

HOW AN INSTRUMENT REACHES A PARTY

Made at one level, in force by stages, binding a role that is one of the six parties.

JURISDICTION

SUPRANATIONAL  European Union

NATIONAL  United States  Ireland

SUBNATIONAL  California  Colorado

LOCAL New York City  San Francisco



Instrument

One statute, regulation, directive or binding guidance document, with its citation, status and date.

[Proposed](#) > [Enacted](#) > [In force](#)

WHOM IT BINDS

Provider  AI Act [MAKER](#)

Importer, distributor  AI Act [DISTRIBUTOR](#)

Deployer  AI Act,  state acts [OPERATOR](#)

Competent authority every regime [OVERSEER](#)

Data subject privacy law [USER](#)

Rightsholder copyright law [COUNTERPARTY](#)

1 LAW HOW LAW IS PUT TOGETHER

Instrument One statute, regulation, directive or binding guidance document, with its citation, status and date.

Jurisdiction A body of law together with the authorities and courts that apply it. A cloud region is not one.

In force The status of a duty that binds today. Enacted means it is coming; proposed means it may never arrive.

Regulation or directive In the EU a regulation applies directly in every member state; a directive is transposed into each state's own law.

Extraterritorial reach How far a law binds parties outside its territory, by the market a system is sold in and where its output is used.

Private right of action A private party's statutory right to sue for a breach, beside enforcement by a public body.

2 SOFTWARE

THE LAW THAT ALREADY BOUND SOFTWARE

Personal data Any information relating to an identified or identifiable person, location, identifiers and inferences included.

Impact assessment A written assessment of a processing operation's risks to the people whose data it uses, made before it starts.

Automated decision-making A decision about a person made by a system without meaningful human involvement, with legal or similar effects.

Text and data mining Automated analysis of text or data, model training included. Lawful without a licence only under an exception.

Age assurance Establishing that a user is above or below an age, by declaration, estimation or verification.

3 SOFTWARE LAW WHOM THE STATUTES BIND

[MAKER](#) makes it [DISTRIBUTOR](#) distributes it [OPERATOR](#) runs it [OVERSEER](#) oversees it

[USER](#) uses it [COUNTERPARTY](#) it talks to

Provider  AI Act Develops an AI system or model and places it on the market under its own name. [MAKER](#)

Importer, distributor  AI Act The parties that bring a system into a market or make it available there, with narrower duties than a provider. [DISTRIBUTOR](#)

Deployer  AI Act,  state acts Uses an AI system under its own authority. [OPERATOR](#)

Controller privacy law Decides why and how personal data is processed, and carries most of the privacy duties. [OPERATOR](#)

Processor privacy law Processes personal data on a controller's instructions, with its own narrower duties. [OPERATOR](#)

Data subject privacy law The person the personal data is about, and the holder of the rights over it. [USER](#)

Rightsholder copyright law The owner of rights in content a system reads, reuses or trains on. [COUNTERPARTY](#)

Competent authority every regime The government body empowered to enforce an instrument in a jurisdiction. [OVERSEER](#)

4 AI WHAT THE AI LAWS ASK

 **Tell the person it is a machine**

 **Mark what the machine made**

 **Tier by risk, with a prohibited top**

 **Keep a person able to intervene**

 **Keep records, and be able to explain**

 **Assign duties by role along a chain**

 **Reach by market and by output**

 **Commence in stages, and change in flight**

High-risk AI system The EU AI Act's class for AI used in listed areas such as hiring, credit, education and policing. The heaviest duties.

Prohibited practice A use an AI act bans outright, the top tier of a risk-tiered law.

General-purpose AI A model that can serve many different tasks, such as a large language model. Its provider owes duties of its own.

WHO THE LAW REACHES THROUGH

Six parties stand around any software; an agent acts on most of them at once.

 **MAKER** makes it
the developer or publisher, the model provider, upstream suppliers, open-source projects

 **DISTRIBUTOR**
distributes it
the store or marketplace, the importer, the reseller, the integrator

 **OPERATOR**
runs it
the operator, a self-hosting customer, hosting and cloud, the services on the request path



AGENT

software that pursues a goal by choosing and taking actions through tools, across more than one step, with limited human intervention between the steps

 **OVERSEER**
oversees it
regulators and courts, auditors, standards bodies, platform rule-setters

 **USER** uses it
the user as principal, the affected person, the data subject, a minor

 **COUNTERPARTY**
it talks to
the sites and interfaces it reads, the recipients it writes to, rightsholders, other users and devices

5 AGENTS

THE WORDS FOR AGENTIC SYSTEMS

Agent Software that pursues a goal by choosing and taking actions through tools, across more than one step.

Harness The software control layer between a model and the outside world. It runs the loop, connects tools, keeps state, records.

Delegation Granting an agent authority to act on behalf of a person, an organisation or a system, within a stated scope.

Human in the loop, on the loop
In the loop, a person must act before the agent proceeds. On the loop, a person watches and may act.

Kill switch A control that lets a person halt an agent at once, whatever it is doing.

Autonomy level How much an agent may do without a person approving it, from suggesting an action to taking it alone.

MCP Model Context Protocol, the open standard agents use to discover and call external tools.

6 INCIDENTS WHEN SOMETHING GOES WRONG: THE CLOCKS

Breach and incident An incident compromises a system's confidentiality, integrity or availability. A breach is the subset that exposes personal data.

Reporting clock A deadline a statute starts when an incident or a breach is detected or known, to a regulator or to the people affected.

Rung One deadline on a staged ladder. Security clocks mostly run an early warning, then a notification, then a final report.