

DATA ARCHIVING, AUDITING, LOGGING

Ulrika Hurt, eFTI Support Team
DLK/Digilogistics Centre

The purpose of archiving, auditing and logging:

- IT operations and data logging and audit for the operations of the IT systems
- IT operations and data exchange monitoring the operations- proof of timely and proper records,
- Evidence of records for ex-post control by authorities

Availability of archiving, auditing and logging also allows:

- Evidence for records for business use
- Evidence for (administrative) disputes and court cases

- Requirements for eFTI platforms and eFTI service providers, Article 9

Functional requirements for eFTI platforms

- (g) all data processing **is duly recorded in operation logs** in order to allow, as a minimum, **the identification of each distinct processing operation**, the natural or legal person having made the operation and the sequencing of the operations on each individual data element; if an operation involves modifying or erasing an existing data element, the original data element shall be preserved;
- (h) **data can be archived** and **remain accessible** for competent authorities in accordance with the relevant Union legal acts and national law laying down the respective regulatory information requirements;
- (i) the **operation logs referred to in point (g)** of this paragraph are **archived and remain accessible** for competent authorities for auditing purposes for the period of time specified in the relevant Union legal acts and national law laying down the respective regulatory information requirements and, for monitoring purposes, for the periods of time referred to in Article 17 [Monitoring];
- (j) data is protected against corruption and theft;

Requirements for eFTI platforms - 1/2

- **User identification:** logs must include the anonymised identity of the **author of the action** that triggered the logging, when available (e.g. eFTI data processing).
- **Timestamping:** every logged action must include a precise timestamp to track events over time.
- **Auditability:** logs must be stored securely and be auditable.
- **Data integrity:** logs must ensure that recorded events nor records/data cannot be altered or deleted without detection.
- **Retention period:** logging data must be retained for a specified period, likely aligned with legal and compliance requirements.

Requirements for platforms for logging- 2/2

- **Access controls:** only authorised personnel should be able to access logs to prevent unauthorized modifications.
- **Security measures:** logs must be protected against tampering, unauthorized access, and cyber threats.
- **Interoperability:** logging mechanisms must be compatible across different eFTI platforms and IT systems.
- **Compliance and reporting:** platforms must provide logging reports upon request to Competent Authorities (CA)s for enforcement and compliance verification.

List of logs

Mandatory (eFTI Regulation and Implementing Act)

- Identification, Authentication and Authorisation (IAA) of users.
- Logging of all accesses to the eFTI Platform (time of logging on and logging off).
- Logging of all data processing made upon eFTI datasets (creation, update, archival, etc.).
- Logging of all incoming and outgoing information exchanges with the eFTI Gate:
 - Upload of identifiers to the relevant registry.
 - eFTI dataset requests.
 - Responses to eFTI dataset requests.
 - Reception of follow-up communication.

Recommended

- Logging of all service interruptions (start and end time) and type of interruption (all services or only particular services).

Recommended actions for logging – 1/5

Implement Write-Once, Read-Many (WORM) storage.

Purpose: prevent deletion or modification of log entries after creation.

Operation:

- Use storage technologies (e.g. AWS S3 Object Lock, immutable file systems, or hardware-based WORM drives) that prevent any modification of stored data.
- Enforce retention policies that mirror legal and compliance requirements.
- Set system-level permissions and use append-only storage APIs.

Benefit:

guarantees that logs are stored in a way that they cannot be changed or deleted (even by administrators).

Recommended actions for logging – 2/5

Apply cryptographic hashing and chaining.

Purpose: detect tampering or modification of log records.

Operation:

- Generate a cryptographic hash (e.g. SHA-256) for each log entry upon creation.
- Implement hash chaining: each new log entry includes a hash of the previous entry (similar to how blockchains operate).
- Optionally, store root hashes periodically (e.g. daily) in an external trusted ledger or timestamping service.

Benefit:

any alteration of a log breaks the hash chain and becomes immediately detectable.

Recommended actions for logging – 3/5

Use digital signatures/ hashes for log entries.

Purpose: ensure integrity and authenticity of log records.

Operation:

- Each log entry or batch of entries is digitally signed using an asymmetric key pair (e.g. RSA or ECC).
- The private key is securely stored in a Hardware Security Module (HSM).
- The public key can be used by auditors or external systems to verify authenticity.

Benefit:

ensures that logs originate from a trusted source and have not been altered.

Recommended actions for logging – 4/5

Use Trusted Timestamping (RFC 3161).

Purpose: provide irrefutable proof of time of log creation.

Operation:

- For each log entry or batch, request a trusted timestamp from a Time Stamping Authority (TSA).
- Store the timestamp token alongside the log.

Benefit: ensures the log existed at a specific point in time and has not been backdated or forward-dated.

Recommended actions for logging – 5/5

Apply tamper-evident log frameworks.

Purpose: enhance assurance of log immutability and auditability.

Operation:

- Use solutions like Apache Kafka with immutability enforcement, Elastic Stack with data lifecycle protection, or dedicated logging systems like Wazuh/Graylog with integrity modules.
- Employ Merkle trees or blockchain-inspired data structures for scalable and tamper-evident logging.

Benefit:

these solutions provide a strong balance between performance, scalability, and forensic soundness.

Summary: key principles logging and audit operations

- Data integrity
- Audit trail comparable between platforms
- Limited to legally required details
- Archives transferrable and standardised
- Specialist support, training
- Appropriate tools, variety available
- GDPR respected
- Anonymisation applied where needed

Thank you!

Ulrika Hurt, eFTI Support Team
DLK/Digilogistics Centre

