CYBERSECURITY · AI · LAW

Voluntary on paper. *Unavoidable in practice.*

What the first ISO standard on the security of AI systems changes for your liability.

Maître Mohamed Zied El Air

Lawyer, Paris and Tunis Bars · Certified DPO

Swipe →

Published 14 October 2026 · 1st edition · ISO/IEC JTC 1/SC 27

What your firewall *cannot see.*

01

Data poisoning

Tampered training data skews the model.

02

Evasion

Inputs crafted to fool the model in production.

03

Model theft

Seemingly legitimate queries are enough to copy it.

04

Model inversion

Reconstructing training data from the outputs.

05

Membership inference

Finding out whether a person is in the training set.

06

Prompt injection

Hidden instructions hijack the system.

What they share: they fly under the radar of firewalls, SIEM and IAM.

LEGAL STATUS

Just guidance?

Not certifiable.

Unlike ISO/IEC 27001 and ISO/IEC 42001.

Not mandatory.

No legislation makes it directly applicable.

Not harmonised.

No presumption of conformity with the AI Act (Art. 40).

And yet, three mechanisms make it unavoidable:

1 The state of the art

2 The AI Act

3 Personal data

MECHANISM 1 / 3 · THE STATE OF THE ART

The state of the art is not decreed. *It is observed.*

GDPR · Art. 32

Appropriate security measures, taking into account the state of the art.

NIS2 · Art. 21

The state of the art and, where applicable, relevant international standards.

In AI security, the state of the art now has a published benchmark.

After an incident, regulators and courts will know where to look.

MECHANISM 2 / 3 · THE AI ACT

Article 15 *already names* the attacks.

High-risk AI systems must be resilient against attempts to exploit their vulnerabilities, including:

- → data poisoning
- → poisoning of pre-trained components
- → adversarial examples and evasion
- → confidentiality attacks

Timeline · Regulation (EU) 2026/1744

Annex III ~~2 August 2026~~ → **2 December 2027**

A compliance window, not a reprieve.

MECHANISM 3 / 3 · PERSONAL DATA

A vulnerable model *still processes* personal data.

Inversion and membership inference	Personal data breach scenarios (GDPR, Art. 33 and 34): notification to the supervisory authority and, where required, to individuals.
EDPB · Opinion 28/2024	A model's resistance to these attacks is a criterion for assessing whether it is anonymous.
For the DPO	ISO/IEC 27090 becomes a reading grid for DPIAs on AI projects.

THE PRIORITY

Six clauses to check in *your AI contracts.*

- ☐ Provenance and integrity of training data
- ☐ No training of models on your data without express consent
- ☐ Notification of AI-specific incidents: poisoning, model extraction, prompt injection
- ☐ Governance of updates and retraining
- ☐ Logging, audit and reversibility
- ☐ Allocation of responsibilities mirroring the AI Act's provider / deployer roles

Financial sector

Alignment with the DORA contractual clauses (Art. 30).

Tunisia

Security audits under Decree-Law No. 2023-17 on cybersecurity.

MY CONVICTION

On the day of an incident, no one will ask whether you were certified. *They will ask whether your measures reflected the state of the art.*

Do your risk registers and vendor contracts already cover AI-specific threats?

Maître Mohamed Zied El Air

Lawyer admitted to the Paris and Tunis Bars

Certified DPO · GDPR, cybersecurity and AI

www.elair-avocat.com/en