis.

Archiving Standard:

Active databases only maintain the last 2-3 years of active schedules to preserve performance. Older records are systematically moved to a cold GCP Storage tier. Archived records carry the exact same cryptographic hash, ensuring they are tamper-proof and authentic.

5. Data Destruction & 'Right to be Forgotten' Protocols

When data reaches its maximum retention period or when a pilot exercises their GDPR/KVKK **Unutulma Hakk■ (Right to be Forgotten)**, Naeron follows strict deletion protocols. Note that aviation training regulatory guidelines take precedence over standard personal data deletion requests under GDPR Article 17(3)(b).

Stage / Step	Action Performed	Execution Protocol & Verification
1. Request Receipt	The user submits a deletion request to privacy@naeron.com.	Verified by the Data Protection Officer (DPO). The user's active pilot status and school boundaries are validated.
2. Legal Screening	Evaluate if active SHGM / EASA archiving obligations are active.	If a pilot completed flight training within 5 years, personal identity can be anonymized, but flight logs are preserved (anonymously) for audit compliance.
3. Logical Soft-Delete	Flag records as 'is_deleted = true' in the primary database schema.	Instantly hides records from all active front-end views, mobile devices, and Naeron ME application modules.
4. Hard Deletion	Database script purges rows permanently from Postgres databases.	Overwrites database blocks. Any linked active Redis cache entries are purged instantly.
5. Backups Purge	Overwrites backup datasets over standard cycle period.	Secondary backups are naturally overwritten on a rolling 30-day lifecycle. Cold archives are destroyed securely.
6. Notification	Official confirmation notice is dispatched.	DPO issues a secure email validating that the data has been legally purged, anonymized, or destroyed.

Anonymization Policy:

In cases where total data purge is blocked by civil aviation law, Naeron implements strict **Anonymization Protocols**. Personally identifiable columns (such as names, IDs, emails) are completely stripped and replaced with irreversible hash keys. The remaining logs (sorties, hours, training assessments) are preserved purely as anonymous statistics, ensuring zero leakage of student identities.

6. Shared Responsibility Model & Sign-Off

As a SaaS provider, Naeron implements state-of-the-art defenses across hosting infrastructure and core applications. However, data safety requires active partnership. Naeron defines an explicit division of operational duties:

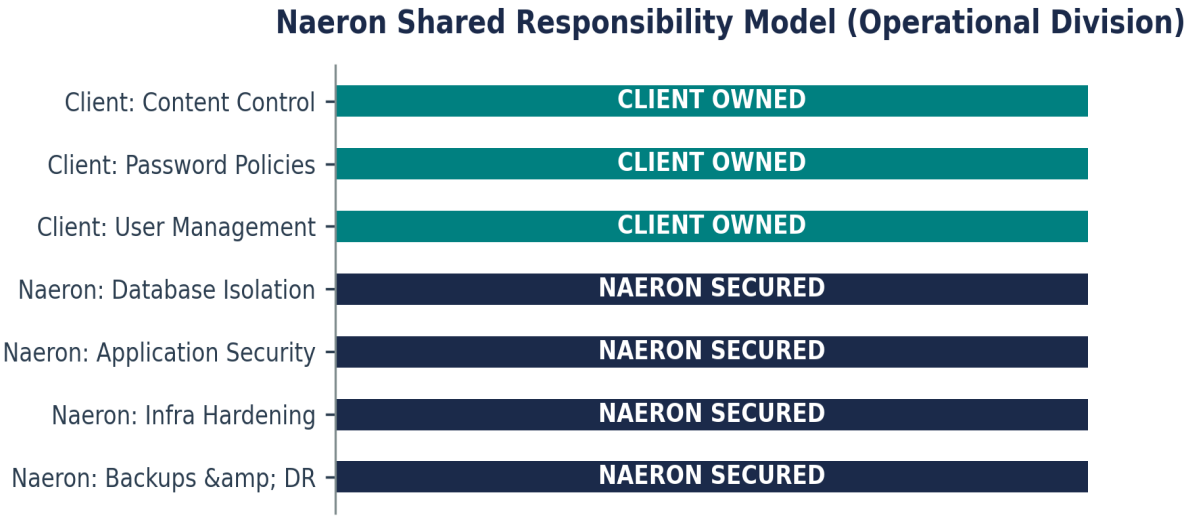

Figure 2: Naeron Shared Responsibility Model - Division of cybersecurity duties between Provider and Client.

Division of Cybersecurity Responsibilities:

• **Naeron's Responsibility:** Application security, API authentication, tenant-level database isolation, cloud infrastructure hardening (firewalls, VPCs), geographical data replication, disaster recovery, and continuous security patching.
• **Client's Responsibility:** Management of internal user credentials, enforcement of robust password rules (length, complexity), setting proper roles and access privileges (CFI, FI, student, maintenance), and auditing internal user activity.

DPO Contact & Inquiries:

All queries, requests to exercise data privacy rights, or notices regarding potential user credentials compromise must be directed to Naeron's Data Protection Officer:
■ **Email:** privacy@naeron.com | support@naeron.com
■ **Official Website:** https://naeron.com/legal/gdpr-kvkk.html

Approved By:	**Verified By:**
Naeron Data Protection Officer (DPO)	Naeron Chief Technology Officer (CTO)
Naeron Security Committee	Naeron Legal Affairs Division