law.no

Do legal frameworks exist for AI?

A short introduction
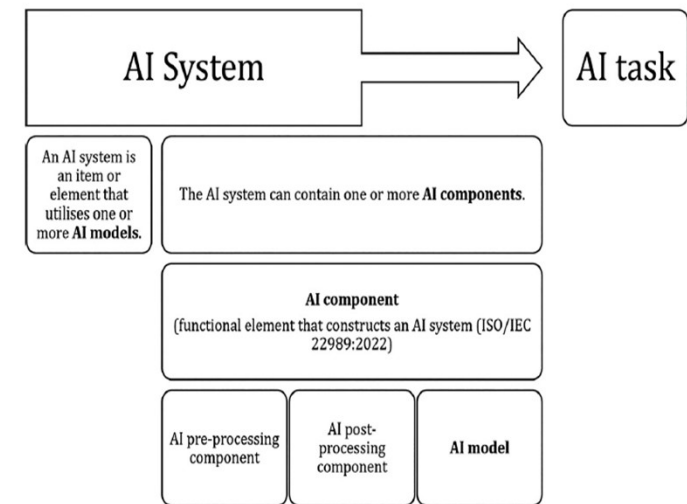
law.no

law.no

AI Act – A risk based law to protect people in the age of AI

What excactly is an AI System?

law.no

- **AI system = machine-based system with autonomy**, used to make predictions, recommendations, or decisions (AI Act Art. 3(1)).

- It includes more than "the model" – pre-processing (e.g. sensor filters) and post-processing (e.g. dashboards) may be in scope (e.g. if it affect AI`s outcome of performance).

- Complex IT systems are often split across microservices – identifying "the AI system" is not always straightforward.

- It is recommended to use **Business Process Modeling (BPMN)** to map out data flows and responsibilities.

- Clear system modeling helps determine whether AI is in scope, and who is accountable under the AI Act.

06.06.2025

Credit: AI Act Compact - Tea Mustać and Peter Hense

The actors: provider vs the deployer

law.no

- **Provider =** The party that develops and places the AI system on the market (e.g. tech vendor - fish health AI, feeding optimizer).

- **Deployer =** The party that uses the AI system in real-world operations (e.g. the fish farmer).
  - {sub parahraph about other roles}

- Both have **legal obligations** under the AI Act, depending on the system's risk level.

- Clarifying roles is key for compliance and contract structuring.

06.06.2025

Four risk levels – The AI Act`s Logic
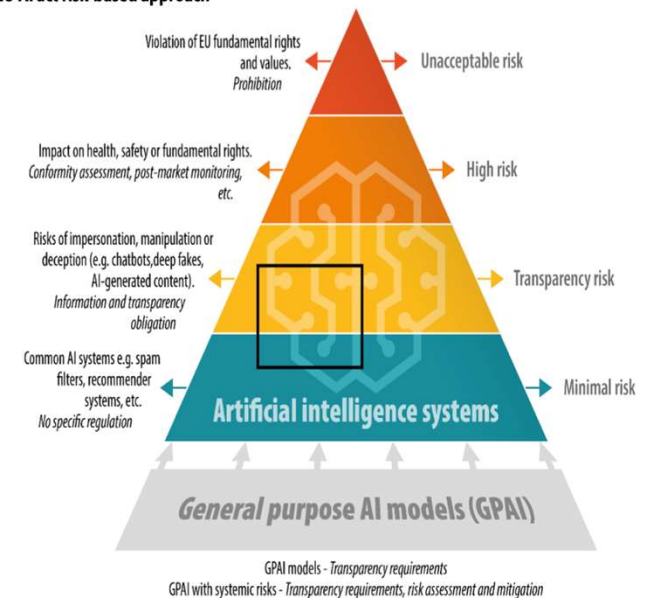
law.no

- The AI Act classifies AI systems by **risk to people's health, safety, and rights**:

- **Unacceptable risk** → banned (e.g. social scoring, manipulative AI).

- **High-risk** → strict rules apply (e.g. AI in CE-marked machinery, HR tools).

- **Limited risk** → transparency rules (e.g. chatbots, synthetic content).

- **Minimal risk** → free use (unregulated), but good practices still encouraged.

EU AI act risk-based approach

Violation of EU fundamental rights and values. *Prohibition* ←→ Unacceptable risk

Impact on health, safety or fundamental rights. *Conformity assessment, post-market monitoring, etc.* ←→ High risk

Risks of impersonation, manipulation or deception (e.g. chatbots, deep fakes, AI-generated content). *Information and transparency obligation* ←→ Transparency risk

Common AI systems e.g. spam filters, recommender systems, etc. *No specific regulation* ←→ Minimal risk

Artificial intelligence systems

General purpose AI models (GPAI)

GPAI models - Transparency requirements
GPAI with systemic risks - Transparency requirements, risk assessment and mitigation

Data source: European Commission

06.06.2025

What is a high- risk system?

- **The starting point**: Product safety rule - Art.6

  - The AI is a safety system for products covered by product safety directives defined in Annex I

  - The product must undergo third party conformity checks according to these directives before it can be placed on the market

- **Annex**: Annex III, which defines certain forms of AI whose use is considered to pose a risk to fundamental rights.

- **Exception**: systems on Annex III that do not pose a risk to health, safety or fundamental rights because one of the conditions in Art. 6(3) is fulfilled.

- **Dynamic system**: The Commission may amend the terms of Art. 6(3) or add/remove uses of AI from Annex III under Art. 6(6) and Art. 7.

06.06.2025

EU AI act risk-based approach

Violation of EU fundamental rights and values. *Prohibition* — Unacceptable risk

Impact on health, safety or fundamental rights. *Conformity assessment, post-market monitoring, etc.* — High risk

Risks of impersonation, manipulation or deception (e.g. chatbots, deep fakes, AI-generated content). *Information and transparency obligation* — Transparency risk

Common AI systems e.g. spam filters, recommender systems, etc. *No specific regulation* — Minimal risk

Artificial intelligence systems

General purpose AI models (GPAI)

GPAI models - *Transparency requirements*
GPAI with systemic risks - *Transparency requirements, risk assessment and mitigation*

Data source: European Commission

High-risk AI in aquaculture
(«safety components» article 6 no 1.)

law.no

Use Case (aquaculture)	Why it may be high-risk under the AI Act	EU / Norwegian legal law
Autonomous feeder-control AI that starts/stops feed blowers and adjusts rate in real time	AI is a safety component of machinery → failure could harm workers (moving parts) trigger Art 6 (1) high-risk duties	• AI Act Art 6 (1) + Annex I (Machinery) • Machinery Directive 2006/42/EC • Forskrift om maskiner (20 May 2009 nr 544)
AI controller for pressurised O_2 / CO_2 skid in a RAS facility (opens valves, maintains pressure)	Part of pressure equipment safety chain; malfunction risks pipe rupture & fish → high-risk	• AI Act Art 6 (1) + Annex I (Pressure Equipment) • Pressure Equipment Directive 2014/68/EU • Forskrift om trykkpåkjent utstyr (10 Oct 2017 nr 1631)

06.06.2025

High risk systems –
who has to do what (high level overview)

law.no

Provider (developer / vendor)	AI Act Article(s)	Deployer (farm / operator)	AI Act Article(s)
Risk-management system (identify, test, mitigate)	Art 9	Use AI system only as intended, based on Instructions for Use	Art 26(1)
High-quality, representative training & validation data	Art 10	Assign trained, competent human oversight	Art 26(2)
Technical documentation (tech file) for authorities	Art 11	— (no duty to retain or provide tech docs, but understand documentation)	—
Logging & record-keeping (built into system)	Art 12	Keep logs if under your control, for at least 6 months	Art 26(6)
Instructions for Use, capabilities & limits	Art 13	Train staff supervising or using the AI	Art 26(2)
Design for effective human oversight (override, fail-safe)	Art 14	Ensure human oversight is implemented and functioning	Art 26(2)
Accuracy, robustness & cybersecurity (by design)	Art 15	Monitor performance; suspend use & report if risk or incident arises	Art 26(5)
Conformity assessment, CE-mark, EU database registration etc	Art 43-49	Verify CE mark & registration before use	Art 26(1)
Testing, post-market monitoring plan & incident reporting	Art 60, 72-73	Report serious incidents to provider and authorities	Art 26(5)
—	—	Modify purpose or substantially alter the system → You become provider	Art 25
—	—	Fundamental Rights Impact Assessment before use (for public bodies & certain Annex III cases)	Art 27

06.06.2025

General Purpose AI
- why is it regulated?

- **GPAI = large foundation models** (e.g. GPT, Claude, vision-language models) trained for many tasks

- Not classified as high-risk on their own

- **AI Act Section V (Articles 52–55):**
  – Requires GPAI providers to publish **model card** and usage conditions
  – If designated as **systemic-risk GPAI**:
  ➤ Must implement risk-management, adversarial testing, cybersecurity measures, incident reporting

- When GPAI is built into an **AI system**, the system's **risk level is based on its intended use** (Article 6)

GPAI – roles and responsibilites

law.no

Role	Who it is	Must share		Can request
GPAI Provider (Art 52–55, Recitals 84–107	OpenAI, Microsoft, Google etc.	Model card (Art 52) Usage terms Copyright compliance policy (Recital 106) Systemic-risk controls if applicable (Art 55)	**Annex XII**: technical docs for downstream providers **Annex XI**: plain-language use instructions for deployers	N/A
Downstream Provider (e.g. livestock software vendor using GPAI)	A software company embedding GPAI in new functionality but not offering the GPAI itself	Classify the final product (Art 6) If **high-risk**: CE, risk file, human oversight If **limited-risk**: enable transparency (Art 50)	**Annex XI** to deployers (proper use & oversight) Optional transparency flags in reports/UI	Can request **Annex XII** from GPAI provider
Deployer (e.g. fish farm using the tool)	The end-user (e.g. site or ops team using the livestock software)	If high-risk only: human oversight, monitoring, incident reporting (Art 26) Otherwise: follow instructions	-	Can request **Annex XI** from provider (usage info)

06.06.2025

GPAI use cases
(risk and who must do what)

law.no

Use case	Risk level	Provider must	Deployer
GPT-powered SOP chatbot (e.g. "How do I clean net cages?")	Minimal	• **GPAI**: model card & usage terms (**Art. 52**) • **System provider**: no AI Act duties	• No obligations • Right to Instructions for Use (Art. 13, Annex XI) • Right to clarity if content simulates human interaction (Recital 85
GPT drafts lice/mortality reports (reviewed by user)	Minimal	• **GPAI**: model card (**Art. 52**) • **System provider**: no AI Act duties	• No obligations • Right to Instructions for Use (Art. 13, Annex XI) • Right to not be misled by AI-generated content (Recital 85)
GPT classifies fish from video feeds (e.g tagging, not used for direct actions)	Limited	• **GPAI**: model card (**Art. 52**) • **System provider**: ensure AI use is descriptive only (avoid automated control = no high-risk trigger)	• No obligations • Right to Instructions for Use, incl. system limits (Art. 13, Annex XI)

GPT ranks job applicants (new HR tool)	**High-risk** (Annex III – HR)	• **GPAI**: model card (Art. 52)
		• **System provider**: full Chapter III duties:
		• CE marking (Art. 43–53)
		• Risk mgmt, human oversight (Art. 9–15)
		   • Logging, registration
			• Obligations under Art. 26:
			  – Assign oversight
			  – Monitor, keep logs
			  – Report serious incidents
			• Right to full usage documentation (Annex XI)

GPT takes voice command over feed pen and activates machinery (new operations)	**High-risk** (Art 6(1)(a))	• GPAI: model card (**Art. 52**)
		• System provider: AI is safety component → full Chapter III compliance: CE marking, risk file, override, logging, etc
			• Obligations under Art. 26:
			  – Ensure human override
			  – Train staff
			  – Log & report incidents
			• Right to full usage documentation & support (Annex XI)

What should you do now?

law.no

- **Strenghten AI literacy in your organization**
  - Make sure your organization understand what AI can and can`t do
  - Staff your employees with the right tools that helps with compliance

- **Map your AI use-cases early**
  - What does the AI actually do? Control something? Rank people? Generate reports?
  - This defines the **risk level** under the AI Act — not the model itself.

- **Know your role: Provider or Deployer?**
  - If you build or brand the tool → you're the **provider**
  - If you operate it → you're the **deployer**
  - If you modify the system or its purpose → you may become the provider (Art. 25)

- **Understand the risk levels**
  - GPT controlling a feeder = safety component → high-risk
  - HR decisions = very often high-risk
  - If unsure: keep AI advisory, not autonomous

- **Vendor management and contracts**
  - Request model cards, instructions for use, and CE declarations (if high risk)
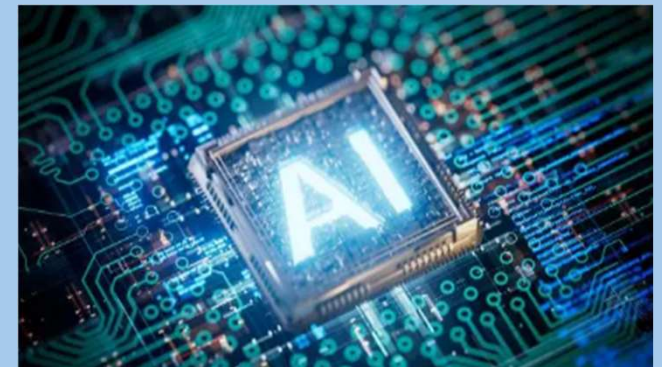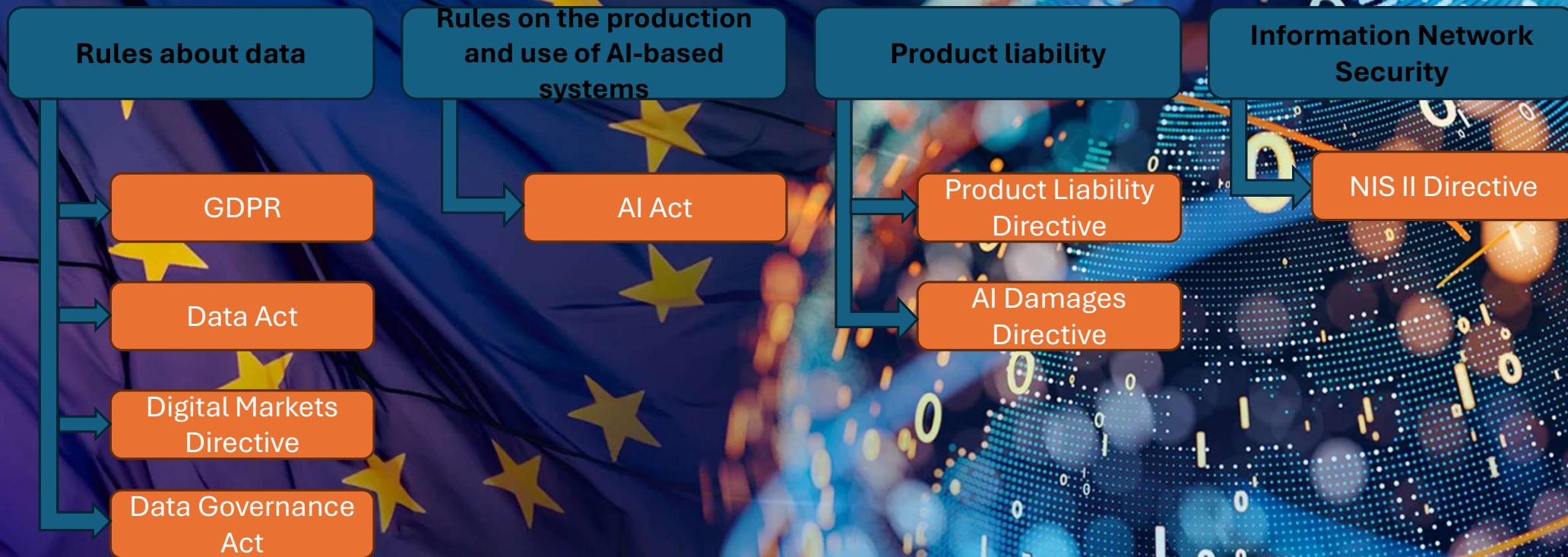 - Include transparency and compliance clauses in your contracts

Foto: Pixabay

06.06.2025

Take a Holistic Approach to Digitalisation Under Current and Emerging EU Tech Laws

Rules about data

Rules on the production and use of AI-based systems

Product liability

Information Network Security

GDPR

Data Act

Digital Markets Directive

Data Governance Act

AI Act

Product Liability Directive

AI Damages Directive

NIS II Directive

06.06.2025

law.no