Standard Intelligence

White paper

Enforcement Architecture

How national competent authorities will supervise AI Act compliance

PUBLISHED

February 2026

WEB

standardintelligence.com

AUDIENCE

For compliance and legal leaders responsible for AI governance in Europe

CONTENTS

Summary 3

1. Supervision is national by default, with the AI Office competent for a defined set of systems 4
   1.1 National market surveillance authorities do the front-line work 4
   1.2 The AI Office supervises general-purpose AI and a defined set of systems 5
   1.3 The United Kingdom runs a separate regime 6

2. What can be enforced now is narrower than what applies from December 2027 6

3. Designation is uneven, but the obligations apply regardless 7
   3.1 Operationally advanced: Spain, Italy, Ireland and Denmark 8
   3.2 Germany has legislated; France and the Netherlands have not finished 9
   3.3 Recent and delayed: Poland, Luxembourg and Belgium 9
   3.4 Designation status in all 27 member states 10

4. Market surveillance is likely to start with the documents 12
   4.1 The reach of surveillance follows the Act's scope 12
   4.2 Documentation review is the primary tool 13
   4.3 Authorities can inspect, test and look upstream 13
   4.4 Post-market monitoring makes compliance continuous 13

5. Four routes are most likely to draw an authority's attention 14
   5.1 Serious incident reports are likely to become the most direct trigger 14
   5.2 Anyone can complain 14
   5.3 Media coverage and parliamentary scrutiny 15
   5.4 Thematic surveillance will grow as authorities build capacity 15

6. With no one-stop shop, a problem in one member state can spread 16
   6.1 The AI Board coordinates but does not enforce 16
   6.2 Joint investigations and the safeguard procedure carry cases across borders 16
   6.3 Data protection enforcement overlaps 17

7. Penalties are tiered, and non-monetary measures may matter more 17
   7.1 The penalty structure 17
   7.2 Non-monetary measures 18

8. Seven actions reduce exposure before first contact 19
   8.1 Inventory and classify every system, with a documented rationale 19
   8.2 Keep technical documentation current and version-controlled 19
   8.3 Run post-market monitoring and incident reporting as operations 19
   8.4 Identify the authority for each system and member state, and engage early 19
   8.5 Contract for cooperation along the supply chain 20
   8.6 Prepare an enforcement response protocol and name a lead contact 20
   8.7 Fold AI Act compliance into GDPR and sectoral governance 20

9. The Standard Intelligence platform is built to produce the evidence an authority asks for 20

Where to start, and what it costs 22

Abbreviations 23

Basis and Standing 24

Sources 25

Summary

Compliance with the AI Act matters in practice because someone can enforce it, and the machinery for doing so has been assembling since August 2025. Supervision runs in layers: national market surveillance authorities on the ground, the AI Office for general-purpose AI models and a defined set of AI systems, and the AI Board coordinating between them. For most organisations the question is no longer whether supervision will reach them, but which authority it will come from, on what and when.

Supervision is national by default. Each member state must designate at least one notifying authority and one market surveillance authority, and market surveillance authorities investigate, order corrective action and, under national rules, impose fines. The AI Office supervises general-purpose AI models and, since 2 August 2026, has been exclusively competent for AI systems built on a provider's own general-purpose AI model and for AI systems in very large online platforms and search engines, with exceptions (Article 75(1), as replaced by Regulation (EU) 2026/1744). Most organisations deploying high-risk AI systems will deal with a national authority, often a sectoral one.

What can be enforced now is narrower than what applies from December 2027. The Article 5 prohibitions have applied since 2 February 2025, with penalties since 2 August 2025. National authorities have supervised AI literacy (Article 4) since 2 August 2026, and the Article 50 transparency obligations have applied since the same date. The high-risk requirements apply from 2 December 2027 for Annex III systems and 2 August 2028 for Annex I systems, subject to Article 111(2) for systems already on the market.

Designation is uneven, but the obligations apply regardless. On the Commission's list of single points of contact (last updated 7 September 2026), nine member states had a designation not marked as pending, twelve had designations pending final adoption and six were not listed. An absent or provisional authority affects when enforcement arrives, not whether the obligation exists. As at 11 October 2026, no fine under the AI Act had been confirmed by any regulator or official source.

Documentation is likely to be what an authority asks for first. Market surveillance authorities are entitled to full access to a provider's documentation and data sets for high-risk systems (Article 74(12)), and technical documentation that is not available is itself a formal non-compliance (Article 83(1)(g)). In our view, a well-documented system with identified and managed limitations is easier to defend than a well-performing system that is poorly documented.

Four routes are most likely to draw attention: incident reports, complaints, public scrutiny and thematic reviews. Serious incident reporting reaches a system only once it is high-risk under Chapter III, so in practice from 2 December 2027 or 2 August 2028, and from then it is likely to become the most direct trigger. Anyone may complain to a market surveillance authority (Article 85).

There is no general one-stop shop, so a problem in one member state can spread. Apart from the AI Office's centralised competence, the AI Act gives no single lead authority for cross-border deployments, and an organisation can face parallel national investigations. A national measure that no other authority or the Commission objects

to within three months (30 days for prohibited practices) is deemed justified, and other authorities must then take appropriate restrictive measures (Article 79(8) and (9)).

Penalties are tiered, and non-monetary measures may matter more. Fines reach EUR 35 million or 7% of worldwide annual turnover for prohibited practices, EUR 15 million or 3% for listed operator obligations and EUR 7.5 million or 1% for misleading information, whichever is higher (whichever is lower for SMEs, and for small mid-caps in the two lower tiers). For an organisation whose service depends on an AI system, an order to withdraw or recall it may cost more than any fine.

Seven actions reduce exposure before first contact. They are to inventory and classify every system; keep technical documentation current; run post-market monitoring and incident reporting as operations rather than paper; identify the authority for each system and state and engage early; contract for cooperation along the supply chain; prepare an enforcement response protocol; and fold AI Act compliance into existing GDPR and sectoral governance. The degree of cooperation, and whether the operator itself notified the infringement, are among the factors an authority weighs when setting a fine (Article 99(7)).

This paper states the position as at 11 October 2026. Basis and Standing, at the end, sets out which propositions are binding law, which are official guidance and which are our own assessment.

1. Supervision is national by default, with the AI Office competent for a defined set of systems

The AI Act does not create a single European regulator. Enforcement is distributed by the type of system, the risk it presents and where it is used, and it runs on authorities and procedures the EU already uses for product regulation.

1.1 National market surveillance authorities do the front-line work

Each member state must establish or designate at least one notifying authority and at least one market surveillance authority (Article 70(1)), which together the Act calls national competent authorities (Article 3(48)). Notifying authorities assess, designate and monitor the conformity assessment bodies that become notified bodies (Article 28(1)); market surveillance authorities supervise AI systems on the market and in use, investigate, require corrective action and apply penalties under national rules. Each member state must also designate one market surveillance authority as its single point of contact, and had to make contact details for its authorities publicly available by 2 August 2025 (Article 70(2)).

A member state may use one authority or several, and the Act sets some defaults:

(a) for high-risk AI systems related to products covered by the Annex I Section A legislation, the market surveillance authority is the one already responsible under that legislation (Article 74(3));

(b) for high-risk AI systems placed on the market, put into service or used by financial institutions in direct connection with financial services, it is the financial supervisor (Article 74(6));
(c) for high-risk biometric systems used for law enforcement, border management, justice and democracy, and for the Annex III systems in law enforcement, migration and the administration of justice and democratic processes, it is the data protection authority or another authority meeting the same independence conditions (Article 74(8)).

Many member states have built on these defaults, assigning AI in each sector to the regulator that already supervises that sector, so one organisation may answer to several authorities in one country. Market surveillance runs through Regulation (EU) 2019/1020 (Article 74(1)), which gives authorities the toolkit they already use for other products. Whether a fine is imposed by the authority itself or by a court depends on the national legal system (Article 99(9)).

1.2 The AI Office supervises general-purpose AI and a defined set of systems

The AI Office is the Commission's function for implementing and supervising the Act at EU level (Article 3(47)). The Commission has exclusive powers to supervise and enforce the obligations of providers of general-purpose AI models and entrusts that work to the AI Office (Article 88(1)). It may request documentation and information (Article 91), evaluate a model, including through access to its APIs or source code (Article 92(3)), and fine a provider up to EUR 15 million or 3% of worldwide annual turnover, whichever is higher (Article 101, applicable from 2 August 2026).

Since 2 August 2026 the AI Office has also been exclusively competent for two kinds of AI system (Article 75(1), as replaced by Regulation (EU) 2026/1744):

(a) AI systems based on a general-purpose AI model where the model and the system are developed by the same provider or undertaking, except AI systems related to Annex I products, Annex III point 2 systems, systems of law enforcement authorities, border management authorities and financial institutions within Article 74(6), and Annex III point 8 systems as regards the administration of justice;
(b) AI systems that constitute or are integrated into a designated very large online platform or very large online search engine.

For these systems the AI Office has the powers of a market surveillance authority, including remote and on-site inspections (Article 75a), and it can fine operators on the Article 99 scale and impose periodic penalty payments (Article 75c). Its competence applies to the providers of these systems, and to deployers only where they are also the provider or part of the same undertaking (Article 75(1)). Beyond these systems, the AI Office supports coordination, joint investigations and the AI Board; it does not supervise the many organisations that deploy third-party AI in their own operations.

> *The AI Office's direct enforcement reach is narrower than many organisations assume: providers of general-purpose AI models, and a defined set of systems built on a provider's own model or integrated into very large platforms. For most businesses using AI in their operations, the supervisor is national.*

Enforcement authority overview

Authority	Jurisdiction	Key powers	Penalty authority
AI Office (European Commission)	All general-purpose AI models (Art. 88); AI systems within Art. 75(1) since 2 Aug 2026	Request documentation, evaluate models, inspect, order corrective measures, accept binding commitments	GPAI providers: up to EUR 15 million or 3% of turnover, whichever is higher (Art. 101, from 2 Aug 2026). Art. 75(1) systems: fines on the Art. 99 scale and periodic penalty payments (Art. 75c)
Market surveillance authority	AI systems placed on the market, put into service or used in its territory, other than those within Art. 75(1)	Documentation and data access, inspections, testing, corrective measures, restriction, withdrawal and recall	Fines under national rules, up to EUR 35 million or 7% (Art. 99)
Sectoral regulator acting as market surveillance authority	For example, financial institutions (Art. 74(6)) and Annex I Section A products (Art. 74(3))	Market surveillance powers alongside sector-specific supervision and licence conditions	Art. 99 for AI Act breaches; sectoral law otherwise
Notified body	Third-party conformity assessment for certain high-risk systems	Assessment, certification, suspension or withdrawal of certificates	No fine authority

1.3 The United Kingdom runs a separate regime

The United Kingdom is not bound by the AI Act. As at 11 October 2026 it had no equivalent statute and no government AI bill; most AI is regulated at the point of use by existing sector regulators, and the AI Security Institute is a research organisation within the Department for Science, Innovation and Technology, not a regulator.

A UK organisation is still within the AI Act where it places systems on the EU market or where its system's output is used in the EU (Article 2(1)(a) and (c)). An organisation operating in both jurisdictions faces materially different obligations and supervisory contacts, and should manage the two regimes as distinct compliance workstreams.

2. What can be enforced now is narrower than what applies from December 2027

The AI Act applies in stages (Article 113, as amended by Regulation (EU) 2026/1744), and an authority can enforce only an obligation that already applies. As at 11 October 2026 the position was as follows.

Obligation	Applies from	Supervised by
Prohibited practices (Article 5)	2 February 2025, with penalties from 2 August 2025; two further prohibitions (non-consensual intimate imagery and child sexual abuse material) from 2 December 2026	Market surveillance authorities; the AI Office for systems within Art. 75(1)
AI literacy (Article 4)	2 February 2025; national supervision and enforcement from 2 August 2026 (Commission AI literacy Q&A)	Market surveillance authorities
Transparency (Article 50)	2 August 2026; for generative systems already on the market, the Article 50(2) marking duty by 2 December 2026 (Article 111(4))	Market surveillance authorities; the AI Office for systems within Art. 75(1)
General-purpose AI model obligations (Chapter V)	2 August 2025 (2 August 2027 for models placed on the market before 2 August 2025, Article 111(3)); Commission fines from 2 August 2026	AI Office
High-risk requirements and operator obligations (Chapter III, Sections 1 to 3)	2 December 2027 (Annex III); 2 August 2028 (Annex I)	Market surveillance authorities; the AI Office for systems within Art. 75(1)

High-risk systems placed on the market or put into service before their application date are caught only if their design changes significantly from that date, although providers and deployers of high-risk systems intended for use by public authorities must comply by 2 August 2030 (Article 111(2), as amended). Post-market monitoring (Article 72) and serious incident reporting (Article 73) sit in Chapter IX, which was not deferred, but they reach a system only once it is high-risk under Chapter III, so in practice they apply from 2 December 2027 or 2 August 2028.

Until December 2027, therefore, an authority's most likely subjects are prohibited practices, AI literacy and transparency, together with general-purpose AI models and the systems within the AI Office's competence. As at 11 October 2026, no fine under the AI Act had been confirmed by any regulator or official source.

> *Once the high-risk obligations apply, we expect many organisations deploying high-risk AI systems in Europe to have their first substantive supervisory engagement. Organisations that have completed their risk classifications and technical documentation before that engagement are likely to have a materially better experience of it than those that have not.*

3. Designation is uneven, but the obligations apply regardless

The 2 August 2025 deadline for designation has passed and the result is uneven. On the Commission's list of single points of contact, last updated 7 September 2026, nine member states had a designation not marked as pending, twelve had designations

pending final adoption and six (Austria, Belgium, Bulgaria, Croatia, Hungary and Slovakia) were not listed. Being pending on that list, or absent from it, is not the same as having no authority: Germany and Hungary have designated their authorities by law, and Spain's AESIA is operational.

The absence of an operational authority does not suspend an organisation's obligations. It affects the timing and likely intensity of enforcement in that member state, and an organisation should calibrate its engagement accordingly.

The Commission has said it may open a formal infringement procedure against a member state that fails to designate. We are not aware of any such proceedings as at 11 October 2026; if they follow, they may increase pressure on the authorities concerned to show enforcement activity once operational.

3.1 Operationally advanced: Spain, Italy, Ireland and Denmark

Spain. In our view Spain has the most purpose-built supervisory structure in the EU. The Agencia Española de Supervisión de la Inteligencia Artificial (AESIA) has its statute in Royal Decree 729/2023, so it was operating before the Act's penalty provisions applied. The draft Organic Law for the proper use and governance of AI, approved by the Council of Ministers on 26 May 2026 and sent to Parliament, gives AESIA a central role as reference body and coordination point, with some competences remaining with sectoral authorities such as the Spanish Data Protection Agency (AEPD) and the General Council of the Judiciary (CGPJ).

Italy. Law No. 132 of 23 September 2025, in force since 10 October 2025, made Italy, with Lithuania and Denmark, one of the first member states with national implementing legislation in force. The Agency for National Cybersecurity (ACN) is the market surveillance authority and single point of contact, and the Agency for Digital Italy (AgID) the notifying authority. The law gave the government twelve months to adopt implementing decrees; the second of these, Legislative Decree No. 179 of 7 October 2026 on the powers of the national authorities (published on 8 October 2026 and taking effect on 23 October 2026), gives the Bank of Italy, CONSOB and IVASS supervision of high-risk systems used in the services they supervise.

Ireland. Ireland took a deliberately distributed approach. The European Union (Artificial Intelligence) (Designation) Regulations 2025 (S.I. No. 366 of 2025) made the Central Bank of Ireland the market surveillance authority for Article 74(6) and the Data Protection Commission for Article 74(8), and in September 2025 the Government confirmed fifteen competent authorities across sectors including financial services, consumer protection, health, utilities and telecommunications.

The Regulation of Artificial Intelligence Act 2026, enacted on 21 July 2026, establishes the AI Office of Ireland (Oifig IS na hÉireann) and designates it as the single point of contact (section 42), with commencement by ministerial order. Given the number of major technology companies with European headquarters in Dublin, we expect Irish authorities to be among the most active in the EU, although systems within the AI Office's competence under Article 75(1) are supervised centrally.

Denmark. Act No. 467 of 14 May 2025, one of the earliest national laws, designates the Agency for Digital Government (Digitaliseringsstyrelsen) as notifying authority, single point of contact and market surveillance authority for the prohibitions in Article 5(1)(a) to (c), (e) and (f). The Danish Data Protection Agency (Datatilsynet) covers Article 5(1)(d) and

(g), and the Danish Court Administration covers the courts' use of AI systems when they are not acting in a judicial capacity.

3.2 Germany has legislated; France and the Netherlands have not finished

Germany. The KI-Marktüberwachungs-und-Innovationsförderungs-Gesetz (KI-MIG), Article 1 of the Act implementing the AI Regulation of 22 July 2026 (BGBl. 2026 I Nr. 223), has been in force since 29 July 2026, although the Commission's list of 7 September 2026 still showed Germany's designation as pending. It makes the Federal Network Agency (Bundesnetzagentur, BNetzA) the single point of contact and, unless the Act provides otherwise, the market surveillance authority, with the Federal Financial Supervisory Authority (BaFin) as market surveillance authority for AI systems directly linked to regulated financial activity. The BNetzA launched a KI-Service Desk on 3 July 2025 to help organisations with compliance questions.

France. France had not adopted its designation as at 11 October 2026. A draft designation published by the Directorate-General for Enterprise (DGE) on 9 September 2025 proposed seventeen market surveillance authorities, a coordinating tandem of the DGE and the Directorate-General for Competition Policy, Consumer Affairs and Fraud Control (DGCCRF), and the data protection authority (CNIL) as the authority for the largest number of use cases. In February 2026 the government proposed, by amendment to its bill adapting French law to EU law (the DDADUE bill), to give the CNIL the central role; the Commission's list shows the DGCCRF as single point of contact, pending final adoption.

The Netherlands. The Netherlands had not formally appointed its market surveillance authorities, though the structure is clear. The Dutch Authority for Digital Infrastructure (RDI) and the Dutch Data Protection Authority (AP) are expected to share coordinating responsibilities, and the Commission lists the RDI as single point of contact, pending final adoption.

3.3 Recent and delayed: Poland, Luxembourg and Belgium

Poland. Poland has established by law a dedicated AI supervisory body, the Commission for the Development and Security of Artificial Intelligence (KRiBSI), which will also receive complaints about AI systems. With Spain's AESIA and the AI Office of Ireland, it is one of the few authorities created specifically for AI. The President signed the Act on AI systems in July 2026, and the Commission lists KRiBSI as Poland's single point of contact.

Luxembourg. Bill No. 8476, which would make the National Commission for Data Protection (CNPD) the default horizontal market surveillance authority, was still before the Chamber of Deputies in July 2026. The Commission lists the CNPD as single point of contact, pending final adoption.

Belgium. Belgium is further behind. On 2 August 2026 no authority had been formally appointed; the Federal Public Service Economy confirmed the Belgian Institute for Postal Services and Telecommunications (BIPT) as the intended authority, but it was still preparing a preliminary draft bill that the government would then have to put to Parliament. Supervision of AI in regional competences, such as education and employment services, was also unresolved.

3.4 Designation status in all 27 member states

Member state	Lead or expected authority	Model	National AI law	Status	Commission list, 7 Sept 2026: single point of contact; status
Spain	AESIA (SPOC, pending)	Purpose-built AI authority	Bill sent to Parliament (26 May 2026)	Operationally advanced	AESIA; pending
Italy	ACN (MSA and SPOC); AgID (notifying)	Cybersecurity-led, sectoral carve-outs	Enacted Oct 2025; Legislative Decree 179/2026 (in force 23 Oct 2026)	Operationally advanced	ACN; not marked pending
Ireland	AI Office of Ireland (SPOC); 15 sectoral authorities	Distributed, sector-led	Enacted (21 July 2026)	Operationally advanced	AI Office of Ireland; not marked pending
Denmark	Agency for Digital Government; Datatilsynet	Centralised MSA	Enacted May 2025 (Act 467/2025)	Operationally advanced	Agency for Digital Government; not marked pending
Germany	BNetzA (MSA and SPOC); BaFin for finance	Multi-authority; BaFin for finance	Enacted July 2026 (in force 29 July 2026)	Designated by law; Commission list shows pending	Bundesnetzagentur; pending
France	DGCCRF (SPOC, pending); CNIL lead proposed Feb 2026	Sector-split; lead not settled	No AI law; designation pending	Advanced; designation pending	DGCCRF; pending
Netherlands	RDI and AP (co-coordinators)	Sector-led; AP active on GDPR overlap	No national law	Advanced; formal appointment pending	RDI; pending
Poland	KRiBSI	Purpose-built AI authority	Enacted (signed July 2026)	Designated	KRiBSI; not marked pending
Luxembourg	CNPD (coordinator)	DPA-led with sectoral bodies	Draft bill	Progressing; delayed	CNPD; pending
Belgium	BIPT (expected)	Telecoms authority as lead	No bill tabled	Delayed	No entry
Sweden	PTS (SPOC, pending)	Telecoms MSA; Medical Products Agency notifying for MDR/IVDR-linked systems (proposed)	Draft in progress	Designation pending	PTS; pending

Member state	Lead or expected authority	Model	National AI law	Status	Commission list, 7 Sept 2026: single point of contact; status
Finland	Traficom (SPOC)	Sector-led	Enacted Dec 2025 (Act 1377/2025, in force 1 Jan 2026)	Designated	Traficom; not marked pending
Lithuania	Communications Regulatory Authority (RRT)	Existing digital authority	Enacted Jan 2025 (Law No. XV-106, in force 1 Apr 2025)	Designated	RRT; not marked pending
Latvia	Consumer Rights Protection Centre (PTAC)	Consumer protection authority	Cabinet Regulation No. 478 (in force 15 Aug 2025) assigns PTAC its AI Act tasks; no dedicated AI law identified	Designated	PTAC; not marked pending
Estonia	Consumer Protection and Technical Regulatory Authority	Existing consumer and technical regulator	No draft published	Designation pending	Consumer Protection and Technical Regulatory Authority; pending
Cyprus	Commissioner of Communications (pending)	Communications regulator	Designation pending final adoption	Designation pending	Commissioner of Communications; pending
Malta	MDIA and IDPC	Innovation authority and DPA	Government draft	Identification confirmed	MDIA; not marked pending
Slovakia	To be confirmed	To be confirmed	Draft proposal	Early stage	No entry
Czechia	Czech Telecommunication Office (ČTÚ) (pending)	To be confirmed	Draft in progress	Designation pending	Czech Telecommunication Office; pending
Hungary	Minister responsible for enterprise development (MSA and SPOC); National Accreditation Authority (notifying); MNB for finance	Ministerial MSA; MNB for finance	Act LXXV of 2025, in force 1 Dec 2025	Designated by law; not on Commission list	No entry
Portugal	ANACOM (pending)	To be confirmed	No implementing law identified; designation	Designation pending	ANACOM; pending

Member state	Lead or expected authority	Model	National AI law	Status	Commission list, 7 Sept 2026: single point of contact; status
			pending final adoption		
Greece	Hellenic Data Protection Authority	DPA-led	Enacted July 2026 (Law 5321/2026)	Designated	Hellenic Data Protection Authority; not marked pending
Romania	ANCOM (pending)	To be confirmed	No implementing law identified; ANCOM proposed by government memorandum	Designation pending	ANCOM; pending
Bulgaria	To be confirmed	To be confirmed	No public announcement	Not yet designated	No entry
Croatia	To be confirmed	To be confirmed	No public announcement	Not yet designated	No entry
Austria	To be confirmed	To be confirmed	No public announcement	Not yet designated	No entry
Slovenia	AKOS (pending)	To be confirmed	Draft referenced	Designation pending	AKOS; pending

Commission list, 7 September 2026: 21 single points of contact (9 not marked pending, 12 pending final adoption of the national designation decision) and 6 with no entry. National-law columns reflect national sources to 11 October 2026.

4. Market surveillance is likely to start with the documents

Market surveillance under the AI Act applies the EU's product framework, Regulation (EU) 2019/1020, to software that can be updated, retrained and modified after it is placed on the market (Article 74(1)).

4.1 The reach of surveillance follows the Act's scope

Authorities supervise AI systems placed on the market, put into service or used in their territory. The Act reaches providers wherever they are established when they place systems on the EU market or put them into service, deployers established or located in the EU, and third-country providers and deployers where the system's output is used in the EU (Article 2(1)(a) to (c)).

Surveillance can be proactive, where an authority examines a category of systems on its own initiative (Regulation (EU) 2019/1020, Article 14(4)(f)), or reactive, prompted by a complaint, an incident report or a referral from another authority.

4.2 Documentation review is the primary tool

For a high-risk system, the provider must draw up technical documentation before the system is placed on the market and keep it up to date (Article 11(1) and Annex IV), and keep it at the disposal of national competent authorities for ten years after the system is placed on the market or put into service (Article 18(1)). On a reasoned request, the provider must supply the information and documentation needed to show conformity, and access to the logs under its control (Article 21). Market surveillance authorities are entitled to full access to the documentation and to the training, validation and testing data sets, where appropriate remotely through APIs (Article 74(12)).

In our view, the documentation is likely to be an authority's first request when it looks at a system, and a gap in it is itself a finding. Technical documentation that is not available is a formal non-compliance which, if it persists, can lead to the system being restricted, withdrawn or recalled (Article 83). An organisation that cannot produce complete, current and accurate documentation promptly risks an early finding against it.

> *In our view, documentation is likely to shape an organisation's initial position in an investigation more than any other factor. A system that performs well but is poorly documented is harder to defend than a well-documented system with identified and managed limitations.*

4.3 Authorities can inspect, test and look upstream

Beyond reviewing documents, market surveillance authorities hold the powers in Article 14(4) of Regulation (EU) 2019/1020, including unannounced on-site inspections and physical checks, entry to business premises, and acquiring samples, including under a cover identity, to inspect and reverse-engineer them. Some of these powers can be exercised remotely for AI systems (Article 74(5)). Access to source code is available on a reasoned request once testing based on the documentation and data has been exhausted or proved insufficient (Article 74(13)), and national bodies protecting fundamental rights can ask the market surveillance authority to organise testing of a high-risk system (Article 77(3)).

Authorities can also require information on the supply chain (Regulation (EU) 2019/1020, Article 14(4)(b)). For organisations that build on third-party components or general-purpose AI models, an investigation can therefore reach upstream, and contracts should ensure that suppliers can and will cooperate with it (section 8.5).

4.4 Post-market monitoring makes compliance continuous

Providers of high-risk systems must run a documented post-market monitoring system that actively and systematically collects and analyses data on the system's performance throughout its lifetime (Article 72(1) and (2)). Deployers must monitor the system's operation on the basis of the instructions for use and, where relevant, inform the provider (Article 26(5)).

Providers must report serious incidents to the market surveillance authorities of the member state where the incident occurred (Article 73(1)), or to the AI Office for systems within its competence (Article 75(1a)). These duties apply in practice from 2 December 2027 (Annex III) or 2 August 2028 (Annex I) (section 2), and from then compliance becomes a continuous obligation rather than a one-off certification.

5. Four routes are most likely to draw an authority's attention

Knowing what prompts an investigation helps an organisation judge its enforcement risk. The Act does not limit what can start supervisory scrutiny, and authorities may investigate on their own initiative, but some triggers are much more likely than others in the early period.

Some sectors are likely to draw attention first. In our assessment, authorities are likely to focus first on sectors where AI adoption is highest and failure most costly: financial services, healthcare, recruitment and critical infrastructure. Organisations in these sectors should treat early voluntary engagement with their authority as an opportunity.

5.1 Serious incident reports are likely to become the most direct trigger

A serious incident is an incident or malfunctioning of an AI system that directly or indirectly leads to death or serious harm to a person's health, a serious and irreversible disruption of the management or operation of critical infrastructure, an infringement of obligations under Union law intended to protect fundamental rights, or serious harm to property or the environment (Article 3(49)). The provider must report immediately once it has established a causal link, or the reasonable likelihood of one, and in any event within 15 days of becoming aware of the incident; the limit is 10 days in the event of a death and 2 days for a widespread infringement or a critical-infrastructure incident (Article 73(2) to (4)).

A report obliges the authority to act: it must take appropriate measures within seven days of receiving the notification (Article 73(8)). Because Article 73 reaches a system only once it is high-risk under Chapter III, this trigger operates in practice from 2 December 2027 or 2 August 2028 (section 2).

5.2 Anyone can complain

Any natural or legal person with grounds to consider that the Act has been infringed may complain to the relevant market surveillance authority (Article 85), and the Commission describes complaints from individuals as "an essential contribution to an effective enforcement of the AI Act". Complaints from affected individuals, civil society organisations, competitors and employees are all plausible.

> *In our view, the AI Act makes competitor complaints a credible enforcement risk, particularly in sectors where AI adoption is concentrated and a non-compliant system could give a significant commercial advantage.*

5.3 Media coverage and parliamentary scrutiny

Regulatory authorities are not immune to external pressure, and they will face political and media attention over prominent AI deployments. In our view, a high-profile story about an AI system causing unfair outcomes, discriminatory decisions or safety failures is likely to prompt an authority to consider whether it has grounds for a formal investigation.

5.4 Thematic surveillance will grow as authorities build capacity

As their capacity grows, we expect authorities to move from reactive enforcement to thematic exercises in which an authority examines a category of AI systems across several providers at once. In other product regimes such reviews typically begin with a questionnaire to identified operators in a sector, followed by documentation reviews and possibly on-site assessment. Selection for a thematic review does not imply suspected non-compliance; authorities use them to build market intelligence as much as to find violations.

Registration also makes a system visible. When monitoring whether providers have wrongly classified Annex III systems as not high-risk, authorities may carry out checks using the information in the EU database (Article 80(8)).

Investigation trigger risk matrix (our assessment)

Trigger	Likelihood	Lead time	Severity if non-compliant	Mitigation
Serious incident report	Medium-High once high-risk obligations apply (from Dec 2027 or Aug 2028)	Immediate	Very High	Incident response plan; rapid engagement with the authority
Third-party complaint (individual)	Medium	Days to weeks	Medium-High	Accessible complaint mechanisms; documented decisions
Competitor complaint	Medium (in concentrated sectors)	Days to weeks	High	Complete conformity documentation
Media or parliamentary attention	Low-Medium	Variable	High (reputational)	Proactive communications strategy
Thematic review	Low-Medium (increasing)	Weeks to months	Medium	Questionnaire readiness; documentation hygiene
Cross-border referral from another authority	Low	Months	High	Consistent EU-wide compliance approach

6. With no one-stop shop, a problem in one member state can spread

AI systems rarely operate within one national jurisdiction. A provider established in Ireland may supply a high-risk system used across the single market, and a German company may license an AI tool developed in France. The AI Act handles this through the AI Board, joint activities and procedures that carry a national measure across borders.

6.1 The AI Board coordinates but does not enforce

The AI Board, established under Article 65, is the main coordination forum for member states. It has one representative per member state; the European Data Protection Supervisor participates as an observer, and the AI Office attends without voting and provides the secretariat (Article 65). Its standing sub-group for market surveillance acts as the administrative cooperation group for the Act (Article 65(6)).

The Board advises and assists the Commission and the member states: it contributes to coordination among national authorities, supports joint activities of market surveillance authorities, issues recommendations and written opinions, and helps develop common criteria and a shared understanding of the Act's concepts (Article 66). It cannot fine or direct an authority, but in our view its opinions will carry considerable persuasive weight and shape how authorities approach enforcement, so organisations should follow its published outputs.

6.2 Joint investigations and the safeguard procedure carry cases across borders

Where specific categories of high-risk AI systems are found to present a serious risk across two or more member states, market surveillance authorities or the Commission may propose joint activities, including joint investigations, conducted by the authorities concerned or jointly with the Commission, with coordination support from the AI Office (Article 74(11)). The Act does not designate a lead authority for them.

A national finding can also travel without a joint investigation. Where an authority considers that non-compliance is not confined to its territory, it must inform the Commission and the other member states (Article 79(3)); if no authority or the Commission objects to its provisional measure within three months (30 days for prohibited practices), the measure is deemed justified and authorities must ensure appropriate restrictive measures, such as withdrawal from their markets (Article 79(8) and (9)). Where there is an objection, the Commission decides, and if it finds the measure justified, every member state must take appropriate restrictive measures (Article 81).

For systems within the AI Office's competence, a market surveillance authority with well-founded reasons to suspect an infringement may ask the AI Office, through its single point of contact, to assess the matter (Article 75(2a)).

> *In our view, these mechanisms raise the enforcement risk for large-scale cross-border deployments. Organisations that run jurisdiction-by-jurisdiction compliance without coordination risk inconsistencies that become visible when authorities compare notes.*

6.3 Data protection enforcement overlaps

Many high-risk AI systems process personal data, bringing them within both the AI Act and the GDPR. The Act makes data protection authorities, or other authorities meeting the same independence conditions, the market surveillance authorities for several categories of high-risk system (Article 74(8)), and requires member states to facilitate coordination between market surveillance authorities and other relevant authorities (Article 74(10)). National bodies that enforce fundamental rights law, including the right to non-discrimination, may request documentation from the market surveillance authority (Article 77(1)), so an investigation under one regime can supply evidence to another.

The GDPR's one-stop shop has no general equivalent. Organisations established in Ireland or Luxembourg that serve customers across the EU may ask whether the AI Act produces a lead-authority model like the GDPR's one-stop shop. Largely it does not. Apart from the AI Office's centralised competence under Article 75(1), as replaced by Regulation (EU) 2026/1744, an organisation may face parallel investigations in every member state where its system is placed on the market or used.

7. Penalties are tiered, and non-monetary measures may matter more

The AI Act's penalty regime is among the most severe in EU regulatory law, scaled to the gravity of the infringement and the size of the operator. Member states lay down the rules on penalties, which may include fines, warnings and non-monetary measures, and must make them effective, proportionate and dissuasive (Article 99(1)).

7.1 The penalty structure

Non-compliance with the Article 5 prohibitions attracts fines of up to EUR 35 million or 7% of total worldwide annual turnover, whichever is higher (Article 99(3)). Non-compliance with the operator and notified-body obligations listed in Article 99(4), which include the obligations of providers (Article 16), authorised representatives, importers and distributors (Articles 22 to 24), the value-chain obligations in Article 25(2) and (4), deployers (Article 26) and the Article 50 transparency obligations, attracts fines of up to EUR 15 million or 3%, whichever is higher. Supplying incorrect, incomplete or misleading information to notified bodies or national competent authorities in reply to a request attracts fines of up to EUR 7.5 million or 1%, whichever is higher (Article 99(5)).

For SMEs, including start-ups, each fine is capped at whichever of the two amounts is lower (Article 99(6)); for small mid-caps the same applies to the Article 99(4) and (5) tiers (Article 99(6a)). A provider found to have misclassified an Annex III system as not high-risk in order to circumvent the requirements is subject to fines under Article 99 (Article 80(7)).

The AI Office applies the Article 99(3) to (7) scale to operators within Article 75(1), and for them any infringement of an applicable provision, including one not listed in Article 99(4), can attract a fine at the Article 99(4) level (Article 75c(4)). It may also impose periodic penalty payments of up to 5% of average daily income or worldwide annual turnover per day to compel compliance with an investigation or decision (Article 75c(5)).

Maximum fines (whichever is higher; whichever is lower for SMEs, and for small mid-caps in the Article 99(4) and (5) tiers)

Infringement	Maximum fine	Share of worldwide annual turnover	Relevant articles
Prohibited AI practices	EUR 35 million	7%	Art. 99(3); Art. 5
Operator and notified-body obligations listed in Art. 99(4)	EUR 15 million	3%	Art. 99(4): Arts 16, 22 to 24, 25(2) and (4), 26, 31, 33(1), (3) and (4), 34, 50
Incorrect, incomplete or misleading information to notified bodies or national competent authorities	EUR 7.5 million	1%	Art. 99(5)
Obligations of providers of general-purpose AI models, including those with systemic risk	EUR 15 million	3%	Art. 101 (Commission; from 2 Aug 2026)
Systems within the AI Office's competence	Art. 99 scale; any applicable provision at the Art. 99(4) level	Periodic penalty payments up to 5% of average daily income or turnover per day	Art. 75c

When deciding whether to fine and how much, an authority must take account of all relevant circumstances, including the degree of cooperation with the authority, the technical and organisational measures the operator had implemented, the manner in which the infringement became known (in particular whether the operator notified it) and any action taken to mitigate the harm (Article 99(7)). These are the factors that preparation can influence.

7.2 Non-monetary measures

Beyond fines, authorities have a broad set of non-monetary measures. Where a system presenting a risk does not comply, the authority must require the operator to take corrective action, withdraw the system or recall it within a period it may prescribe and in any event within the shorter of 15 working days or the period set by the relevant sectoral legislation (Article 79(2)); if the operator does not act, the authority takes provisional measures to prohibit or restrict the system (Article 79(5)). Authorities can also require measures for a compliant system that still presents a risk (Article 82) and act against formal non-compliance such as missing documentation or registration (Article 83).

> *For an organisation whose service depends on an AI system, an order to suspend, withdraw or recall it may be a greater operational risk than any fine.*

8. Seven actions reduce exposure before first contact

Enforcement risk under the AI Act is not binary. It depends on the systems an organisation operates, the quality of its compliance programme and how far responsible AI governance is embedded in how it works, and it can be reduced across four dimensions: governance, documentation, readiness for surveillance and engagement with the authority.

8.1 Inventory and classify every system, with a documented rationale

Before any enforcement risk can be managed, an organisation needs to know which AI systems it provides or deploys. Each system should be mapped against the Act's risk classification, with a documented rationale. The inventory should be completed before the high-risk obligations apply (2 December 2027 for Annex III systems; 2 August 2028 for Annex I systems), and should note which systems were already on the market and fall under Article 111(2).

In our view, systems classified as not high-risk that should have been classified as high-risk are among the largest compliance exposures: an authority can evaluate the classification and require the provider to bring the system into compliance (Article 80(1) and (2)), and misclassification to circumvent the requirements attracts fines (Article 80(7)).

8.2 Keep technical documentation current and version-controlled

Documentation under Article 11 must be complete and kept up to date, so it should be treated as a living record rather than a one-off submission. Version control should ensure that each update to a system is assessed against its conformity assessment, because a substantial modification requires a new conformity assessment (Article 43(4)).

8.3 Run post-market monitoring and incident reporting as operations

Post-market monitoring is among the most demanding operational requirements in the Act. An organisation should designate a responsible function, set up data collection on system performance, define incident classification criteria and build the internal processes needed to meet the Article 73 reporting periods. In our view, authorities are likely to distinguish organisations with working monitoring programmes from those with paper frameworks.

8.4 Identify the authority for each system and member state, and engage early

The table in section 3.4 is the starting point; for each system, identify the market surveillance authority in each member state where it is placed on the market or used, including any sectoral default under Article 74. Authorities may provide guidance and advice, in particular to SMEs and small mid-caps (Article 70(8)), and each member state must have at least one AI regulatory sandbox operational by 2 August 2027 (Article 57(1)). Early voluntary engagement, through consultations, service desks such as the BNetzA's KI-Service Desk, sandboxes or direct dialogue, gives insight into supervisory expectations and may build goodwill that matters if a compliance issue later arises.

8.5 Contract for cooperation along the supply chain

Providers that integrate third-party AI components remain responsible for their own system's compliance, and deployers must use high-risk systems in accordance with the instructions for use (Article 26(1)). A provider and a third party supplying an AI system, model, tool or component used in a high-risk system must specify by written agreement the information, technical access and other assistance the provider needs to comply (Article 25(4)), and this obligation is fineable at the Article 99(4) level once the high-risk obligations apply. Contracts with AI suppliers should also include compliance representations and warranties, audit rights and obligations to cooperate with investigations.

8.6 Prepare an enforcement response protocol and name a lead contact

An organisation should prepare for an investigation before one begins. A response protocol sets out who leads the response, how documentation will be retrieved and reviewed, how legal privilege will be managed and how communications with the authority will be coordinated, and it should name the person who acts as the authority's contact. Providers must supply documentation on a reasoned request (Article 21), and the degree of cooperation and whether the operator notified the infringement are among the factors weighed when a fine is set (Article 99(7)(f) and (h)).

8.7 Fold AI Act compliance into GDPR and sectoral governance

For an organisation with a mature GDPR programme, the AI Act adds obligations that are structurally similar in several respects: documentation, risk assessment, accountability and cooperation with supervisory authorities. The most efficient approach is to integrate AI Act compliance into existing data governance and regulatory compliance frameworks rather than run it as a standalone workstream.

9. The Standard Intelligence platform is built to produce the evidence an authority asks for

The seven actions in section 8 describe what an organisation needs to do. The Standard Intelligence platform is designed to make that work evidenced, auditable and reproducible under regulatory pressure, through three capabilities: the AI Intelligence Centre, the AI Regulatory Navigator and the AI Literacy Certification Platform.

In our experience, the difference between organisations that manage compliance well and those that struggle is rarely intent; it is architecture. An organisation that has assembled its compliance position from spreadsheets, shared drives and manually maintained records will have a very different experience of an investigation from one whose records are structured, version-controlled and generated from auditable events.

> *Authorities do not assess compliance in the abstract. They assess the evidence an organisation can produce, on request and under time pressure, so the architecture of a compliance programme matters as much as its substance.*

The AI Intelligence Centre holds the compliance register. It is the central register of every AI System Documentation Pack (AISDP) in an organisation's portfolio. In an investigation it gives an immediate view of the organisation's AI systems and their compliance status, and it generates a Submission Package designed to be handed to a notified body or national competent authority without further preparation.

Every AISDP in the register carries live status, risk classification, the applicable Annex III category, operator role, deployment date, certification expiry and the date of the last substantive change. Every modification creates a sequentially numbered, timestamped snapshot recording the author, the reason for the change and the complete state of the entry at that point. The platform generates the record of lifecycle changes that Annex IV point 6 requires, which in our view is the evidence an authority will look for that the organisation has assessed its systems continuously.

The AI Regulatory Navigator records classification decisions. We expect misclassification to be among the early findings in investigations, and the Navigator is designed to surface it before deployment. An organisation describes its AI application in plain language, and the Navigator returns a structured regulatory assessment grounded in the text of the AI Act (articles, annexes and recitals) and published Commission guidance, with every claim supported by an inline citation to the passage relied on.

When an authority asks how an organisation decided that a system fell outside Annex III, "we assessed it internally and concluded it was not high-risk" is a much weaker answer than a saved Navigator assessment dated before deployment, grounded in the Act and Commission guidance, with citations attached to the system record. The Navigator turns a classification discussion into dated, citable documentary evidence.

The AI Literacy Certification Platform records the Article 4 measures. Article 4 has applied since 2 February 2025. As replaced from 27 July 2026 by Regulation (EU) 2026/1744, it requires providers and deployers to take measures to support AI literacy and does not require them to guarantee any specific level. National market surveillance authorities have supervised it since 2 August 2026, and the Commission has said no certificate is needed.

In our view, dated, role-specific records are the most useful evidence that such measures were taken. The platform carries a taxonomy of forty-one roles across seven functional groups, and a user assigned a role is enrolled in the curriculum tracks mapped to it within sixty seconds of assignment. Its deployment gate blocks go-live until every user assigned to an operational role on the system holds a valid, unexpired AI Literacy Credential, so an authority asking whether staff were trained before deployment receives an answer recorded by a system-enforced checkpoint rather than a claim made after the event.

Enforcement response capability map

Question an authority may ask	Platform capability	Evidence produced
What AI systems do you operate?	AI Intelligence Centre, portfolio register	Live register with risk tier, status and dates for every AISDP
How did you classify this system?	AI Regulatory Navigator	Saved assessment with inline citations, dated and attached to the system record
Is your technical documentation complete?	AI Intelligence Centre, AISDP	Structured documentation pack with section-labelled evidence bundle
What AI literacy measures have you taken?	AI Literacy Certification Platform	Article 4 report; append-only credential ledger
Were staff trained before deployment?	AI Literacy Certification Platform, deployment gate	Deployment readiness record confirming credential status at go-live
Has the system been monitored since deployment?	AI Intelligence Centre, version history	Immutable, timestamped change log with author and reason for every modification
Can you produce a submission package?	AI Intelligence Centre, documentation output engine	Signed ZIP archive with SHA-256 manifest, Annex documents and evidence bundle

Where to start, and what it costs

The enforcement architecture is now taking operational form. Most member states have notified a single point of contact, although many designations were still pending final adoption in September 2026; the AI Office is staffed and active; and we expect thematic surveillance to build up ahead of the 2 December 2027 application date for Annex III systems. For most organisations, what remains open is when enforcement will reach their sector and how well prepared they will be.

First: the inventory and the authority map. Inventory and classify every system with a documented rationale (section 8.1), and identify the authority for each system in each member state where it is placed on the market or used (sections 3 and 8.4). Check now the obligations that already apply: the Article 5 prohibitions, the Article 4 literacy measures and the Article 50 transparency duties (section 2).

Next: the documentation and the response protocol. Bring the technical documentation for every high-risk system to a complete, current and version-controlled state (section 8.2), prepare the enforcement response protocol and name the lead contact (section 8.6), and put cooperation obligations into supplier contracts (section 8.5).

Before each system's high-risk date: monitoring and incident reporting in operation. Post-market monitoring and serious incident reporting must work as processes by 2 December 2027 for Annex III systems and 2 August 2028 for Annex I systems (section 8.3).

Ongoing: keep it current. Update the documentation and the authority map as systems and designations change, follow the AI Board's outputs, and integrate the work into existing GDPR and sectoral governance (section 8.7).

What it costs. Most of the effort is the inventory, the documentation and the staff time to keep both current, and much of it can be shared with existing GDPR and sectoral compliance. Against it sit fines of up to EUR 15 million or 3% of turnover for most operator obligations (EUR 35 million or 7% for prohibited practices) and, for many organisations more seriously, the restriction, withdrawal or recall of a system the business depends on (section 7).

On timing. As at 11 October 2026, no fine under the AI Act had been confirmed by any regulator or official source. The high-risk obligations apply from 2 December 2027 (Annex III) and 2 August 2028 (Annex I), subject to Article 111(2), and the inventory and documentation they depend on take time to build.

The architecture's patchwork character creates real difficulty for organisations operating across several member states, and these steps are both the most effective and the most straightforward response to it. An organisation that has taken them can tell any authority that asks which systems it operates, how each was classified and why, which authority supervises it, and where the evidence is.

Abbreviations

Abbreviation	Meaning
AESIA	Agencia Española de Supervisión de la Inteligencia Artificial (Spanish Artificial Intelligence Supervision Agency)
AI	Artificial intelligence
AISDP	AI System Documentation Pack
AKOS	Agencija za komunikacijska omrežja in storitve (Slovenian Agency for Communication Networks and Services)
ANACOM	Autoridade Nacional de Comunicações (Portuguese communications regulator)
ANCOM	Autoritatea Națională pentru Administrare și Reglementare în Comunicații (Romanian communications regulator)
AP	Autoriteit Persoonsgegevens (Dutch Data Protection Authority)
BNetzA	Bundesnetzagentur (German Federal Network Agency)
CNIL	Commission nationale de l'informatique et des libertés (French data protection authority)
DPA	Data protection authority
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
GPAI	General-purpose AI
IDPC	Information and Data Protection Commissioner (Malta)
KI-MIG	KI-Marktüberwachungs-und-Innovationsförderungs-Gesetz (German AI market surveillance and innovation act)
KRiBSI	Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji (Polish Commission for the Development and Security of Artificial Intelligence)

Abbreviation	Meaning
MDIA	Malta Digital Innovation Authority
MNB	Magyar Nemzeti Bank (Central Bank of Hungary)
MSA	Market surveillance authority
PTS	Post- och telestyrelsen (Swedish Post and Telecom Authority)
RDI	Rijksinspectie Digitale Infrastructuur (Dutch Authority for Digital Infrastructure)
SPOC	Single point of contact

This paper is provided for information and is not legal advice. It describes the AI Act, as amended by Regulation (EU) 2026/1744, and national authority designations as publicly available at 11 October 2026; designations in particular may change. Take advice before making decisions on the obligations that apply to your own organisation and systems.

Basis and Standing

Binding law. AI Act (Regulation (EU) 2024/1689), as amended by Regulation (EU) 2026/1744 (the Digital Omnibus on AI, in force 27 July 2026): Articles 2(1), 3(47) to (49), 4, 5, 11, 18, 21, 25(4), 26(1) and (5), 28(1), 43(4), 50, 57(1), 65, 66, 70, 72 to 75 (Article 75(1) as replaced, and Articles 75a and 75c as inserted, by Regulation (EU) 2026/1744), 77, 79 to 83, 85, 88, 91, 92, 99, 101, 111 and 113, and Annex IV. Application dates are those in Article 113 as amended: 2 February 2025 for Chapters I and II (2 December 2026 for Article 5(1), points (ba) and (bb)); 2 August 2025 for Chapters V, VII and XII except Article 101; 2 August 2026 generally, including Article 101 and Chapter IX; 2 December 2027 (Annex III) and 2 August 2028 (Annex I) for Chapter III, Sections 1 to 3, subject to Article 111(2) as amended. Regulation (EU) 2019/1020, Article 14(4), applied by Article 74(1). National implementing measures as listed in Sources, as identified to 11 October 2026.

Official guidance and lists, not law. The Commission's list of single points of contact for market surveillance (last updated 7 September 2026), its page on market surveillance authorities (on complaints and possible infringement procedures) and its AI literacy Q&A (on national supervision of Article 4 from 2 August 2026 and the absence of a certificate requirement).

Our assessment, not law. The likely focus sectors, the investigation trigger risk matrix, the expectation of first substantive engagement after the high-risk dates, the view that documentation is likely to be an authority's first request and the main influence on an organisation's initial position, the persuasive weight of AI Board opinions, the risk of competitor complaints, the characterisation of Spain's structure and Irish activity, and the seven actions and staged path are our own analysis and recommendations. The documentation, cooperation and supply-chain actions reflect Articles 11, 18, 21, 25(4), 74(12), 83 and 99(7).

Secondary sources. Statements on France's draft designation and the February 2026 amendment, Belgium's status, Ireland's September 2025 announcement and Italy's

Legislative Decree No. 179/2026 rely on the secondary or official sources listed, as noted against each.

Enforcement position. As at 11 October 2026, no fine under the AI Act had been confirmed by any regulator or official source.

Sources

1. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
2. Regulation (EU) 2024/1689, consolidated text of 27 July 2026. https://eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27/eng
3. Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 (Digital Omnibus on AI; proposal COM(2025) 836 final, procedure 2025/0359(COD)), OJ L, 24.7.2026. https://eur-lex.europa.eu/eli/reg/2026/1744/oj
4. Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products, Article 14. https://eur-lex.europa.eu/eli/reg/2019/1020/oj/eng
5. European Commission, Market surveillance authorities under the AI Act (list of national single points of contact, last updated 7 September 2026; accessed 11 October 2026). https://digital-strategy.ec.europa.eu/en/policies/market-surveillance-authorities-under-ai-act
6. European Commission, AI Literacy: Questions and Answers. https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers
7. Denmark, Act No. 467 of 14 May 2025 (supplementary provisions to the AI Regulation). https://www.retsinformation.dk/eli/lta/2025/467
8. Italy, Law No. 132 of 23 September 2025, Gazzetta Ufficiale 25 September 2025. https://www.gazzettaufficiale.it/eli/id/2025/09/25/25G00143/sg
9. Italy, Legislative Decree No. 179 of 7 October 2026, Gazzetta Ufficiale No. 234 of 8 October 2026, as summarised by NicFab, “D.Lgs. 179/2026: autorità, sanzioni, sperimentazione e formazione”, 9 October 2026 (secondary source). https://www.nicfab.eu/it/posts/dlgs-179-2026-overview/
10. Spain, Royal Decree 729/2023 of 22 August 2023 (AESIA Statute). https://www.boe.es/buscar/act.php?id=BOE-A-2023-18911
11. Spain, La Moncloa, Council of Ministers, 26 May 2026: approval of the draft Organic Law for the proper use and governance of artificial intelligence. https://www.lamoncloa.gob.es/lang/en/gobierno/councilministers/paginas/2026/20260526-council-press-conference.aspx
12. Ireland, European Union (Artificial Intelligence) (Designation) Regulations 2025 (S.I. No. 366 of 2025). https://www.irishstatutebook.ie/eli/2025/si/366/made/en/print
13. Ireland, Regulation of Artificial Intelligence Act 2026 (Number 31 of 2026), 21 July 2026. https://www.irishstatutebook.ie/eli/2026/act/31/enacted/en/html

14. Law Society Gazette (Ireland), “Big news day for AI regulatory framework”, 18 September 2025 (secondary source). https://www.lawsociety.ie/gazette/top-stories/2025/september/big-news-day-for-ai-regulatory-framework/
15. Germany, Gesetz zur Durchführung der Verordnung über künstliche Intelligenz of 22 July 2026, BGBl. 2026 I Nr. 223 (28 July 2026), Article 1 (KI-MIG). https://www.recht.bund.de/eli/bund/bgbl-1/2026/223
16. Bundesnetzagentur, “Bundesnetzagentur’s AI Service Desk launched”, press release, 3 July 2025. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2025/20250703_KI_ServiceDesk.html
17. AI-Regulation (MIAI), “EU AI Act Implementation: France Still Without Designated National Competent Authorities”, 20 January 2026 (secondary source). https://ai-regulation.com/eu-ai-act-implementation-france-still-without-designated-national-competent-authorities/
18. Next, “Finalement, le gouvernement prévoit de donner la régulation de l’IA à la CNIL”, 13 February 2026 (secondary source; subscription access). https://next.ink/224252/finalement-le-gouvernement-prevoit-de-donner-la-regulation-de-lia-a-la-cnil/
19. Poland, Ministry of Digital Affairs, “Ustawa o systemach AI: bezpieczny rozwój sztucznej inteligencji w Polsce”, 27 July 2026. https://samorzad.gov.pl/web/gov/ustawa-o-systemach-ai---bezpieczny-rozwoj-sztucznej-inteligencji-w-polsce
20. Luxembourg, Bill No. 8476 implementing Regulation (EU) 2024/1689, Chamber of Deputies dossier (opinion document of 17 July 2026). https://wdocs-pub.chd.lu/docs/Dossiers_parlementaires/8476/20260717_Avis.pdf
21. VRT NWS, “Geen toezichthouder, wel al strengere regels” (Belgium’s AI Act supervisor), 2 August 2026 (secondary source). https://www.vrt.be/vrtnws/nl/2026/07/29/geen-toezichthouder-wel-al-strengere-regels-hoe-ver-staat-belg/
22. Hungary, Act LXXV of 2025 (2025. évi LXXV. törvény), Nemzeti Jogszabálytár; Government Decree 344/2025 (X. 31.). https://njt.jog.gov.hu/eli/TV/2025/75
23. Finland, Act 1377/2025 on the supervision of certain AI systems (Laki eräiden tekoälyjärjestelmien valvonnasta), in force 1 January 2026. https://www.finlex.fi/fi/lainsaadanto/saadoskokoelma/2025/1377
24. Lithuania, Law No. XV-106 of 14 January 2025 amending the Law on Information Society Services (consolidated text from 1 April 2025). https://e-seimas.lrs.lt/rs/actualedition/TAIS.277491/mEBznJakRX/
25. Latvia, Cabinet Regulation No. 478 of 12 August 2025 amending the Consumer Rights Protection Centre statute. https://likumi.lv/ta/id/362440
26. Greece, Law 5321/2026, as described by the Hellenic Data Protection Authority, press release of 18 August 2026. https://www.dpa.gr/en/enimerwtiko/press-releases/hellenic-dpa-takes-leading-role-implementing-eu-ai-act-greece
27. Romania, Chamber of Deputies written question No. 6258A of 14 September 2026 on AI Act implementation. https://www.cdep.ro/interpel/2026/i6258A.pdf
28. Lewis Silkin, “AI judgment day on the horizon while UK lawmakers play catch up”, 14 September 2026 (secondary source, on the absence of a UK AI bill). https://www.lewissilkin.com/insights/2026/09/14/ai-judgment-day-on-the-horizon-while-uk-lawmakers-play-catch-up

Provisions are cited by article in the text above.

Standard Intelligence

GET IN TOUCH

Reduce enforcement risk before contact.

EMAIL

hello@standardintelligence.com

WEB

standardintelligence.com

LOCATION

Manchester, United Kingdom

AI Use: AI tools were used in research, editorial review and drafting support. All sources were retrieved and checked against the published record by the author, who holds editorial responsibility for the contents and for the conclusions drawn. This disclosure is made voluntarily. To the extent the Article 50(4) obligation in Regulation (EU) 2024/1689 applies to this paper as text published to inform the public on matters of public interest, the exception for content that has undergone human review and for which a person holds editorial responsibility applies.

STANDARD INTELLIGENCE LIMITED · REGISTERED IN ENGLAND AND WALES · COMPANY NO. 16737890