When missing logs prevent a sensitive-data breach from being reconstructed

Vastaamo | Finland | Unauthorised access 2018-2019 | Regulatory decision 2021

UNAUTHORISED LOGINS	FIREWALL-FREE EXPOSURE	ADMINISTRATIVE SANCTION	DECISION STATUS IN SOURCE
At least two	**Nov 2017-Mar 2019**	**EUR 608,000**	**Not yet final**
S01	S01	S01	S01

DOCUMENTED EVENT

Vastaamo notified Finland's Data Protection Ombudsman in September 2020 about an attack against its patient-record database. The authority's 2021 announcement states that an external party logged in without authorisation at least twice, in December 2018 and March 2019, but that insufficient logs and documentation prevented investigators from determining the exact timing, network addresses or methods. The most likely cause identified by the authority was an unprotected MySQL port: the database root account had no password, could log in from any IP address and the server was open to the internet without a firewall from at least 26 November 2017 to 13 March 2019. The authority found failures in data security, breach notification and accountability documentation and imposed a EUR 608,000 administrative sanction. Its announcement states that the decisions were not yet final. Vastaamo had been declared bankrupt in February 2021. [S01]

NFRISK SCENARIO ADAPTATION - NOT AN EXTERNAL FINDING

An organisation holds highly sensitive records in a legacy database. Basic access-control and network restrictions are assumed rather than continuously evidenced, while logs are retained for less time than investigators would need to reconstruct an intrusion. A destructive database event is restored operationally, but no incident process joins restoration records, privileged-account activity and external-access logs. Months later, the organisation cannot establish when access occurred, how it happened or when the breach should have been notified.

STRESS-TEST QUESTIONS

01 Can you evidence that every privileged account holding sensitive data uses strong authentication and is unreachable from unapproved networks?

02 Would current logs establish who accessed sensitive records, from where and how, across the full period an investigation may need to reconstruct?

03 Does a destructive database event or unexplained restoration automatically trigger security investigation and breach-notification assessment?

04 Who owns the controller-level notification decision when knowledge is fragmented across technology, legal, operations and third parties?

CONNECTED RISK

Data & Control Integrity (primary)
Operational Resilience (contributing)
Conduct & Governance Risk (contributing)

FRAMEWORK RELEVANCE

GDPR Article 32: security appropriate to risk
The Finnish authority found that Vastaamo had not implemented basic technical and organisational security measures appropriate to the sensitivity and risk of the processing. [S02]

GDPR Article 33: breach notification without undue delay
The authority found that Vastaamo should have notified both the regulator and affected customers without delay once the March 2019 event indicated a high-risk personal-data breach. [S02]

NFRISK PRACTITIONER INTERPRETATION

For sensitive data, logging is part of the protective control, not only a forensic convenience. The control objective should specify privileged authentication, network exposure, log completeness, retention, tamper resistance and escalation from destructive or anomalous events. Notification governance must operate at controller level and cannot depend on which individual knew. Business failure or restructuring does not remove continuing responsibilities for retained personal data.

PRIMARY-SOURCE REGISTER

S01 Data Protection Ombudsman's Office, Finland (2021)
Administrative fine imposed on psychotherapy centre Vasta...
S02 European Union (2016)
Regulation (EU) 2016/679 - General Data Protection Regula...

EVIDENCE BOUNDARY Official findings are separated from the institutional scenario, framework interpretation and NFRisk practitioner view.