



European Union: AI Act, GDPR and Product Liability

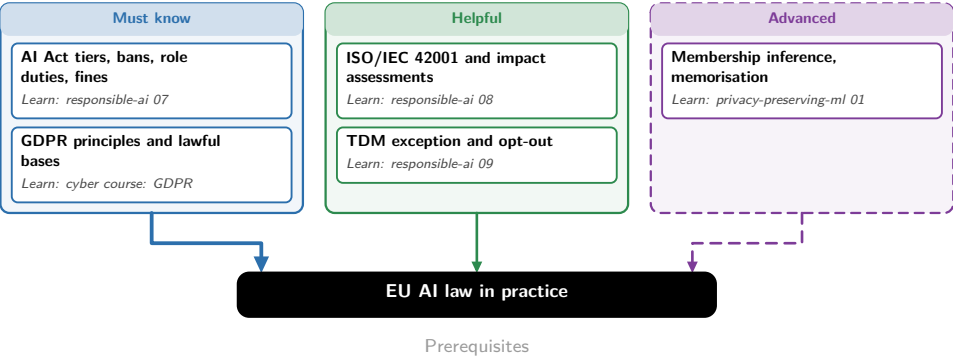
AI law by jurisdiction | AI Act in practice (scope, role changes, enforcement bodies, standards), GDPR for training and automated decisions, the new Product Liability Directive and the EU digital rulebook around AI. Obligations overview as of 2026, not legal advice: check with counsel

#EU #AIAct #GDPR #PLD #2026

● The EU picture in one look

AI in EU law (as of 2026)	
In one sentence ●○○○	One AI statute (AI Act, Regulation (EU) 2024/1689, in force 2024-08-01) sits on top of laws that already applied: data protection, product safety and liability, consumer, platform and cyber rules.
Practitioner ●●○○	The AI Act regulates by use and role; GDPR regulates any processing of personal data, including training and inference; the PLD makes software, AI included, a product for no-fault liability. - AI Act duties are mostly ex ante - PLD and national tort law are ex post
Expert ●●●○	Enforcement is split: the AI Office for GPAI models, national market surveillance authorities for systems, data protection authorities for GDPR, courts for liability. one incident can trigger several authorities
Under the hood ●●●●	The 2026 Digital Omnibus moved high-risk dates; harmonised standards and Commission guidelines still fill in the details. read the consolidated text, then the guidelines

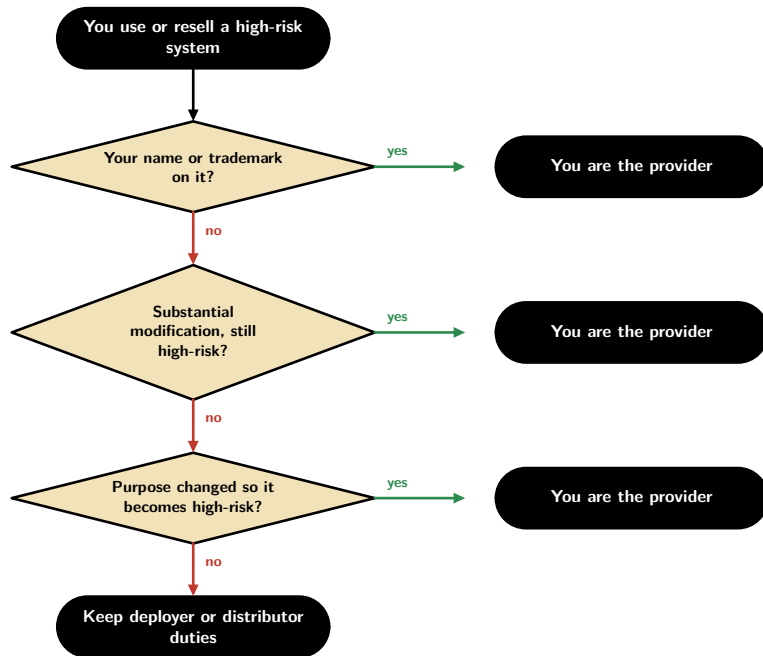
EU AI law at four depths



◎ AI Act: scope and role changes

In scope	Out of scope
Providers placing AI systems or GPAI models on the EU market, wherever they are established	Systems used exclusively for military, defence or national-security purposes
Deployers established or located in the EU	AI developed and used for the sole purpose of scientific research and development
Non-EU providers and deployers when the output is used in the EU	Research, testing and development before market placement (real-world testing stays regulated)
Importers, distributors, product manufacturers integrating AI	Purely personal, non-professional use by individuals
Authorised representatives of non-EU providers	Free and open-source components, unless high-risk, banned or subject to Art. 50

Who is in scope (Art. 2) and who is out



When does a deployer, importer or distributor become the provider of a high-risk system (Art. 25)? Stop at the first yes

📖 Trap: fine-tuning a GPAI model

Fine-tuning or modifying a GPAI model can make you a **GPAI provider** for the modification; Commission guidelines set an indicative threshold (about one third of the original training compute) below which the modifier is not treated as a new provider. Check the current guidelines before relying on the figure.

🏛️ AI Act: who enforces what

Body	Level	Role
AI Office	Commission	supervises GPAI models, requests information, evaluates models, fines GPAI providers; runs the Code of Practice and templates
European AI Board	EU	Member State representatives; consistent application, opinions, guidance
Scientific panel	EU	independent experts; qualified alerts on systemic-risk GPAI
Market surveillance authorities	national	investigate systems, order corrective action, withdraw, fine (Art. 74); financial supervisors act as MSA for financial institutions
Notifying authorities and notified bodies	national	designate and run third-party conformity assessments

Data protection authorities	national	GDPR, and MSA role for some biometric, law-enforcement, migration and justice uses (Art. 74(8))
Courts	national / CJEU	liability claims, judicial review of authority decisions

Enforcement architecture

DPIA (GDPR Art. 35) risk to data subjects from processing personal data; controller	vs	FRIA (AI Act Art. 27) risk to fundamental rights from a high-risk system; certain deployers
Tell: Is the trigger personal data or a high-risk use? FRIA complements an existing DPIA (Art. 27(4))		
Internal control (Annex VI) provider self-assesses; most Annex III systems	vs	Notified body (Annex VII) third party; biometrics without standards, many Annex I products
Tell: Does a third party sign the conformity?		
Authorised representative acts for a non-EU provider under the AI Act	vs	GDPR Art. 27 representative acts for a non-EU controller under GDPR
Tell: Which law appointed them? A company may need both		
Harmonised standard voluntary, gives presumption of conformity	vs	Common specification Commission implementing act if standards are missing
Tell: Who adopted it: CEN-CENELEC or the Commission?		

Pairs readers confuse

🔒 GDPR applied to AI

Stage	GDPR rule	What to do
Training data collection	Art. 6 lawful basis; Art. 9 special categories	document a legitimate-interest assessment (purpose, necessity, balancing); filter special categories or find an Art. 9 condition
Bias detection	AI Act Art. 10(5)	special-category data may be processed for bias detection in high-risk systems, with strict safeguards and deletion afterwards
Model weights	anonymity test	a model trained on personal data is anonymous only if extraction and inference of that data is insignificant; assess case by case
Information to people	Art. 13-14	say that AI is used, the purposes, and for Art. 22 decisions meaningful information about the logic involved
Automated decisions	Art. 22	contract, law or explicit consent; human intervention, right to express a view and contest
High-risk processing	Art. 35 DPIA	run before launch; new technology plus profiling usually triggers it
Breach	Art. 33	notify the authority 72 h after awareness, calendar hours (Art. 33)

GDPR touchpoints along the AI lifecycle

EDPB Opinion 28/2024 — European Data Protection Board opinion on AI models (December 2024): anonymity of models, the three-step legitimate-interest test, and consequences of unlawful training for later deployment.

CJEU C-634/21 SCHUFA — Court of Justice ruling (2023): a credit score is itself an Art. 22 decision when a third party draws strongly on it to grant or refuse a contract.

CJEU C-203/22 Dun & Bradstreet Austria — Court of Justice ruling (2025): the person must receive an explanation of the procedure and principles actually applied, in an intelligible form; trade secrets are weighed by the authority or court, not used to refuse outright.

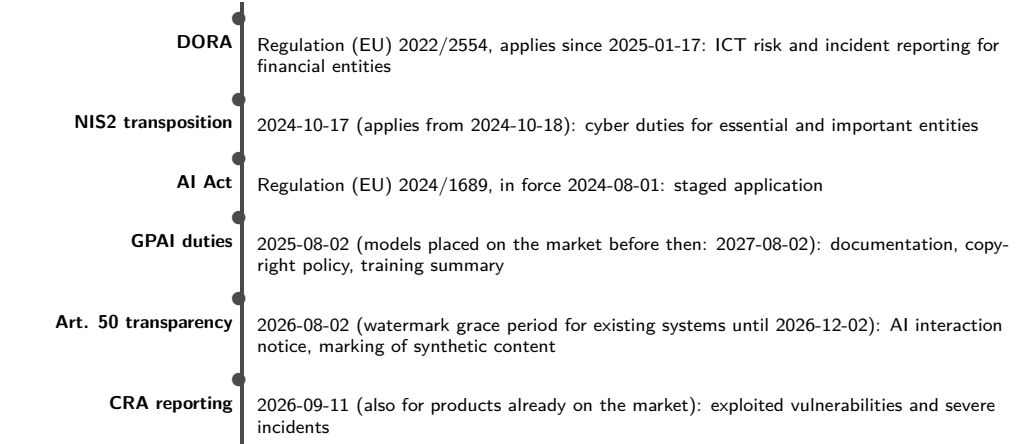
🔥 Enforcement already happens through GDPR

Italy's data protection authority (Garante) temporarily restricted ChatGPT in 2023 and fined OpenAI 15 M EUR in December 2024 (appealed). Several authorities fined Clearview AI for scraping facial images, including 20 M EUR in Italy, France and Greece and 30.5 M EUR in the Netherlands. GDPR fines reach 20 M EUR or 4 % of worldwide turnover (Art. 83(5)).

✔ Product liability and the wider rulebook

Point	Rule
Product	software is a product, whatever its delivery (embedded, SaaS, download), so AI systems are covered; free and open-source software supplied outside a commercial activity is excluded
Liable persons	manufacturer, including whoever substantially modifies a product; importer, authorised representative or fulfilment service provider when the manufacturer is outside the EU
Defect	safety a person is entitled to expect, including effects of continued learning after market placement, software updates under the manufacturer's control and cybersecurity weaknesses
Damage	death, personal injury incl. medically recognised psychological harm, damage to property, destruction or corruption of non-professional data
Proof	court-ordered disclosure of evidence; presumptions of defect or causation when technical complexity makes proof excessively difficult
Time limits	claims expire 10 years after market placement, 25 years for latent personal injury

New Product Liability Directive, Directive (EU) 2024/2853 (replaces 85/374/EEC; national transposition due by December 2026, verify the national law)



High risk, Annex III

2027-12-02 (was 2026-08-02): hiring, credit, education, essential services

CRA in full

2027-12-11: products with digital elements

High risk, Annex I

2028-08-02 (was 2027-08-02): AI safety components of regulated products

The EU digital rulebook around AI: application dates from the course facts registry

DSA, Regulation (EU) 2022/2065	very large platforms and search engines assess and mitigate systemic risks, including from generative AI features and recommender systems
Data Act, Regulation (EU) 2023/2854	access to data from connected products, cloud switching; affects training data sourcing
CRA, Regulation (EU) 2024/2847	cybersecurity of products with digital elements, AI products included
DSM Copyright Directive (EU) 2019/790	Art. 4 text-and-data-mining exception with machine-readable opt-out (see responsible-ai 09)
AI Liability Directive	proposal withdrawn in 2025: fault-based claims stay under national tort law

Worked example

PROBLEM Which EU obligations stack on the bank, and which does it inherit from the vendor?

GIVEN

- Vendor: US company, provider of the scoring system
- Bank: EU deployer, retraining the model on its own data
- Output: accept or reject consumer loans

1 Classify the use

creditworthiness of natural persons = AI Act Annex III high-risk

Why: fraud detection is excluded, credit scoring is not

2 Check the role

retraining that changes performance beyond the foreseen scope = substantial modification → bank becomes provider (Art. 25)

Why: otherwise it stays deployer

3 AI Act duties

as provider: risk management, data governance, documentation, logs, oversight, conformity, registration; as deployer: FRIA (Art. 27), oversight, log retention

Why: both roles can coexist for different versions

4 GDPR

Art. 22 applies (SCHUFA): explicit basis, human review on request, meaningful explanation (C-203/22); DPIA

Why: personal data, significant effect

5 Sector law

consumer credit rules on creditworthiness and explanation; banking supervisor acts as MSA

Why: see sheet 09

6 Vendor

authorised representative in the EU, instructions for use, technical documentation passed downstream

Why: non-EU provider (Art. 22)

ANSWER The bank carries provider and deployer duties, GDPR Art. 22 and sector rules; the US vendor still needs an EU representative and full documentation for its original system

CHECK ✓ Annex III duties apply from 2027-12-02 (was 2026-08-02); GDPR and credit law apply today

A German bank deploys a vendor's credit-scoring model that it fine-tunes on its own loan book

★ Myths and recap

MYTH OR FACT?

"The AI Act replaced GDPR for AI"

MYTH: Both apply in parallel
AI Act Art. 2(7): GDPR is unaffected; FRIA complements, does not replace, the DPIA.

MYTH OR FACT?

"Software cannot be a defective product"

MYTH: Under the new PLD it is Directive (EU) 2024/2853 covers software and AI, including defects from learning after release.

MYTH OR FACT?

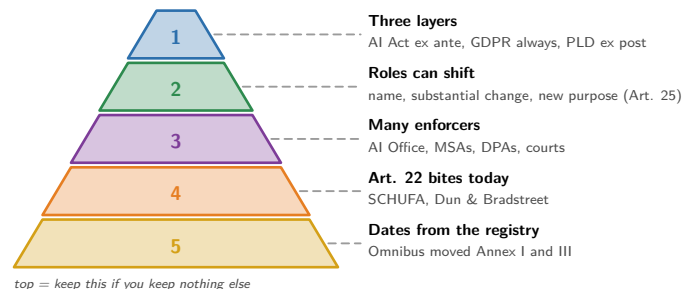
"A US provider with no EU office is outside the AI Act"

MYTH: Output used in the EU brings it in Art. 2(1)(c); it must appoint an authorised representative for high-risk systems and GPAI.

MYTH OR FACT?

"Postponed high-risk dates mean nothing to do now"

MYTH: GDPR, PLD, bans and GPAI duties already bite
Only Annex I and Annex III duties moved.



Q1 Three ways a deployer becomes provider of a high-risk system?

A Putting its name or trademark on it, substantially modifying it while it stays high-risk, or changing its purpose so it becomes high-risk (Art. 25).

Q2 Who supervises GPAI models under the AI Act?

A The AI Office in the Commission; national market surveillance authorities handle AI systems.

Q3 What did CJEU C-634/21 SCHUFA decide?

A A credit score is an Art. 22 automated decision when a third party draws strongly on it to grant or refuse a contract.

Q4 What may a high-risk provider do with special-category data under AI Act Art. 10(5)?

A Process it strictly for bias detection and correction, with safeguards, then delete it.

Q5 Does the new PLD cover open-source software?

A Not when developed or supplied outside a commercial activity; commercial supply is covered.

Q6 Which damages does the PLD cover?

A Death, personal injury incl. psychological harm, property damage, and destruction or corruption of non-professional data.

Q7 What happened to the AI Liability Directive?

A The Commission withdrew the proposal in 2025; fault-based claims stay under national tort law.

Q8 Which EDPB text addresses training on personal data?

A Opinion 28/2024: model anonymity, the three-step legitimate-interest test, consequences of unlawful training.

Q9 When must a non-EU GPAI provider appoint an authorised representative?

A Before placing the model on the EU market (Art. 54).