A COMPARISON OF AI REGULATORY FRAMEWORKS

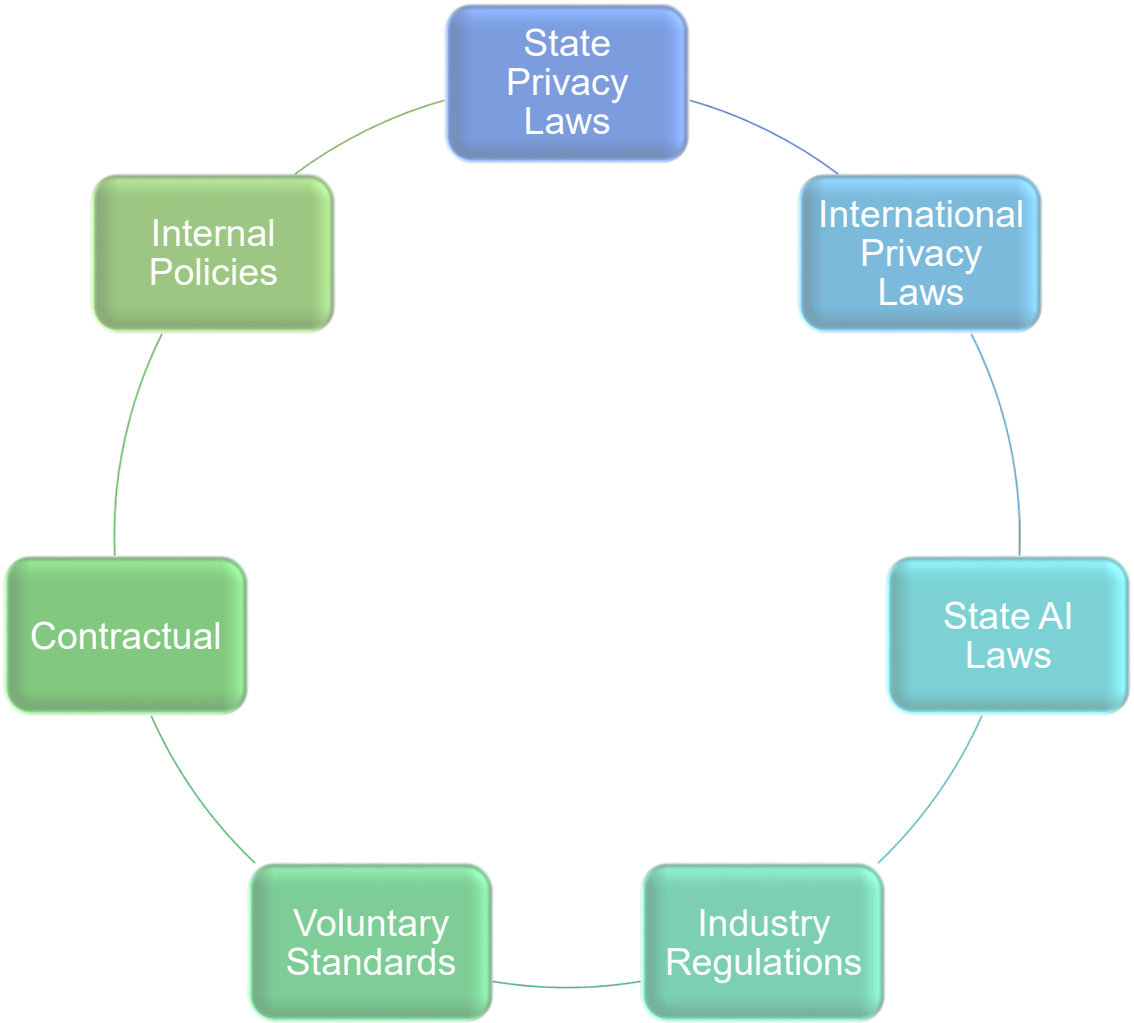
Paolo Sbuttoni
Paolo.sbuttoni@footanstey.com

Greg Szewczyk
szewczykg@ballardspahr.com

FootAnstey

Ballard Spahr LLP

POTENTIAL SOURCES OF AI OBLIGATIONS



THE EU AND UK APPROACHES

The EU AI Act 2024 (Regulation 2024/1689)

Comes into force on 1 August 2024

What is being regulated?

- "A machine-based system designed to operate with varying levels of autonomy"; and
- "The system adapts after deployment and infers from the input it receives how to generate outputs. "

Scope and Application

- Providers (developers), deployers, distributors and importers.
- Providers based outside EU where (i) the system is available on the EU market, or (ii) the output generated is used in the EU.
- Non-EU providers of GPAI models and high-risk AI systems are required to appoint an AI representative in the EU.

Risk Classification

- Unacceptable Risk (Prohibited)/High Risk/Limited Risk/Minimal Risk
- General Purpose AI

Penalties

- Fines of up to EUR35m or 7% of global annual turnover.

Navigating the EU AI Act

A basic overview

Is the activity in scope? Art 2

- Is your entity a Provider, Deployer, Distributor, Product, Manufacturer, Authorised Representative, Affected Person (Art 2) and carrying out an in-scope activity?
- Is the system an 'AI System' as defined in Art 3 (if your system is a General Purpose (GPAI) Model then specific obligations apply on a provider under Art 53.

Exemptions? Art 2

- There are a number of exemptions, including AI system used for military purposes, public bodies or international organisations using AI systems within international frameworks, and AI components provided under free and opensource licenses, amongst others (Art 2). The Act will not apply to systems operating within an exemption.

Is the AI System Prohibited? Art 5

- Prohibited systems include those which adopt subliminal techniques, exploit vulnerabilities, creating or expand facial recognitions databases through untargeted scraping from the internet or CCTV footage, inferring emotions, biometric categorisation, amongst others. A prohibited system is illegal under the Act.

Is the AI System High Risk? Art 6

- A system will be high-risk if (i) the AI system is intended to be used as a safety component or a product, or the AI system is itself a product covered by legislation in Annex 1 of the Act, AND (ii) is itself or part of a product required to undergo a third-party conformity assessment, with a view to the placing on the market or putting into service that product pursuant to the legislation in Annex I (Art 6(1))
- AI Systems will not be considered high risk of they do not pose significant risk of harm to the health, safety or fundamental rights of a natural person, including by not materially influencing the outcome of decision making.

High-risk system obligations

Provider obligations (Art 16)

- Include but are not limited to: ensure the AI systems are compliant with the AI Act, use quality management systems, keep specific documentation and logs, carrying out conformity assessments, preparing declarations of conformity for each high-risk system, technical documentation, record keeping, human oversight.

Deployer obligations (Art 26)

- Include but are not limited to: taking appropriate technical and organisational measures to ensure compliance with provider instructions, allocate human oversight to natural persons who are competent, ensure input data is relevant and sufficiently representative (to the extent the deployer exercises control over it), monitor the operation of the high-risk AI system and report incidents to the provider and relevant national supervisory authorities, keep records of logs generated by the high-risk AI system (if under the deployer's control) for at least six months, cooperate with relevant national competent authorities, and complete a fundamental rights impact assessment before using a high-risk AI system.

Transparency obligations (Art 50)

Providers and deployers of certain AI systems and GPAI models are also subject to transparency obligations to:

- Ensure that users are aware that they are interacting with AI, inform users when emotion recognition and biometric categorisation systems are being used, and label AI-generated content as such.

EU AI Act 2024

Key Milestones for Organisations and Businesses

AI Category	Sub-type	NEW SYSTEMS KEY MILESTONES (Enforcement)	EXISTING SYSTEMS KEY MILESTONES (Enforcement)
Prohibited AI	All prohibited AI and AI Literacy	**Feb 2025**	**Feb 2025**
General Purpose AI	Models with under 10^{25} compute used	**Aug 2025**	**Aug 2026**
	'Systemic risk' models with over 10^{25} compute used	**Aug 2025**	**Aug 2026**
High-Risk AI	Systems that could be discriminatory	**Aug 2026**	**Aug 2027**
	Safety components of EU-regulated products	**Aug 2027**	**Aug 2027**
	Large-scale IT systems or systems used by public authority	**Aug 2026**	**Aug 2028**

The UK Approach

how will a new Labour Government will regulate AI?

What do we know so far?

- **No "AI Bill" yet:** Reports in the press prior to the King's speech had indicated that Starmer would introduce an "AI Bill". A multitude of bills were proposed in the speech but there is no reference to an AI "bill".

- **Regulation likely for "Developers of the most powerful AI models":** a statement at the King's Speech indicates Labour's priority is to regulate "developers of the most powerful artificial intelligence models".

- **"Requirements on Developers":** Technology Secretary Peter Kyle has previously said that Labour will introduce a "statutory code" requiring AI developers to share safety test data with the government. AI companies would have to inform the Government whether they were planning to develop AI systems over a certain level of capability and would need to conduct safety tests with independent oversight. Kyle has also said that Labour would create a "regulatory innovation office" to encourage greater speed and adaptability to new tech from regulators.

- **A different approach to the previous Conservative Government:** The Sunak-led government backed a 'pro-innovation' approach, developing a non-binding, cross-sector, principles-based framework to enable existing regulators such as the ICO and FCA to set their own rules. It prioritised remaining agile as new technologies emerged, but arguably failed to deliver the regulatory certainty needed by UK firms and investors.

THE US APPROACH—STATE BY STATE

COLORADO AI ACT

- Only state to pass dedicated AI law
- "High Risk AI Systems"
  - Education, employment, financial or lending, health care, housing, insurance, legal services
- Obligations for developers *and* users that do business in Colorado
- AG Rulemaking Authority
- Effective Date: February 2026

COLORADO AI ACT—DEVELOPER OBLIGATIONS

To Deployers and Other Developers:

- Disclosure of uses and risks
- Documentation of:
  - Data used
  - Limitations of system
  - Discrimination evaluation and mitigating steps
  - Information reasonably necessary to understand risk
  - Information reasonably necessary for impact assessment

On Website:

- Summary of systems that are available to deployers or other developers
- Management of reasonably foreseeable risks

To AG:

- Deployed system has caused or is likely to cause discrimination

COLORADO AI ACT—DEPLOYER OBLIGATIONS

- Risk Management Program
- Impact Assessment
- Notification to Consumers
- Right to Appeal
- Website Disclosures
- Notice to AG upon finding of discrimination

California Privacy Protection Agency

AUTOMATED DECISION-MAKING TECHNOLOGY REGULATIONS

- Still in draft form
- Involves processing personal information
- General obligations:
  - Notice
  - Opt-out
  - Risk Assessments
- Potential for impact on common employment practices

BEST PRACTICES FOR CORPORATE GOVERNANCE

Track Regulation

- International
- State
- Municipal

Develop AI Governance Programs

- Leverage existing Privacy & Data Security programs
- Risk assessments
- Assign management responsibilities
- Ensure board reporting

Vendor Management

- Contracting
- Cross border transfer
- Understanding data usage

THANK YOU FOR JOINING

Paolo Sbuttoni
Partner, Foot Anstey LLP
Paolo.sbuttoni@footanstey.com
+44 (0)117 403 8980
+44 (0)7870 832 927

Gregory P. Szewczyk
Partner, Ballard Spahr LLP
szewczykg@ballardspahr.com
303.299.7382

CyberAdviser
Subscribe to award-winning our blog at
https://www.cyberadviserblog.com