

AI governance terms in plain language

19 key terms from the AI Act, GDPR, ISO standards and security — explained in plain language, in alphabetical order.

A

AI Act

The EU regulation on artificial intelligence. It divides AI systems into risk categories (from minimal to unacceptable) and imposes obligations depending on the level of risk.

AIMS (AI Management System)

A system for managing artificial intelligence in an organisation, in line with ISO/IEC 42001. It covers processes, roles and procedures for overseeing AI.

AISO

Usually short for AI Security Officer — the person responsible for the security of AI systems in an organisation. The meaning may vary between companies.

AISO Retainer

A subscription agreement (retainer) under which a company pays a fixed fee for regular access to the services or advice of an AISO specialist instead of paying per assignment.

Annex A controls

A list of specific safeguards and actions (controls) in an ISO standard that an organisation can implement to meet its requirements. In ISO/IEC 42001 they cover AI risk management, transparency and oversight of systems.

B

BAA (Business Associate Agreement)

An agreement required in the US (HIPAA rules) when a company processes patients' medical data on behalf of another organisation.

C

Copyright law

A set of rules protecting the creators of works (texts, code, graphics etc.) against unauthorised copying or use of their work.

D

DPA (Data Processing Agreement)

An agreement between a data controller and an entity that processes the data on its behalf (e.g. a cloud provider). Required by the GDPR.

E

EDPB (European Data Protection Board)

The EU body bringing together national data protection authorities. It issues guidelines on applying the GDPR across the EU.

G

GDPR

The EU General Data Protection Regulation (in Polish: RODO). It governs how companies may collect, store and process the personal data of EU citizens.

GPAI (General Purpose AI)

A general-purpose AI model. A term from the EU AI Act for models (e.g. large language models) that can be used for many different applications rather than one specific purpose. GPAI providers have additional obligations (e.g. technical documentation, transparency), and models with particularly high computing power face even stricter requirements (so-called “systemic risk”).

I

ISO/IEC 27001

An international standard for information security management systems. It defines how a company should protect data against leaks, loss or unauthorised access.

ISO/IEC 42001

An international standard setting out requirements for an AI management system (AIMS) in an organisation. It helps deploy AI in a responsible and controlled way.

N

NIST AI RMF

A US framework (AI Risk Management Framework) developed by NIST. It helps organisations identify and manage risks related to AI systems. It is voluntary, not law. It is built on 4 pillars:

- **Govern** — Establishing an organisational culture, oversight principles and accountability policies for AI.
- **Map** — Identifying the context, goals and potential risks of a specific AI system.
- **Measure** — Assessing and quantifying identified risks with technical and qualitative tools.
- **Manage** — Implementing mitigation plans, allocating resources and continuous monitoring after deployment.

P

Polish AI Systems Act

A planned Polish act implementing the EU AI Act into national law. It is to define, among other things, the national supervisory authority and penalties for infringements.

R

RFP (Request for Proposal)

A document in which a company describes its needs and asks vendors to submit an offer for a service or product.

S

SIEM (Security Information and Event Management)

A system that collects and analyses security logs from a company's entire infrastructure to detect suspicious activity and incidents in real time.

SOC 2

A US security audit standard for service companies (e.g. SaaS). It checks whether a company properly protects client data in terms of security, availability and confidentiality.

T

ToS (Terms of Service)

A document setting out the rules for using a product or service and the rights and obligations of the user and the provider.