

Where law meets innovation in technology

London

10th September 2026

Explore more

*Click the links for further information

Topics

Topic 1

[AI developments and emerging regulation](#)

Topic 2

[Technology investment, M&A and market trends](#)

Topic 3

[The impact of AI on businesses, workforces, and risk](#)

Topic 4

[AI Act enforcement and compliance considerations](#)

Product Launch – LexRay

AI Developments and Emerging Regulation

Click the email to get in touch:



Jaap Tempelman, Partner, Amsterdam
E: jaap.tempelman@simmons-simmons.com



Christopher Götz, Partner, Munich
E: christopher.goetz@simmons-simmons.com



Sophie Sheldon, Partner, London
E: sophie.sheldon@simmons-simmons.com



Edoardo Tedeschi, Partner, Milan
E: edoardo.tedeschi@simmons-simmons.com

Agenda

- The Digital Omnibus and current state of play
- Guidelines on High Risk AI Systems
- UK AI regulatory developments
- AI in M&A

Key Takeaways

- The Digital Omnibus on AI (Regulation (EU) 2026/1744) simplifies the AI Act, reduces regulatory burden, bans AI nudity applications, and pushes the high-risk obligations back to December 2027 for Annex III systems and August 2028 for Annex I systems.
- A provider of an AI system that qualifies by default as "high-risk" under the EU AI Act may, in certain circumstances, rely on the exception mechanism set out in Article 6(3) to bring the AI system outside the scope of high-risk classification. The European Commission's draft guidelines on high-risk classification, published in May 2026 and currently still in consultation, provide practical examples of when the filter may or may not apply; based on these examples, the Commission appears to interpret the conditions for applying the filter restrictively, suggesting that providers should not assume the filter will readily apply without careful analysis of the specific use case.
- The UK continues without an AI Act, relying instead on five sectoral regulators, with the ICO's statutory code on AI and automated decision-making and the rebuilt Article 22 rules under the DUA Act 2025 as the most consequential near-term changes.
- AI in M&A – Where a target develops, markets or uses AI systems, the buyer inherits regulatory exposure (EU AI Act – GDPR etc.). We set out a five stage methodology to identify a target's AI risk, providing worked examples in fintech, HR-tech and life sciences. We progress with (i) inventory and system mapping (ii) risk AI classification (iii) documentary verification by category (iv) quantifying exposure and (v) contractual allocation of risks under specific representations and warranties.

The Digital Omnibus and current state of play



Jaap Tempelman

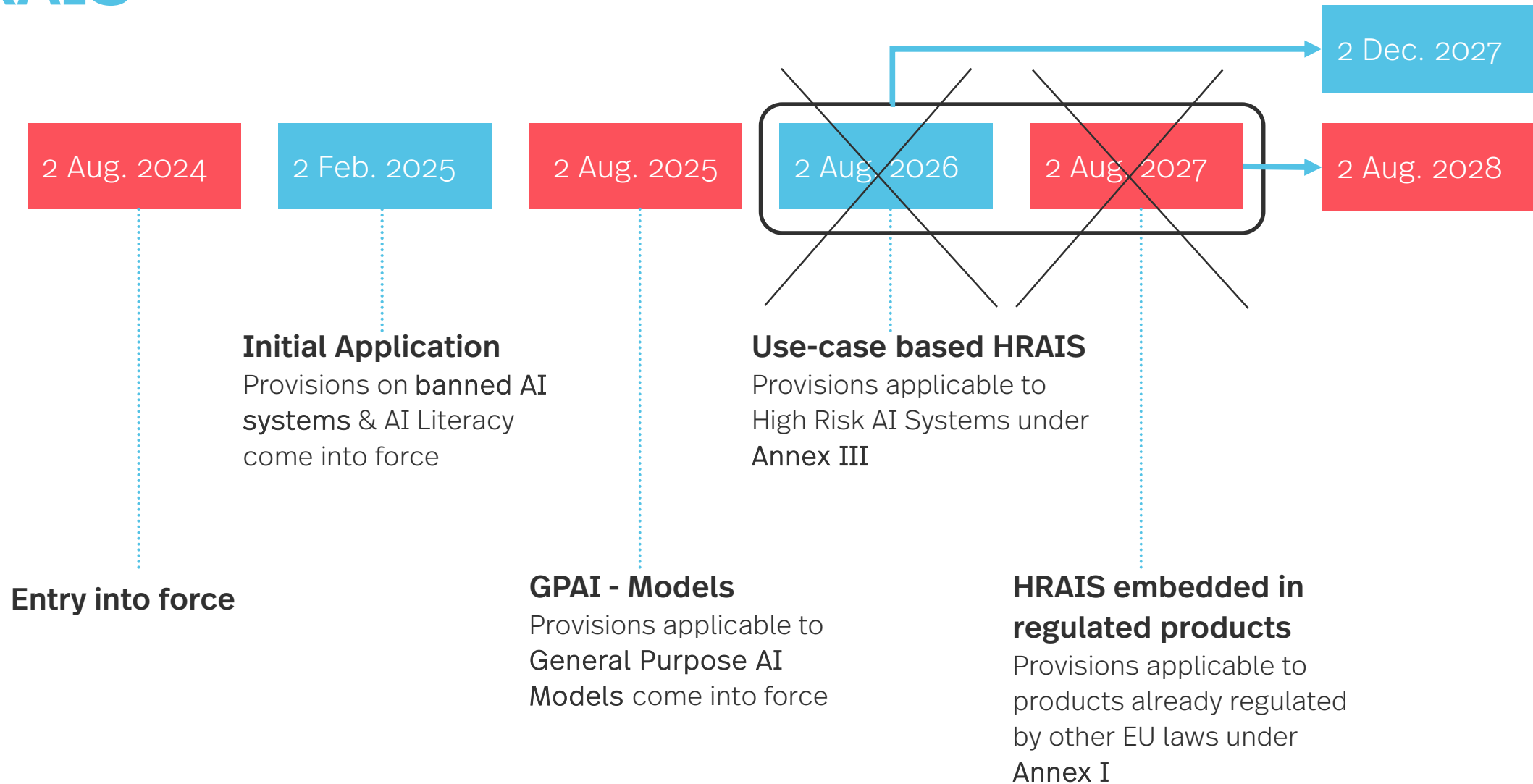
E: jaap.tempelman@simmons-simmons.com

Digital Omnibus - What and why?

- **Regulation (EU) 2026/1744** – prioritised regulation with targeted simplification measures of a technical nature to amend the AI Act.
- **Simplification:**
 - Simplify implementation and reduce regulatory burden without lowering the level of protection.
 - Part of the Commission’s “Simpler and Faster Europe” / Digital Omnibus package
- **Standards not ready** – harmonised standards, common specifications and guidance lagging behind the timetable.
- **National infrastructure incomplete** – delayed designation of competent authorities and conformity assessment (notified) bodies.

Delay: new implementation dates for HRAIS

§ New implementation dates



Some other material changes (I)

Grace period for (water)marking obligation (Art.50(2) and 111(4))

- Grace period until 2 December 2026 for systems placed on the market before 2 August 2026.

SME/SMC scope extension (Art. 1, 3, 17, 63, 95–96, 99)

- New "small mid-cap" definition. Existing SME simplifications – documentation, quality-management, penalties, support tools – extended to SMC enterprises.

Processing special category personal data for bias detection/correction (Art. 4a)

- Statutory exception extended to providers of non-high-risk systems and models, and to deployers.

Some other material changes (II)

New prohibition on nudity applications (Art. 5)

- Prohibition of AI systems that generate realistic images depicting nudity or sexual acts, including child sexual abuse material. Applies from 2 December 2026.

AI Literacy obligation softened (Art. 4)

- Open-ended staff-training mandate becomes a duty to "take measures to support" literacy, with Commission/Member State resources.

Overview Material Changes

Change	AI Act clause(s)	What changes
Postponed high-risk timelines	Art. 6, 113	High-risk rules (Ch. III, Secs 1–3) apply from 2 Dec 2027 (Annex III systems) and 2 Aug 2028 (Annex I products), not 2 Aug 2026/2027; clarified grace period for units already placed on the market.
SME/SMC scope extension	Art. 1, 3, 17, 63, 95–96, 99	New "small mid-cap" (SMC) definition; existing SME simplifications (documentation, quality management, penalties, support tools) extended to SMCs.
Narrowed "safety component" definition	Art. 3(14)	Only components whose intended purpose is to prevent/mitigate health-safety risk count, tightening the trigger for high-risk classification under Annex I products.
AI literacy softened	Art. 4	Direct staff-training obligation replaced by a duty on providers/deployers to "take measures to support" AI literacy, with Commission/Member State support.
New legal basis for bias-data processing	New Art. 4a (replaces Art. 10(5))	Extends the special-category personal data processing basis for bias detection/correction beyond high-risk providers to deployers and to providers/deployers of other AI systems and models.
Watermarking/marking grace period	Art. 50(2), 111(4), 113	Marking obligation for AI-generated synthetic content (Art. 50(2)) already applies generally from 2 August 2025; new Art. 111(4) grants providers whose systems were placed on the market before 2 August 2026 an extended compliance deadline of 2 December 2026.
Unified notified body designation	Art. 28–30, 43; new Annex XIV	Single application/assessment procedure for bodies seeking designation under both the AI Act and sectoral law (e.g. medical devices); new AI system classification codes.
Simplified EU database registration	Art. 49, Annex VIII	Streamlined/removed registration for Art. 6(3) systems assessed as not high-risk (e.g. narrow procedural tasks); assessment documentation still required.
Expanded sandboxes & real-world testing	Art. 57, 58, 60, new Art. 60a	EU-level AI regulatory sandbox (AI Office, from 2028); real-world testing extended to high-risk systems under Annex I product legislation, with safeguards.
Centralised AI Office oversight	Art. 75–77	AI Office gains exclusive competence over systems built on GPAI models by the same undertaking, and over systems embedded in/qualifying as VLOPs or VLOSEs under the DSA.
New prohibitions: deepfakes & CSAM	Art. 5	Explicit prohibition on AI systems generating/manipulating non-consensual intimate ("nudification") material and child sexual abuse material, applying from 2 December 2026, subject to defined safeguards and defences.
Machinery carve-out	Annex I (Section A→B); Reg. 2023/1230	Machinery Regulation moves from Section A to Section B of Annex I; AI Act's high-risk essential requirements to be integrated directly into the Machinery Regulation instead.
Reduced Commission implementing-act powers	Art. 50(7), 56(6), 69, 72(3)	Empowerments to adopt implementing acts on codes of practice, sandbox fees and post-market monitoring templates removed; replaced by guidance/voluntary templates.

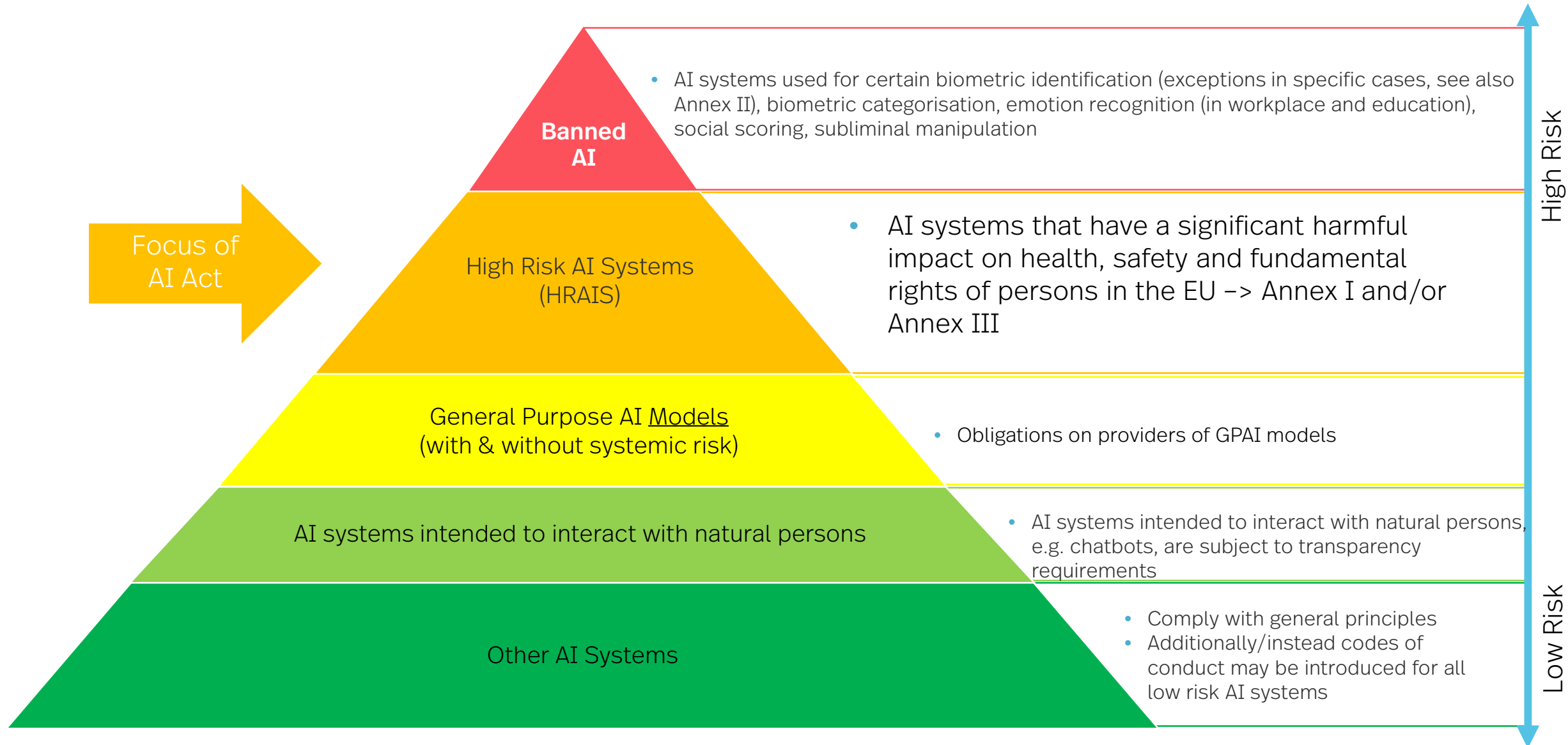
EU AI Act: Draft Guidelines on High-Risk AI Systems



Christopher Götz

E: christopher.goetz@simmons-simmons.com

EU AI Act: Risk-based approach



High-risk AI systems under Annex III

By default: any AI systems listed in Annex III

AI system e.g. intended to be used for:

1

Employment and workers' management (e.g.):

Recruitment and selection, including targeted job advertisements, analysis and filtering of applications and candidate evaluation; and decisions affecting work-related relationships, promotion or termination.

2

Critical infrastructure:

safety component in the management / operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity

3

Remote biometric identification (RBI):

identification of persons at a distance by comparing biometric data (e.g. facial images, voiceprints) against a reference database, without their active involvement; does not cover biometric verification whose sole purpose is to confirm that a person is who he or she claims to be

4

Access to essential private services and essential public services and benefits:

Creditworthiness checks, establishing credit scores, eligibility re healthcare services

Assessment of "intended purpose": Who's perspective & what to take into account when determining the purpose?

Draft High-Risk AI Guidelines

Status and Timeline

- **19 May 2026**
Draft Guidelines published for stakeholder consultation (167 pages)
- **(23 June 2026)**
Original consultation deadline
- **23 July 2026**
Extended deadline for stakeholder feedback
The deadline was extended by four weeks following requests from stakeholders.
- **By the end of 2026**
Final Guidelines expected by the Commission

CURRENT STATUS

Draft, non-binding and subject to revision following stakeholder feedback.

What do the Draft Guidelines cover?

GENERAL PRINCIPLES

- AI system definition
- Classification responsibility

ARTICLE 6(1) AND ANNEX I

- Products and safety components
- Third-party conformity assessment
- Interaction with EU product-safety legislation

ARTICLE 6(2) AND ANNEX III

- Eight Annex III areas and listed use cases
- Classification concepts
- How to determine the intended purpose
- Article 6(3) filter mechanism
- Practical classification examples



Focus: classification, not compliance

The Draft Guidelines explain whether an AI system is high-risk. They do not set out the detailed requirements applicable once a system has been classified as high-risk.

Provider's perspective: intended purpose

Does the provider's intended purpose encompass an Annex III use case?



YES

Falls within the Article 6(2) AI Act assessment.
Consider whether the Article 6(3) filter applies.



NO

Not high-risk under Article 6(2) AI Act.

How is the provider's intended purpose determined?

- Contractual arrangements and terms of service
- Instructions for use
- Technical documentation
- Promotional and sales materials
- Provider statements and overall product positioning

Key takeaway:

The provider's intended purpose must be determined holistically across all relevant materials.

A general disclaimer excluding high-risk uses is insufficient where the provider's overall presentation, examples or product positioning provides for or promotes such uses.

High Risk AI System

Exception (“Filter”)

“AI system does not pose a significant risk of harm to health, safety or fundamental rights of persons”

Art. 6 (3) EU AI Act



High Risk AI System – Annex III

Filter: Significant risk of harm?

AI system does not lead to significant risk of harm in case

It does not materially influence the decision-making (*Recital 53*)

- ❑ AI system is used to detect duplicates among a large number of application
- ❑ task performed by AI system is *intended to improve the result of a previously completed human activity*
- ❑ AI system is *intended to perform a task that is only preparatory or narrow procedural task*

Draft High-Risk AI Guidelines

Status and Timeline

- **19 May 2026**
Draft Guidelines published for stakeholder consultation (167 pages)
- **(23 June 2026)**
Original consultation deadline
- **23 July 2026**
Extended deadline for stakeholder feedback
The deadline was extended by four weeks following requests from stakeholders.
- **By the end of 2026**
Final Guidelines expected by the Commission

CURRENT STATUS

Draft, non-binding and subject to revision following stakeholder feedback.

What do the Draft Guidelines cover?

GENERAL PRINCIPLES

- AI system definition
- Classification responsibility

ARTICLE 6(1) AND ANNEX I

- Products and safety components
- Third-party conformity assessment
- Interaction with EU product-safety legislation

ARTICLE 6(2) AND ANNEX III

- Eight Annex III areas and listed use cases
- Classification concepts
- Provider-defined intended purpose
- Article 6(3) filter mechanism
- Practical classification examples



Focus: classification, not compliance

The Draft Guidelines explain whether an AI system is high-risk. They do not set out the detailed requirements applicable once a system has been classified as high-risk.

Article 6(3) filter in practice

When can the filter conditions in Article 6(3)(a)–(d) be relied on?

Selected examples from and based on the European Commission's Draft Guidelines on high-risk classification

Filter applies → Not high-risk

Example: Recruitment – duplicate application detection

The system identifies and flags duplicate applications without ranking, scoring or evaluating candidates.

Why: Narrow procedural task that does not materially influence the recruitment decision (Art. 6(3)(a)).

Example: Education – admission process

The system categorises applications into predefined categories, such as education level or grade, without evaluating applicants' suitability or making admission decisions.

Why: Narrow procedural task – the system **does not materially influence** the decision-making (Art. 6(3)(a), Recital 53).

Filter does not apply → High-risk AI system

Example: Recruitment – candidate shortlisting

The system produces **scores, rankings** (e.g. 'top 5 candidates') and/or fit categories to shortlist candidates. **Recruiters may review or override the recommendations, but the rankings and scores are a primary input for the decision.**

Why: The system **materially influences** the decision – it could lead to low ranking or exclusion of candidates of a certain gender or with disabilities → high-risk under Annex III, point 4(a).

Example: Employment – performance evaluation

The system generates performance scores, ranks employees against peers and suggests ratings used for compensation or other employment-related decisions.

Why: The system materially influences decisions affecting workers; the Art. 6(3) filter does not apply → high-risk under Annex III, point 4(b).

Always high-risk: The Article 6(3) filter cannot be relied on where the AI system performs profiling of natural persons. Article 6(3), third subparagraph, EU AI Act

Checklist: key obligations for providers and deployers of high-risk AI systems

Common Foundation

AI literacy

Ensure a sufficient level of AI literacy among staff and persons dealing with AI systems.

Provider

Design, compliance and market access

- ☐ Risk management and data governance
- ☐ Technical documentation and logging
- ☐ Transparency and instructions for use
- ☐ Human oversight, accuracy, robustness and cybersecurity
- ☐ Quality management and conformity assessment
- ☐ CE marking, registration and corrective actions

Deployer

Responsible operation and use

- ☐ Use in accordance with instructions
- ☐ Human oversight
- ☐ Relevant and representative input data
- ☐ Monitoring, incidents and suspension of use
- ☐ Log retention
- ☐ Applicable impact, information and cooperation duties

Providers focus on building and placing compliant systems on the market; deployers focus on responsible use and oversight.

UK AI regulatory developments



Sophie Sheldon

E: sophie.sheldon@simmons-simmons.com

UK approach: five regimes, no AI Act

1

No standalone AI statute – yet

- Sectoral, pro-innovation approach persists
- Regulating for Growth Bill (announced King's Speech, May '26): sandbox powers across regulators
- Question: does this change the "no AI Act" calculus?

2

DUA Act 2025: Art. 22 rebuilt

- Arts 22A–22D replace UK GDPR Art. 22 (in force 5 Feb '26)
- “Prohibited unless” → “permitted provided” safeguards
- Info, representations, human intervention, contest (Art. 22C)

3

ICO statutory AI/ADM Code

- SI 2026/425; in force 12 May '26
- ICO Code on AI + ADM, incl. children's data
- Most consequential near-term development for practitioners

4

DRCF: five regimes, not one

- ICO, CMA, FCA, Ofcom each carving out AI positions
- No single AI regulator; overlapping remits
- Practical challenge: advise across regimes simultaneously

5

AI Growth Lab / sandboxes

- Rapid, temporary “targeted regulatory modification”
- Test products under relaxed rules; safeguards retained
- Requires primary legislation – not yet in force

AI in M&A

(target side risks and DD tests)



Edoardo Tedeschi

E: edoardo.tedeschi@simmons-simmons.com

Artificial intelligence in M&A: target-side risk and AI in due diligence and SPA

I. Target – Side Risk

Where a target develops, markets or uses AI systems, the buyer inherits regulatory exposure under Regulation (EU) 2024/1689 (AI Act) and Regulation (EU) 2016/679 (GDPR): mapping, classification, quantification, contractual allocation.

II. AI as a Due Diligence Tool

AI can be deployed directly by the buyer and its advisers to make due diligence and execution of the transaction faster, broader and more defensible, subject to appropriate governance safeguards.

AI ACT – REG. (EU) 2024/1689
(Artificial Intelligence Act)

GDPR – REG. (EU) 2016/679
(General Data Protection Regulation)

DIGITAL OMNIBUS ON AI – R
EG. (EU) 2026/1744

Identifying a target's AI risk: a five-stage methodology

- 1. Inventory and system mapping** – AI systems developed/used by the target; provider/deployer role; date first placed on the market or put into service.
- 2. Risk classification** – prohibited practice, high-risk, transparency-only, or GPAI model, cross-checked against overlapping sector-specific legislation. Under the Digital Omnibus on AI (Regulation (EU) 2026/1744, in force from 27 July 2026), the high-risk rules in Chapter III, Sections 1–3, now apply from **2 December 2027** for systems classified as high-risk under Article 6(2)/Annex III, and from **2 August 2028** for systems classified as high-risk under Article 6(1)/Annex I.
- 3. Targeted documentary verification** – technical documentation, conformity assessment, risk management and human oversight for high-risk systems, benchmarked against the postponed application dates; providers of AI systems generating synthetic content already on the market before 2 August 2026 have a transitional period to 2 December 2026 to comply with Article 50(2) marking obligation. The postponed new dates are not expressed as conditional on future standards-readiness milestones; the Digital Omnibus on AI recitals nonetheless note the continuing importance of timely guidance and harmonised standards to support compliance, which should be monitored as implementation progresses.
- 4. Quantifying exposure** – fines of up to € 35 million or 7% of worldwide turnover for prohibited practices (Art. 5, Art. 99(3)), and up to € 15 million or 3% for breaches of high-risk and Art. 50 obligations (Art. 99(4)), remediation costs and reputational/commercial risk, with remediation timelines tested against the revised statutory deadlines.
- 5. Contractual allocation of residual risk** – dedicated representations and warranties with indemnity, a remediation condition precedent, a price adjustment or reinforced escrow, or deal restructuring, with verification milestones tied to the dates above.

R&W must not stand down on Art. 50 AI Act on transparency obligations (as amended by the Digital Omnibus on AI): a target that has paused compliance work on these obligations may face exposure in the 3% penalty tier, subject to verifying the system's specific classification and grace-period status.

Worked examples: applying the methodology by sector

Fintech

AI-Drive Credit Scoring

High-risk under Annex III, point 5(b). Check DORA/CRD IV governance if the target is a credit institution. Remediation typically 3-6 months, to be completed well ahead of the 2 December 2027 application date applicable to Annex III systems.

→ Indemnity + escrow with milestones

HR-Tech

Personnel Selection Tool

High-risk under Annex III, point 4, for both provider and deployer configurations. Profiling of natural persons is relevant to the classification, including by disapplying the Article 6(3) exception for systems that would otherwise not be considered high-risk. Focus: human oversight and fundamental rights impact assessment.

→ DD intensity calibrated to role

Life Sciences

AI in Clinical Trials

High-risk if a safety component of a device under Regulations (EU) 2017/745/746 (Annex I, Section A), with the 2 August 2028 application date as the relevant benchmark. Health data under Article 9 GDPR: lawful basis and the new Article 4a AI Act on bias detection (inserted by the Digital Omnibus on AI, Regulation (EU) 2026/1744).

→ Earn-out on regulatory milestones

Third-Party GPAI

Target Build on a Third-Party Model (API)

Substantial fine-tuning may make the target a "provider" for the modified component. DD focus on the contract with the model provider (indemnities, limitations, Chapter V AI Act transparency commitments).

→ Stand-alone warranty from the target

Deploying AI in due diligence tools (and for the SPA): lines of action and safeguards

1. Data Room Review & Red Flag Reporting

AI-assisted first-pass triage across the entire data room; full human review reserved for high-risk/material documents. Contractual safeguards: no reuse of data for training, deletion after completion, allocated liability for material errors.

2. Valuation & Synergy Modelling

AI output treated as an input to the financial model, never as a substitute for professional judgment. Systematic documentation of human review and of any departure from AI-generated projections, for defensive due diligence on price disputes.

3. Document Automation & Negotiation Support

AI for first drafts and automated redlining; full legal review of every economically or legally material clause (price, indemnities, conditions precedent, governing law). Internal negotiation playbook for the AI to reference.

4. Monitoring Conditions Precedent & Post-Signing

AI as an alerting layer on deadlines, conditions precedent and covenants between signing and closing; register of conditions maintained and validated by the legal team; mandatory human sign-off before any AI-generated communication to counterparties/authorities.

Strategy for the SPA: stress testing of all R&W by using AI tools

Technology investment, M&A and market trends

Click the email to get in touch:



Micheál Mulvey, Partner, Dublin
E: micheal.mulvey@simmons-simmons.com



Frances Doherty, Partner, London
E: frances.doherty@simmons-simmons.com



Luke Christoforidis
External speaker



John Spindler
External speaker

Agenda

- The trends shaping AI-related investments and M&A activity
- Assess whether current valuations are justified
- Today's market – sustainable opportunity or an investment bubble?



Key takeaways

- We heard where Barclays Innovation Bank and Twin Path Partners are seeking to put their money as we got an overview of the market and where investors are seeing most activity.
- Commentary on current valuations:
 - AI is a fundamental technological/structural shift that will drive second order effects.
 - Balance needs to be struck between technology value and commercial execution.
 - Increasing valuations are driving the time frame for deal execution.
- There is a need for great academic research and funding in the UK to drive innovation and develop talent in the field of AI.
- M&A execution and practical realities:
 - AI has changed due diligence and deal execution.
 - AI-specific issues are now appearing in diligence and the related risks need to be appropriately managed to protect investors.

Coffee Break – 15 minutes



Impact of AI on businesses, workforces & risk management

Click the email to get in touch:



Mandy Perry, Partner, London
E: mandy.perry@simmons-simmons.com



Lauren Dickinson, Managing Associate, London
E: lauren.dickinson@simmons-simmons.com

Agenda

- The use of AI in employment and how this can be managed
- Managing unintended consequences of AI in the employment relationship
- AI and its use in HR systems



Key takeaways

- Employment relationships are one of the most heavily controlled and regulated areas of business in most countries.
- Some key considerations that should be taken into account when adopting AI in HR tools include:
 - EU AI Act
 - Data protection
 - Employment law (the biggest risk being the threat of discrimination claims)
 - Works councils (particularly in European jurisdictions)
 - DSARs and disclosure in litigation, as AI systems create more documents that need to be disclosed in data subject access requests and DSARs
 - AI note-takers
- Carry out cross-practice risk assessments for new AI in HR tools.
- Employee use of AI has led to a rise in grievances and complaints, as well as a rise of claims at tribunal.
- Clear policies on AI use at work are strongly recommended.

Enforcement of the EU AI Act

Click the email to get in touch:



Minesh Tanna, Partner, London
E: minesh.tanna@simmons-simmons.com



Alejandro Guerrero, Partner, Brussels
E: alejandro.guerrero@simmons-simmons.com



Laura Cortes Lopez, Associate, Brussels
E: laura.corteslopez@simmons-simmons.com

Agenda

- Background to the AIA & Enforcement
- AI Act Interplay with the DSA and GDPR
- Transparency Obligations
- Prohibited AI
- What should organisations be doing now?



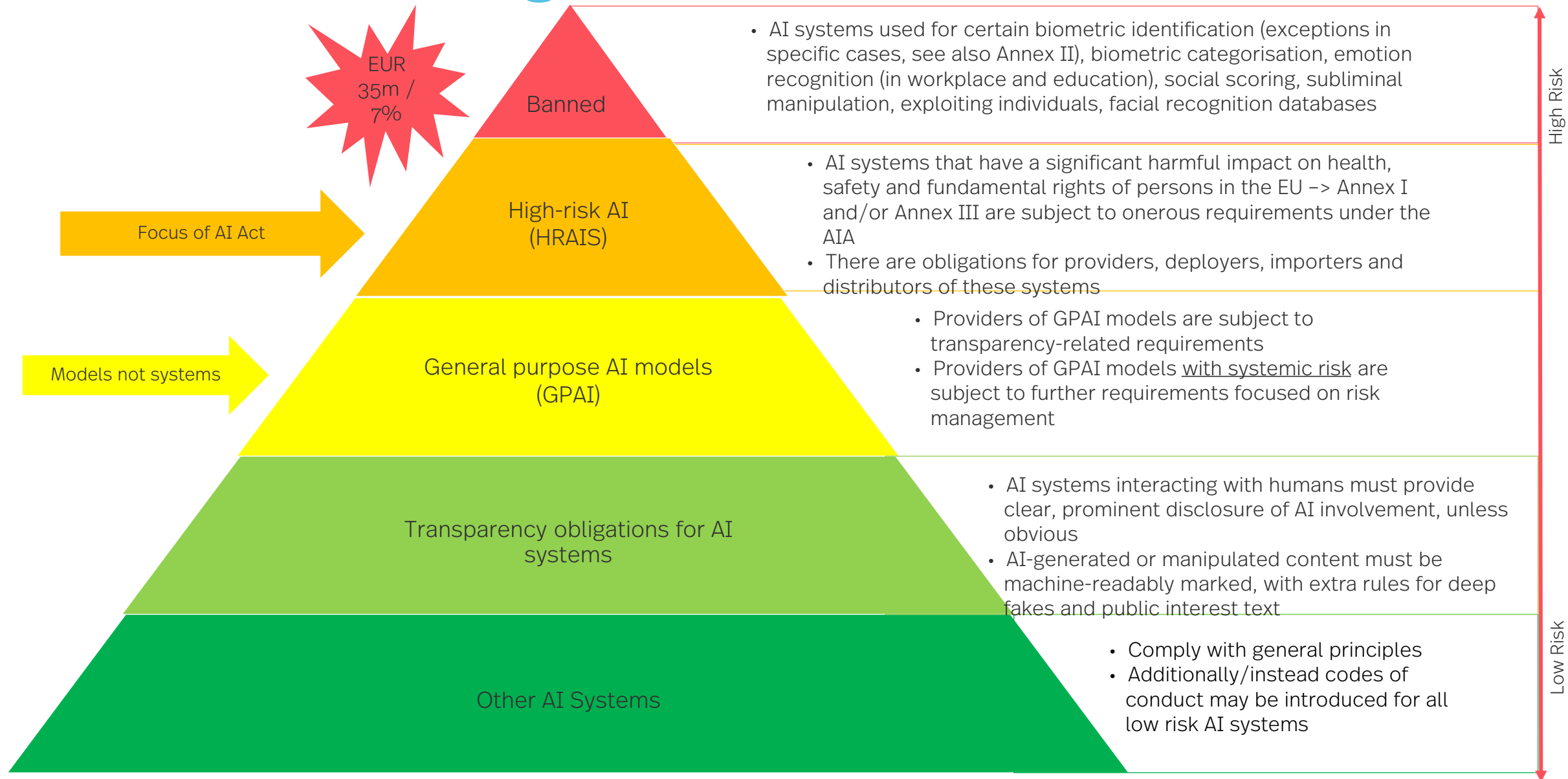
Key Takeaways

- The prohibitions are already live. They have applied since 2 February 2025, so manipulative interfaces, social scoring and untargeted facial-image scraping are present-tense exposure at the EUR 35 million / 7% band – not a 2026 planning item. The newly added CSAM and NCII prohibition follows on 2 December 2026.
- Enforcement capacity is uneven, and that cuts both ways. Roughly half of Member States have designated a market surveillance authority; others are only at proposal stage. Where MSAs do exist, they can run inspections and dawn raids and order withdrawal or recall – and a single state may host many of them, with 13 in Ireland alone.
- GPAI is regulated at model level. The AI Office has dedicated supervisory and enforcement powers in relation to general-purpose AI models, including evaluations and access via "appropriate technical means and tools, including source code," with fines up to €15 million or 3% falling on the provider rather than the undertaking.
- Transparency duties split between provider and deployer. Providers must build the technical capabilities that enable transparency, while deployers must ensure the required disclosures are made in the real-world context of use.
- Your GDPR and DSA work is a running start. Fundamental rights assessments can build on existing DPIAs, and Article 22 controls map closely onto the Act's human oversight requirements.

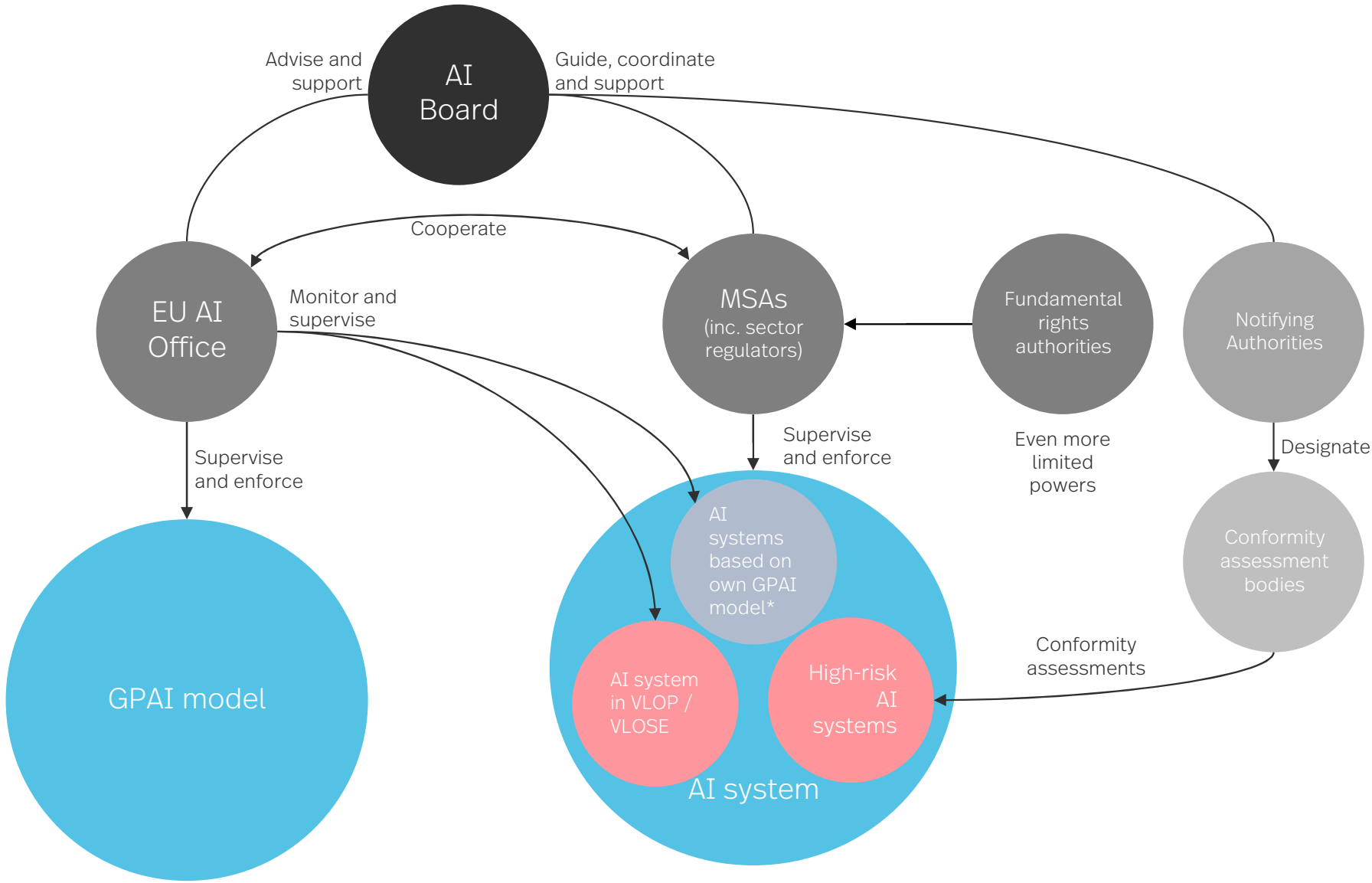
Background & Enforcement



EU AI Act – Background



Regulatory landscape



*Except where AI system is in the following categories:

- Critical infrastructure
- Law enforcement
- Border management
- Financial institutions
- Justice / democratic process
- Annex I

Market Surveillance Authorities

- HRAIs and transparency obligations will mainly be enforced by MSAs
- There may be multiple MSAs in each Member State (e.g. 13 in Ireland)
- MSAs have a wide range of regulatory powers, including:
 - Requests for information / access
 - Withdrawal, restriction or recall
 - Inspections, dawn raids, etc.
 - Fines of up to 7% worldwide turnover

Jurisdiction	MSA?	Jurisdiction	MSA?
Austria	No	Italy	Designated
Belgium	Proposed	Latvia	Designated
Bulgaria	No	Lithuania	Designated
Croatia	No	Luxembourg	Proposed
Cyprus	Designated	Malta	Designated
Czech Republic	Proposed	Netherlands	Proposed
Denmark	Designated	Poland	Designated
Estonia	No	Portugal	Proposed
Finland	Designated	Romania	Proposed
France	Proposed	Slovakia	Proposed
Germany	Designated	Slovenia	Designated
Greece	Designated	Spain	Proposed
Hungary	Designated	Sweden	Designated
Ireland	Designated		

Powers to investigate

- Request information and documentation regarding GPAI models
- Conduct evaluations of GPAI models to assess compliance or investigate systemic risk
- Request access to the GPAI model via *“appropriate technical means and tools, including source code”*

Power to request measures

- Request *“appropriate measures”* to comply with Arts. 53 - 54
- Request mitigation of systemic risks
- Restrict making available on the market, withdraw or recall a GPAI model

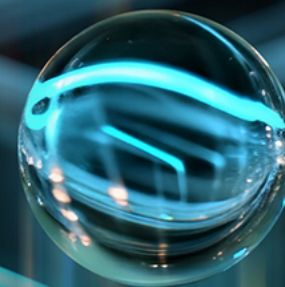
Power to impose fines

- Impose administrative fines of up to €15 million or 3% of the provider’s worldwide annual turnover for GPAI models
- Fines apply to the provider, rather than the undertaking (as for AI systems)

Powers in respect of AI systems falling within its competence

- Increased coordination: MSA & AIO
- All MSA powers for AI systems (investigatory + corrective)
- New safeguards + info provided to operators
- Local law (e.g. judicial oversight)
- Binding ‘commitments’ by operators
- Clearer procedure for non-compliance decisions

AI Act Interplay with the DSA and GDPR



Three complementary EU regulatory frameworks

DIGITAL SERVICES ACT



Online safety and trust

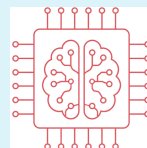
REGULATORY OBJECT

Intermediary services, including hosting services, online platforms and VLOPs/VLOSEs

PRIMARY AUTHORITIES

European Commission for VLOP/VLOSE-specific obligations; national Digital Services Coordinators for other intermediary services.

AI ACT



AI safety and fundamental rights

REGULATORY OBJECT

AI systems and general-purpose AI models across the AI value chain

PRIMARY AUTHORITIES

AI Office for GPAI and matters allocated to it; national market-surveillance authorities for other AI Act obligations

GDPR



Protection of personal data

REGULATORY OBJECT

Processing of personal data by controllers and processors

PRIMARY AUTHORITIES

National supervisory authorities; lead supervisory authority and EDPB consistency mechanism for cross-border processing

Interplay between the DSA and the AI Act

DSA

Systemic-risk frameworks

Large platforms must find and reduce the systemic risks their service creates, algorithms included.

Arts. 34–35 DSA

Synthetic-content risks

Platforms must manage deepfake risks and report how they moderate that content.

Arts. 15 and 34–35 DSA

Content moderation

Platforms must explain moderation rules and tools, and let users flag illegal content.

Arts. 14–16 DSA

Online advertising

No ad targeting on sensitive data, and no profiling of minors for advertising.

Arts. 26(3) and 28(2) DSA

Interfaces & recommenders

Interfaces must not mislead users, and platforms must explain what drives the feed.

Arts. 25, 27 and 28(1) DSA

AI ACT

Risk management

The AI Act requires risk management for high-risk AI systems and it also requires systemic-risk assessment and mitigation for GPAI models with systemic risks.

Arts. 9 and 55 AI Act

Synthetic-content marking

Imposes marking and labelling obligations on providers and deployers of certain AI systems to facilitate the identification and disclosure of synthetic and deepfake.

Art. 50 AI Act · Recital 136

AI used for moderation

The moderation tool must not be a banned practice, and faces stricter rules if high-risk.

Art. 5 and Arts. 9–15 AI Act

AI used for advertising

The ad system cannot sort people by biometrics or exploit their vulnerabilities.

Art. 5(1)(b) and (g) AI Act

AI shaping interfaces & feeds

Manipulative techniques are banned: the DSA looks at what users see, the AI Act at the system.

Art. 5(1)(a)–(b) AI Act

Interplay between the GDPR and the AI Act

GDPR

Lawful and minimal use of data

Any personal data used needs a legal basis, a clear purpose and no more data than necessary.

Arts. 5, 6, 9 and 25 GDPR

Impact assessment

High-risk processing must be assessed before it starts.

Art. 35 GDPR

Information and access

People must be told clearly how their data is used and be able to access it.

Arts. 12–15 GDPR

Automated decisions

GDPR Article 22 provides data subjects with the right not to be subject to a decision based solely on automated processing

Art. 22 GDPR

Independent supervision

Data protection authorities enforce the GDPR, and coordinate on cross-border cases.

Arts. 51–58 and 60–65 GDPR

AI ACT

Data governance

Training and testing datasets must be relevant, representative and properly governed.

Art. 10 AI Act

Rights assessment

Some deployers must assess the impact on fundamental rights, which can build on the privacy assessment.

Arts. 26(9) and 27 AI Act

Transparency

Users must be told how the AI system works and, in some cases, its role in a decision.

Arts. 13, 26(11) and 86 AI Act

Human oversight

High-risk systems must be built so a person can genuinely oversee and use them properly.

Arts. 14 and 26 AI Act

Regulatory cooperation

Those same authorities may join sandboxes and supervise certain AI systems.

Arts. 57(10), 59 and 74(8)–(10) AI Act

Transparency Obligations



Transparency Obligations: What Is Required in Practice?

§ Transparency

DEVELOPER / PROVIDER



Direct interaction with individuals

Inform people that they are interacting with an AI system, unless this is obvious in the circumstances.



Synthetic content marking

Mark AI-generated or manipulated text, audio, image and video outputs in a machine-readable and detectable format.



Technical standard

Use solutions that are effective, interoperable, robust and reliable, to the extent technically feasible.

USER / DEPLOYER



Deepfakes

Disclose when image, audio or video content constituting a deepfake has been artificially generated or manipulated.



Public-interest text

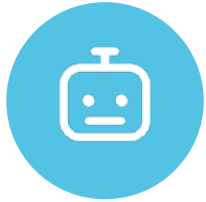
Disclose AI-generated or manipulated text published to inform the public, subject to the human review and editorial responsibility exception.



Emotion recognition / biometric categorisation

Inform individuals exposed to the operation of the system and comply with applicable data protection rules.

Transparency Obligations: Examples



Customer-facing chatbot

A company integrates a third-party chatbot into its customer service channel.

PROVIDER Design the system to inform users that they are interacting with AI, unless obvious.

DEPLOYER Ensure the notice is actually presented at the first interaction.



Synthetic marketing campaign

A marketing team creates an advertisement using AI-manipulated images of a celebrity.

PROVIDER Ensure AI-generated images are marked in a machine-readable and detectable manner.

DEPLOYER Add a user-facing disclosure where the published content **qualifies as a deepfake**.



Public-interest article

A company uses generative AI to publish text informing the public on a public-interest matter.

PROVIDER Ensure generated text is technically marked.

DEPLOYER Disclose AI generation unless human review or editorial control applies and editorial responsibility is assumed.



Authorities may require corrective action, restrict or prohibit use, or order withdrawal or recall; fines may also apply. In practice, prior regulatory engagement may be more likely, depending on the seriousness and circumstances, including whether the issue is isolated or reflects repeated conduct.

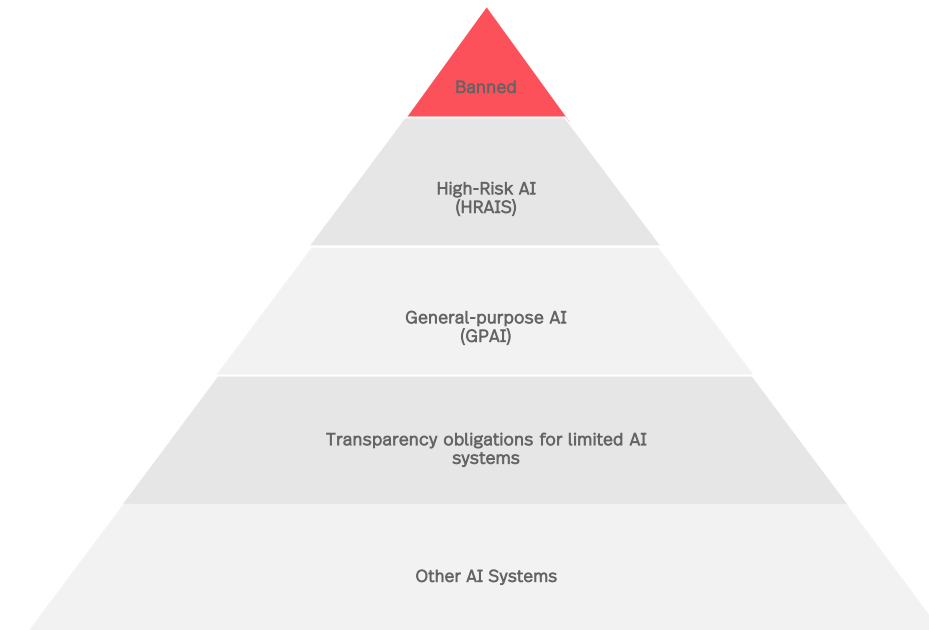
Prohibited AI



Prohibited AI

- Using [subliminal](#), [manipulative](#) or [deceptive](#) techniques, or [exploiting vulnerabilities](#) (with 'significant harm' test)
- Using protected characteristics/attributes to infer or categorise according to sensitive characteristics ([Biometric Categorisation Systems](#))
- Evaluating or classifying persons based on social behaviour or personality characteristics
- Predicting [criminal risk](#) based solely on profiling/personality traits
- Creating or expanding [facial recognition](#) databases using non-targeted scraping
- Using of 'real-time' [remote biometric identification](#) in public spaces by law enforcement
- Inferring emotions in the workplace/education setting ([emotion recognition software](#))
- Recently added: Generating/manipulating child sexual abuse material (CSAM) or non-consensual intimate images (NCII)

Prohibitions have been in force since 2 February 2025 (excl. CSAM/NCII which apply from 2 Dec 2026)



Prohibited AI: Examples and Potential Consequences



Manipulative AI interface

An online platform uses AI to identify moments when vulnerable users are most susceptible to pressure and deliberately prompts them to make purchases or continue gambling.

PROHIBITED PRACTICE

Using subliminal, purposefully manipulative or deceptive techniques where the statutory harm threshold is met.



Social scoring

An organisation evaluates individuals over time using social behaviour or inferred personality characteristics and uses the score in unrelated contexts.

PROHIBITED PRACTICE

Social scoring that results in unjustified, disproportionate or contextually unrelated detrimental treatment.



Facial recognition database

A company creates or expands a facial recognition database through untargeted scraping of facial images from the internet or CCTV footage.

PROHIBITED PRACTICE

Untargeted scraping of facial images to create or expand facial recognition databases.

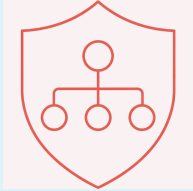


Authorities may prohibit the practice, restrict the system, or order withdrawal or recall. Fines may reach EUR 35 million or 7% of worldwide annual turnover. Given the seriousness of prohibited practices, coercive measures are more likely than prior engagement.

What should organisations be doing now?



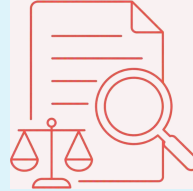
What should organisations be doing now?



01

Governance and accountability

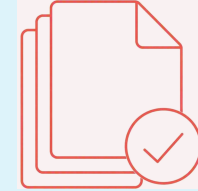
Implement appropriate governance, risk management and accountability mechanisms.



02

Informed decision-making

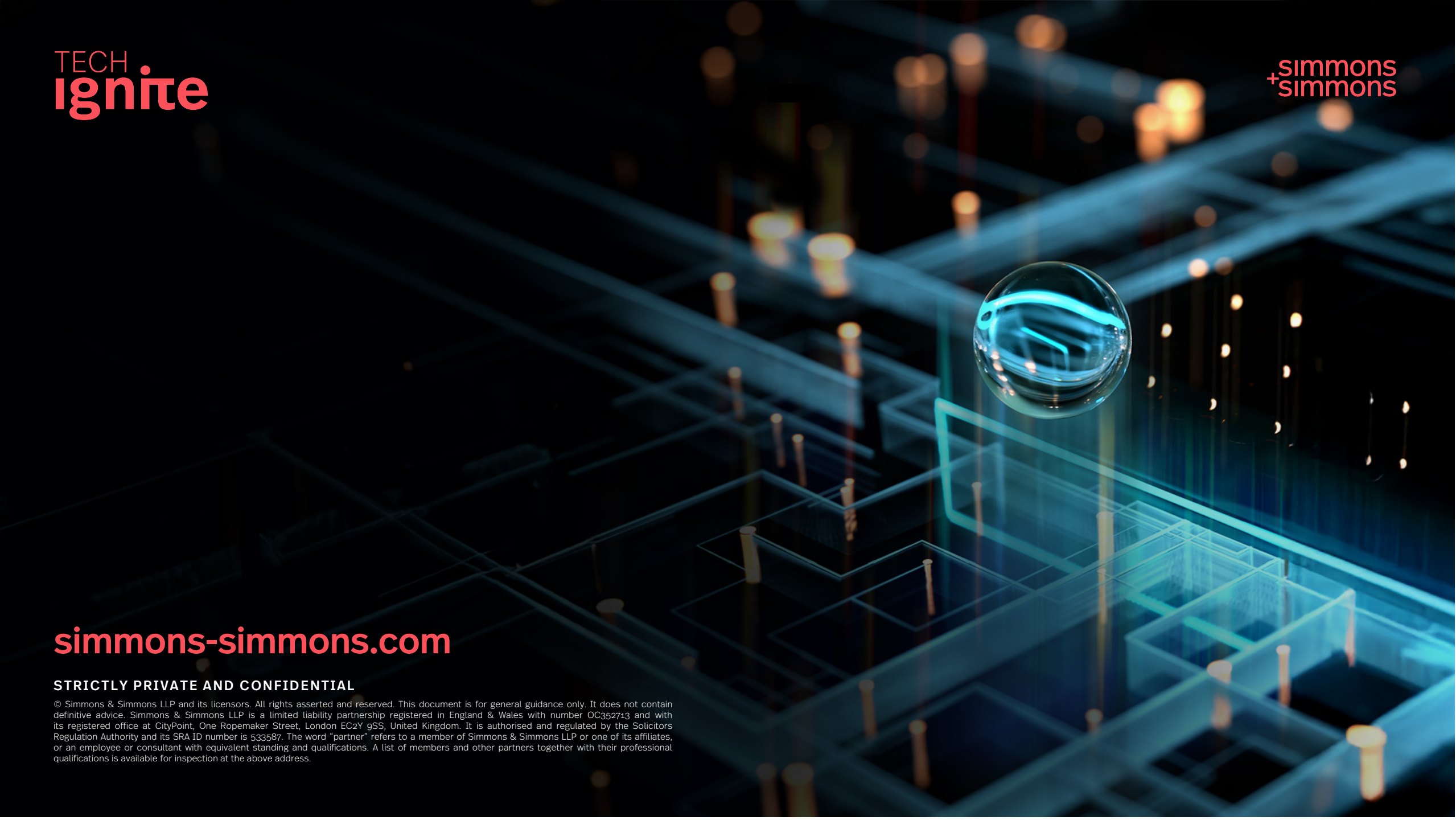
Ensure that key decisions are based on accurate information and supported by documented legal analysis.



03

Auditable records

Maintain a complete and auditable record of decisions, supporting evidence and compliance measures.



TECH
ignite

+simmons
simmons

simmons-simmons.com

STRICTLY PRIVATE AND CONFIDENTIAL

© Simmons & Simmons LLP and its licensors. All rights asserted and reserved. This document is for general guidance only. It does not contain definitive advice. Simmons & Simmons LLP is a limited liability partnership registered in England & Wales with number OC352713 and with its registered office at CityPoint, One Ropemaker Street, London EC2Y 9SS, United Kingdom. It is authorised and regulated by the Solicitors Regulation Authority and its SRA ID number is 533587. The word "partner" refers to a member of Simmons & Simmons LLP or one of its affiliates, or an employee or consultant with equivalent standing and qualifications. A list of members and other partners together with their professional qualifications is available for inspection at the above address.