e-REAL®
by LOGOSNET

Artificial Intelligence. Liability and Sanctions under EU and Member State Law

A COMPARATIVE PROGRAM



One AI system. Five kinds of liability. Twenty-seven ways to enforce them.

Administrative, criminal, civil, data-protection and consumer liability under the EU AI Act and the national laws that implement it, compared across member states. Short live modules and practice labs for general counsel, legal departments and compliance teams. Online or onsite.

PACT FOR SKILLS Leader

Logosnet with the e-REAL Labs are a member of the European Union's Pact for Skills

www.e-real.net

e-REAL by LOGOSNET

WHY THIS PROGRAM

The AI Act is not the whole story

Who can be sanctioned, by whom and under which rules when an AI system causes harm: the whole sanctions system, for every potential liable party.

The AI Act sets administrative fines of up to 35 million euros or 7% of worldwide annual turnover, whichever is higher, and leaves the rest to the member states: who enforces, how proceedings run, which national fines are added, and whether a breach is also a crime. Around it sit the GDPR, the Digital Services Act, the Data Act, NIS2, the Cyber Resilience Act, the revised Product Liability Directive and consumer law, each with its own sanctions and its own authority.

Italy has gone furthest: Law 132/2025 and Legislative Decree 160/2026 make the omission of security and human-oversight measures on high-risk systems a criminal offense (art. 437-bis of the Criminal Code), punish the unlawful dissemination of AI-generated or manipulated content (art. 612-quater) and add both to the predicate crimes under Legislative Decree 231/2001 (art. 25-vicies), with fines up to 1,000 quotas and disqualification; Decree 179/2026 entrusts supervision to AgID and ACN. Germany adds national fines of up to 50,000 euros under the KI-MIG and has a deepfake offense before Parliament; in Spain AESIA is operational, but the organic law bill lapsed when the Cortes were dissolved. The same deployment therefore carries a different liability profile in each country. This program maps it, compares it and trains participants to manage it.

Administrative liability

The Act's fines and the national ones added to them; who the authority is, how proceedings run, what a cooperation duty means in practice.

Criminal and corporate liability

Where a breach becomes a crime, who is liable, and when the company itself answers: Italy's Decree 231/2001, Germany's OWiG, Spain's Código Penal.

Civil and sectoral liability

Product liability for AI, contractual allocation with vendors, data-protection and consumer claims, cybersecurity duties, collective redress.

PACT FOR SKILLS Leader

Logosnet with the e-REAL Labs are a member of the European Union's Pact for Skills. Certificates of Completion for this program are issued by Logosnet within that framework.

e-REAL by LOGOSNET

THE MAP

Five layers of liability, one deployment

What the program covers, by type of liability and by jurisdiction. The map is updated at each edition.

LIABILITY	EU LAYER	ITALY	GERMANY	SPAIN	FRANCE	NL · NORDICS
Administrative	AI Act art. 99: up to €35M / 7%; GDPR art. 83; DSA, Data Act, NIS2, CRA fines	Law 132/2025, Decree 179/2026: AgID and ACN; art. 99 tiers + fourth tier up to €1M / 0.5%	KI-MIG (29 July 2026): BNetzA; § 15: up to €50,000	AESIA operational; organic law bill (up to €35M / 7%) lapsed, Oct. 2026	DDADUE bill (Senate Feb. 2026); CNIL lead, DGCCRF, Arcom	NL: implementing act in consultation; AP and RDI; DK, FI, SE regulator networks
Criminal	No criminal offenses; penalties left to member states (art. 99(1))	Art. 437-bis (high-risk security and oversight), 612-quater (deepfakes)	§ 201b StGB in the Government's bill (Oct. 2026); existing StGB	Sexual deepfakes: arts. 173.1, 189.1.d CP; art. 173 bis in lapsed bill	Deepfake offense art. 226-8 CP (SREN law 2024)	Existing provisions (WODC)
Corporate	No corporate-crime regime; administrative fines apply directly to operators, legal persons included	Decree 231/2001 art. 25-vicies: up to 1,000 quotas + disqualification	OWiG §§ 30, 130: fines up to €10M	Código Penal art. 31 bis	General corporate liability	General rules
Civil	Revised Product Liability Directive (software, AI); national tort and contract law	Decree 160/2026 arts. 17–20 (disclosure, presumption of causation, direct action); Civil Code	BGB, ProdHaftG transposition	Civil Code, consumer law	PLD transposition due Dec 2026; Civil Code	PLD transposition; national tort law
Data and consumer	GDPR art. 22 and 83; DSA; UCPD; collective redress directive	Garante; AGCM	Data-protection authorities of the Länder; UWG	AEPD; consumer law	CNIL; DGCCRF	AP; consumer authorities

Figures and references as they stand at the date of delivery; bills before parliaments are marked as such in class. The map does not replace advice on a specific case.

MODULE CATALOG · 01

The EU layer

The sanctions in the Act and in the regulations that surround it.



EU-01 **The AI Act's own sanctions**

Article 99 and the three fine tiers; the role of national authorities and the AI Office; proceedings, cooperation and information duties; SME and public-sector rules; what an authority can order beyond a fine: withdrawal, recall, prohibition.

Live · 1 session · every path

EU-02 **Who answers: roles along the value chain**

Provider, deployer, importer, distributor, authorized representative; when a deployer becomes a provider; how obligations and sanctions move with the role; allocating them in contracts with vendors and integrators.

Live · 1 session · every path

EU-03 **Data protection and automated decisions**

GDPR and the AI Act read together: lawful basis, article 22, DPIAs and fundamental-rights impact assessments, the two fine regimes and how they cumulate, the data-protection authority as de facto AI supervisor.

Live · 1 session

EU-04 **Product liability and civil claims**

The revised Product Liability Directive: software and AI as products, defect and disclosure, the presumption rules; national tort and contract law; collective redress; how to document a system so a claim can be defended.

Live · 1 session

EU-05 **Cybersecurity, platforms and consumers**

NIS2 and the Cyber Resilience Act duties that overlap with the Act's robustness requirements; the DSA for AI on platforms; unfair commercial practices and consumer law applied to AI-driven offers and decisions.

Live · 1 session

Content is revised at each edition to the law in force; participants of earlier editions are invited to the update session.

e-REAL by LOGOSNET

MODULE CATALOG · 02

The national layer

The same AI Act; different crimes, authorities and corporate-liability rules.



NA-IT **Italy**

Law 132/2025, Decrees 160/2026 and 179/2026: the offense of omitted security and human-oversight measures on high-risk systems (art. 437-bis), the deepfake offense (art. 612-quater), corporate liability under art. 25-vicies of Decree 231/2001, the civil provisions (disclosure, presumption of causation, direct action), AgID and ACN and the fourth fine tier.

Live · 1 session · Italian or English

NA-DE **Germany**

The KI-MIG in force since 29 July 2026: BNetzA as market-surveillance authority, national fines under § 15 of up to 50,000 euros alongside the Act's, the deepfake offense in the Federal Government's bill, corporate liability under §§ 30 and 130 OWiG, data-protection supervision by the Länder.

Live · 1 session · German or English

NA-ES **Spain**

AESIA, already operational, and the other supervisory authorities; the organic law bill on the good use and governance of AI (graded sanctions up to 35 million / 7%), lapsed with the dissolution of the Cortes in October 2026; sexual deepfakes under current law (arts. 173.1 and 189.1.d of the Código Penal); corporate criminal liability under art. 31 bis of the Código Penal.

Live · 1 session · Spanish or English

NA-FR **France**

The DDADUE bill, passed by the Senate at first reading (February 2026), and the CNIL's lead role in a decentralized enforcement model; the deepfake offense of art. 226-8 of the Code pénal (SREN law 2024: up to one year and 15,000 euros, two years and 45,000 if spread online); the Product Liability transposition due by 9 December 2026.

Live · 1 session · French or English

NA-NL **The Netherlands and the Nordic approach**

Supervision through coordinated networks of existing regulators: in the Netherlands the implementing act under consultation in 2026, with AP and RDI coordinating; the Danish, Finnish and Swedish models; the WODC view that existing criminal law already reaches most deepfakes.

Live · 1 session

NA-EU **Cross-border deployment**

One system, several member states: mapping sanctions, authorities and notification routes onto a single deployment, choosing where the compliance evidence sits, keeping the map current as national acts arrive.

Live · 1 session · every path

All 27 member states on request, with local counsel: Belgium, Austria, Portugal, Poland, Czechia, Romania, Hungary, the Baltics, Greece, Cyprus, Malta, Ireland and the rest of the European Union.

e-REAL by LOGOSNET

MODULE CATALOG · 03

From liability to accountability

The modules that turn the map into governance. The labs where participants put it into practice.

CC-01 **Liability versus accountability**

Liability looks back: who answers after harm. Accountability looks forward: who designs, supervises and documents the system so harm is prevented and defended. How the OECD principles, ISO/IEC 42001 and the Act converge on documentation, traceability and oversight, and what that means for a legal department.

Live · 1 session · every path

CC-02 **Regulatory entropy and the compliance model**

Overlapping rules, staggered dates, authorities still being set up: uncertainty comes from the interaction of sources, not their number. Building a model that locates each duty in the right framework, assigns an owner and a review trigger, and integrates the AI inventory with the existing compliance program.

Live · 1 session

CC-03 **Human oversight as a legal duty**

Article 14 and 26(2) of the Act: competence, training, authority and support of the people who oversee high-risk systems; how the duty becomes a criminal element in Italy and an evidentiary one everywhere; designing oversight roles that stand up in an investigation.

Live · 1 session

Practice labs

L-01 **Map the exposure**

A client group deploys one AI system in three member states. Participants map administrative, criminal, corporate and civil exposure per country, identify the authorities and decide where the evidence sits. An avatar board asks for a one-page answer.

Lab · 1 session

L-02 **Update the compliance model**

The Italian case: map the systems, identify the high-risk ones, assign oversight roles, update the Decree 231/2001 model and the code of ethics, with an avatar supervisory board asking what evidence exists. Adaptable to the OWiG and Spanish regimes.

Lab · 1 session

L-03 **Answer the authority, then the court**

An information request from a market-surveillance authority after an incident; then a civil claim under the Product Liability Directive. Participants reconstruct documentation, decide what to disclose and draft the response, with an avatar inspector and an avatar opposing counsel asking the follow-up questions.

Lab · 1 session

e-REAL by LOGOSNET

HOW IT WORKS

Map. Decide. Defend. Repeat.

Feedback connects each decision to the rule it rests on and to the evidence behind it.

01 Case

A system, three countries, an incident.

02 Map

Which liability, which authority, which rule.

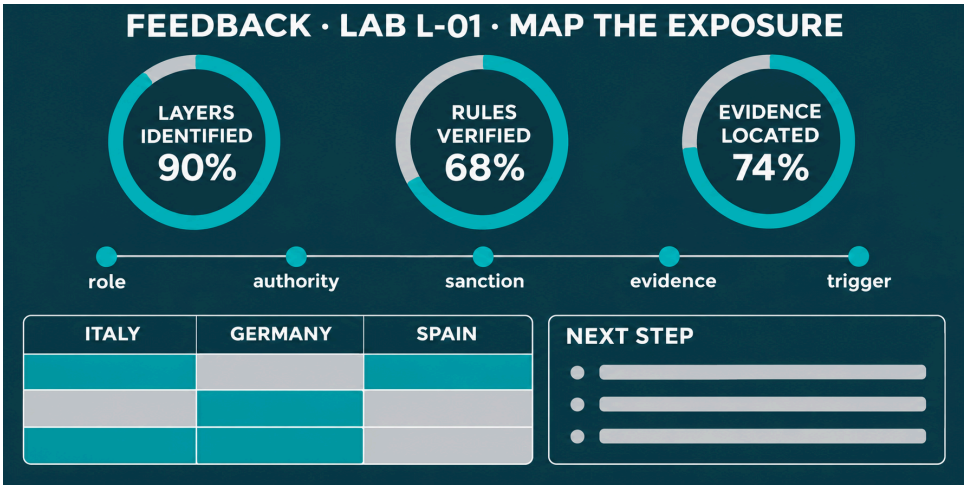
03 Decide

Allocate, document, disclose.

04 Defend

Answer the authority and the court.

Example of feedback after a lab



What the feedback looks at

Correct identification of the liability layers and the roles; the state of each rule actually checked; completeness of the exposure map; quality of the evidence relied on; clarity of the answer for a board and for an authority; residual risk stated, with triggers for review.

Built on the book *Generative Artificial Intelligence and the Future of Law*

The program draws on Fernando Salvetti's book (Springer, in press): the distinction between liability and accountability, the concept of regulatory entropy, and the comparative analysis of AI governance across the European Union, Switzerland, the United Kingdom, Canada, the USA, the Middle East, Africa, the Far East and Australia.

e-REAL by LOGOSNET

FORMAT AND CERTIFICATE

Online, onsite, or both

Short live sessions that fit a working week. Onsite when it helps, even for a launch or closing event alone.

Fully online

Live sessions of 90 to 120 minutes, at most 16 participants, one session a week. Materials, the liability map and recordings on the e-REAL platform.

Onsite, as much as you want

Any module at your offices, in an e-REAL immersive room or at a venue we arrange: the whole path, a few modules, or only a launch or closing event with a live simulation.

Languages

English throughout. National modules in Italian, German, Spanish, French, Portuguese, Greek or Dutch where indicated. Avatars in the simulations speak more than 40 languages, following each participant's preference.

For whom

General counsel and legal departments

In-house lawyers who answer for AI systems to the board, to regulators and in litigation, and who negotiate the contracts that allocate the risk.

Compliance, privacy and risk functions

Compliance officers, data protection officers and risk managers who integrate the AI inventory into the existing compliance model and prepare for inspections.

Law firms advising corporate clients

Practice groups that advise on AI deployment across member states and need one comparative map rather than five separate memos.

PACT FOR SKILLS Leader

Certificate of Completion
Paths of four modules or more lead to a Certificate of Completion issued by Logosnet, a member of the Pact for Skills, stating the hours completed: 8 to 18 continuing-education hours depending on the path. Credits recognized where the bar, professional body or employer provides for it.

LET'S MAP YOUR EXPOSURE

Tell us the member states, the AI systems and the roles. We will propose a path and a calendar.
www.e-real.net

CONTACT

Logosnet, Turin
+39 011 19620030
danils@logosnet.org