DRAFT OUTLINE FOR REVIEW

IAPP UK Intensive 2026

Privacy | AI governance | Cybersecurity law

Training 23-24 February

Workshops 24 February

Conference 25-26 February

LONDON

#IAPPIntensive26

The Digital Compliance Matrix

Making sense of the overlapping web of data laws

WELCOME AND INTRODUCTIONS

Jane Finlayson-Brown
Partner

A&O SHEARMAN

Caroline Goulding
Data Protection Officer,
DMA Compliance Officer

TikTok

Jas Johal
Partner, AI, Data and Privacy

hbh HUNTER BRIGHT HEADMAN

Ruth O'Toole
Global Data Protection officer

Pinterest

The Digital Compliance Matrix
Making sense of the overlapping web of data laws

1

Understanding the Digital Law Matrix

- ***Regulatory Overview***
- ***Global Baseline & Common Themes***
- ***Digital Omnibus – Practical Considerations & Operational Impact***
- ***Initial Considerations & Opportunities for Multi-Domain Compliance***

2

Operationalizing a multi-domain compliance program

- ***Scaling Multi-Domain Compliance Programs : Best Practices & Standards***
- ***Embedding Digital Compliance into Product***
- ***Digital Governance & Evolving Role of DPO***
- ***Role of Privacy Enhancing Technologies & Automation in Scaling Compliance***
- ***Legal complexities impacting operationalization of digital laws***

3

Wrap Up, Future Trends & Key Takeaways

- ***Regulatory Enforcement Trends***
- ***Geo-political Considerations Impacting Digital Compliance Strategies***
- ***Key Lessons Learned & Practical Takeaways***

4

Concluding Remarks and Q&A

- ***Q&A***

Key digital risks

- Privacy and data protection
- Cyber security
- Emerging tech
- Threats to children and vulnerable people
- Threats to democracy

EUROPEAN DIGITAL RIGHTS AND PRINCIPLES

- Putting **people and their rights at the centre** of the digital transformation
- Supporting **solidarity and inclusion**
- Ensuring **freedom of choice** online
- Fostering **participation in the digital public space**
- Increasing **safety, security and empowerment** of individuals (especially young people)
- Promoting the **sustainability of the digital future**

- Growth agenda
- Geo-political challenges and uncertainty
- Regulatory fragmentation and inconsistency
- Skills and resourcing

European digital landscape

- **Digital Fairness Act**
  Tackles manipulative online practices (dark patterns, addictive design, exploitative personalisation, influencer marketing) to strengthen consumer protection online.

- **Digital Omnibus**
  Horizontal simplification package adjusting timelines & implementation across the data acquis
- **FIDA**
  Framework for secure, consent-based financial data sharing enabling customers to access, control, and port their financial data across the EU's open finance ecosystem.

- **Digital Omnibus on AI**
  Proposed adjustments to compliance timelines.
- **AI Act secondary legislation and delegated acts** (2026–2028)

- **CSA2 ↔ DNA**
  Digital infrastructure & cybersecurity package, proposed EU-level cyber response.
- **U.K. Cybersecurity and Resilience Bill** Revisions to U.K. NIS Regs

- **Tech Sovereignty Package** (Planned)
  Upcoming cluster of initiatives to reinforce European autonomy in cloud, compute, quantum and deep-tech infrastructure.(Cloud & AI Development Act, Quantum Act, European Innovation Act

E-COMMERCE

- **P2B Regulation**
  Ensures fairness for business users on platforms.

- **E-Commerce Directive**
  Baseline rules for online services and liability.
- **Digital Services Act**
  Obligations for platforms incl. content moderation.
- **U.K. Online Safety Act**
  Obligations for platforms and search services regarding legal and illegal online harms
- **Digital Markets Act**
  Gatekeeper rules for fair digital markets.
- **U.K. Digital Markets, Competition and Consumers Act** Digital markets regime for undertakings with strategic market status and consumer protection
- **ePrivacy Directive**
  Current e-communications privacy rules. ePrivacy Regulation proposal — withdrawn (2025 Work Programme)
- **U.K. ePrivacy Regulation**
  Current e-communications privacy rules

DATA

- **Data Governance Act**
  Rules for data intermediaries & reuse of protected public-sector data.
- **Open Data Directive**:
  Re-use of public sector information (PSI)
- **Free Flow on Non-personal Data Regulation** (FFNPD) enables free movement on non personal data within the EU

- **GDPR**
  EU-wide data protection framework.
- **U.K. GDPR**
  UK-wide data protection framework
- **Data Act**
  Access & sharing framework for IoT/device data, switching cloud providers.
- **EHDS**
  Framework for sharing electronic health data
- **U.K. Data (Use and Access) Act**
  Enabling legislative framework for data access and sharing

AI

- **AI Liability Directive (Withdrawn)** Withdrawn proposal for AI civil liability

- **AI Act**
  Risk-based regulation of AI systems.
- **Product Liability Directive**
  Adapting the product liability regime to the digital age to include software and AI integrated products.

CYBERSECURITY

- **NIS2 Directive**
  Replacing NIS 1 - cybersecurity baseline for key sectors.
- **U.K. NIS Regulations**
  Cybersecurity baseline for key sectors.
- **DORA**
  Operational resilience for financial sector.
- **U.K. Financial Services and Markets Act and regulator rules**
  Operational resilience for financial sector
- **Cyber Resilience Act**
  Cybersecurity for digital products.
- **U.K. Product Security and Telecommunications Infrastructure Act** Cybersecurity for certain digital products
- **CER Directive**
  Physical resilience of critical entities.
- **eIDAS 2.0**
  Trust services and digital identity wallet.
- **U.K. eIDAS Trust service framework.** DUAA also addressing approach to digital verification

◇ Adopted ◇ Proposal ◇ Withdrawn ◇ Proposal for repeal under the Digital Omnibus

A multitude of bodies for AI -U.K./EU

Government Digital Service

Incorporates Central Digital and Data Office, Geospatial Commission, AI Incubator and parts of Responsible Tech Adoption Unit

Creating Responsible AI Advisory Panel

Site of expertise and supports joined-up digital delivery in government

Digital Regulation Cooperation Forum

Collaboration and cooperation between ICO, Ofcom, CMA and FCA

Regulatory Innovation Office

Supports growth in areas of fast-growing tech

Cross cutting approach

Reducing regulatory barriers to innovation

AI Standards Hub

Government supported partnership to advance role that standards can play in governance and innovation

EU National Public Authorities

Enforce High Risk AI systems obligations under EU AI Act

Ada Lovelace Institute

Research institution and policy influencer

EU Conformity Assessment Bodies

Perform third party assessment activities in relation to EU AI Act

Sandboxes

U.K. AI Growth Lab proposal

FCA

Ofcom

AI Opportunities Unit

Implements AI Opportunities Action Plan recommendations

European Commission

Sovereign AI Unit

Supports government in harnessing AI capability to unlock economic growth and enhance national security

Alan Turing Institute

Research institution and policy influencer

AI Safety Institute

Research organisation

Testing AI systems strengthening AI development practice and fostering collaboration

Working with Central AI Risk Function established as part of AI Policy Directorate within DSIT

National Cyber Security Centre

ISO

International Organization for Standardization

CEN

European Committee for Standardization

EU Data Protection Board

Supports consistent application and enforcement of data protection law across EEA

CMA

ICO

BSI

British Standards Institution

CENELEC

European Committee for Electrotechnical Standardization

ETSI

European Telecommunications Standards Insittute

EU AI Office

Part of EU AI governance system

Acts as centre of AI expertise

Supports national governance bodies

Enforces EU AI Act re GPAI

EU AI Advisory Forum and Scientific Panel of Independent Experts

Part of EU AI governance system

Advisory Forum to advise the AI Board and EU Commission

Scientific panel to advise and support the AI Office

EU National Competent Authorities

Market surveillance authorities and notifying authorities (re conformity assessment bodies) in relation to EU AI Act

EU AI Board

Part of EU AI governance system

Coordinates and ensures member state cooperation for consistent implementation of the EU AI Act

Provides advice on AI policy and strategic matters

The Digital Compliance Matrix
Making sense of the overlapping web of data laws

1

Understanding the Digital Law Matrix

- ***Regulatory Overview***
- ***Global Baseline & Common Themes***
- ***Digital Omnibus – Practical Considerations & Operational Impact***
- ***Initial Considerations & Opportunities for Multi-Domain Compliance***

2

Operationalizing a multi-domain compliance program

- ***Scaling Multi-Domain Compliance Programs : Best Practices & Standards***
- ***Embedding Digital Compliance into Product***
- ***Digital Governance & Evolving Role of DPO***
- ***Role of Privacy Enhancing Technologies & Automation in Scaling Compliance***
- ***Legal complexities impacting operationalization of digital laws***

3

Wrap Up, Future Trends & Key Takeaways

- ***Regulatory Enforcement Trends***
- ***Geo-political Considerations Impacting Digital Compliance Strategies***
- ***Key Lessons Learned & Practical Takeaways***

4

Concluding Remarks and Q&A

- ***Q&A***

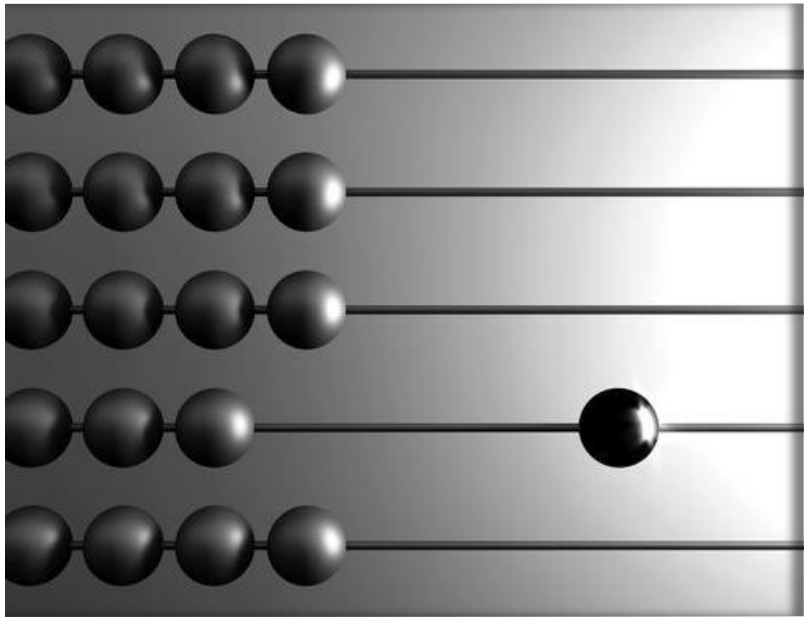
The Digital Omnibus and AI Omnibus

TARGETED EU INITIATIVE TO "SIMPLIFY" AND ALIGN DIGITAL REGULATION

- Proposed 19 November 2025
- Creating coherence across fragmented EU digital regulation framework
- Reducing overlaps across compliance obligations
- Making compliance more proportionate and innovation-friendly
- Driving innovation by reducing unnecessary regulatory friction

EDPB AND EDPS PUBLISHED JOINT OPINION REGARDING THE DIGITAL OMNIBUS ON THE AI REGULATION PROPOSAL (20 JAN 2026)

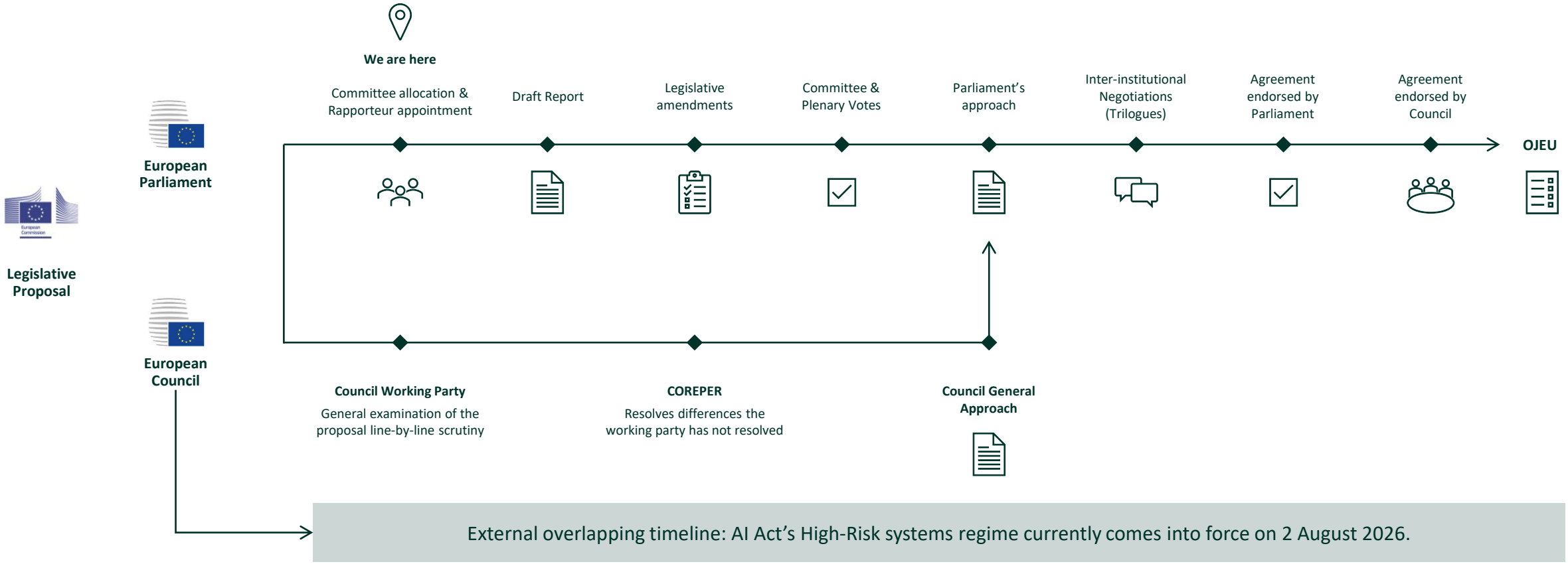
EDPB AND EDPS PUBLISHED JOINT OPINION REGARDING ON THE DIGITAL OMNIBUS REGULATION PROPOSAL (11 FEBRUARY 2026)



Next steps

Assumes that the Parliament and the Council reach an agreement in first reading.

If not, the file moves to second reading – starting with a new draft report after Trilogues.



Digital Omnibus: The response, the praise, the push back

In general

- Praise for goals but nuanced responses flagging scope/need for improvement rather than unconditional endorsment

Privacy advocates

- Strong opposition to perceived weakening of fundamental rights
- Proposals considered a significant rollback rather than simplification
- Concern over scrutiny of proposals

Member States

- Concerns raised regarding national security, AI related changes, and key definitions etc
- Commission proposals like to be adjusted/removed

The Digital Compliance Matrix
Making sense of the overlapping web of data laws

1

Understanding the Digital Law Matrix

- ***Regulatory Overview***
- ***Global Baseline & Common Themes***
- ***Digital Omnibus – Practical Considerations & Operational Impact***
- ***Initial Considerations & Opportunities for Multi-Domain Compliance***

2

Operationalizing a multi-domain compliance program

- ***Scaling Multi-Domain Compliance Programs : Best Practices & Standards***
- ***Embedding Digital Compliance into Product***
- ***Digital Governance & Evolving Role of DPO***
- ***Role of Privacy Enhancing Technologies & Automation in Scaling Compliance***
- ***Legal complexities impacting operationalization of digital laws***

3

Wrap Up, Future Trends & Key Takeaways

- ***Regulatory Enforcement Trends***
- ***Geo-political Considerations Impacting Digital Compliance Strategies***
- ***Key Lessons Learned & Practical Takeaways***

4

Concluding Remarks and Q&A

- ***Q&A***

Compliance in a fragmented landscape: the AI slice

Diverging approaches to AI regulation to align with country's strategic objectives

Additional complexity from evolving laws for privacy, digital, IP, antitrust, FDI, consumer, sector-specific regulation

Significant intervention already by **data and antitrust authorities** in all major jurisdictions. Expected to increase

U.S.

- De-regulatory approach
- No federal AI legislation
- Revocation of Biden's AI Executive Order
- New Executive Order 'Ensuring a National Policy Framework for AI'
- Federal vs State tensions
- Fragmented state laws –legislatures in all 50 states introduced AI related bills (dozens enacted)
- California safe harbour
- NIST Risk Management framework
- Active enforcement by regulators, e.g., SEC, FTC – expected to reduce

U.K.

- No AI-specific legislation
- AI Security Institute
- AI Opportunities Action Plan
- Active regulators, e.g., FCA, CMA, ICO, Ofcom – all part of DRCF
- Focus on AI assurance alongside growth potential
- Interplay with data/digital laws, e.g., GDPR, Data (Use and Access) Bill

EU

- EU AI Act
- Pressure to simplify regulatory burden – Digital Omnibus proposing adaptations to adapt and simplify data and AI regulations
- AI Office
- Codes of Practice for AI developers and GPAI models
- EDPB opinion on use of personal data in AI training
- AI innovation package. AI continent action plan. Apply AI strategy
- Interplay with data / digital laws, e.g., GDPR, Data Act, Data Governance

APAC

- PRC regulating AI to protect state's objectives
- Highly fragmented across region
- Interplay with wider privacy and data protection laws
- Convergence toward risk-based and sector-specific regulation

GLOBAL EMERGING CORE PRINCIPLES

- **Safety**
- **Security**
- **Transparency**
- **Explainability**
- **Accountability**
- **Contestability and redress**

Underpinned by a respect of existing human rights frameworks.

AI STANDARDS

e.g. ISO/IEC on

AI management systems, risk management, impact assessments and governance implications

Compliance will be **onerous in near- to mid- term.**

AI Regulatory Landscape in the U.K.

No AI-specific legislation:

- Despite private members bills
- No substantive AI provisions in Data (Use and Access) Act, though ADM requirements adjusted

Focus on AI enablement, innovation and growth:

- U.K. AI Opportunities Plan

Active regulators:

- E.g. FCA, CMA, ICO, Ofcom – all part of DRCF
- Expecting ICO Code on AI and ADM

AI Growth Lab:

- Proposals for cross-economy sandbox with statutory basis to temporarily disapply regulatory requirements
- Potential to apply regulatory changes based on sandbox outcomes

Getty v Stability AI:

- High court finds in favour of Stability AI and rejects Getty's secondary copyright infringement arguments

AI Regulatory landscape in the Americas

US Federal Level regulation:

- De-regulatory approach
- No federal AI legislation
- New EO - Ensuring a National Policy Framework for Artificial Intelligence

US State Level regulation:

- Federal vs State tensions.
- Fragmented state laws.
- Legislatures in all 50 states have introduced AI related bills with dozens enacted (e.g. Utah, Texas, California, Colorado)

US guidance on risks to AI systems e.g. re. cyber:

- NIST AI RMF: Sets out principles for secure and trustworthy AI systems
- NSA “Deploying AI Systems Securely”: practical controls for externally developed AI tools
- Treasury on AI cyber risks: Threat review and best practices, with a focus on the financial services industry

Latin America developing AI regulation:

- Early stages of AI specific legislative activity
- AI related bills and proposals in e.g. Brazil, Argentina, Chile, Colombia, Mexico, Peru
- Typically risk-based approaches

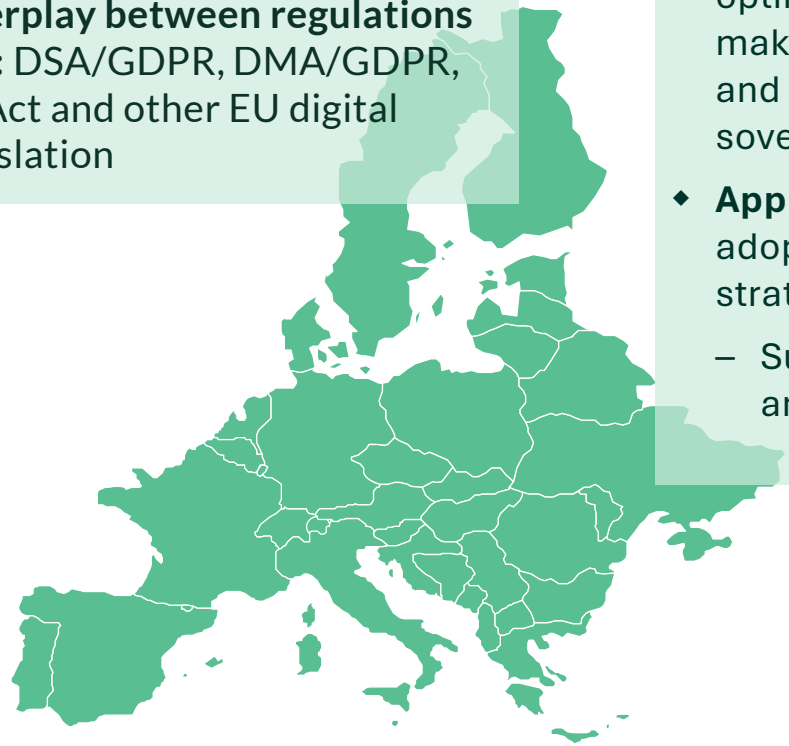
AI Regulatory Landscape in the EU

Familiar EU AI Act now in force –focus on application and implementation:

- **AI Act Service desk:** accessible information hub offering guidance on EU AI Act application
- **Single Information Platform:** online gateway to EU-wide AI resources
- **EU AI Office** key role in implementing EU AI Act, supports governance by MS, enforces rules for GPAI models and leads on AI Continent Action Plan and Apply AI Strategy
- **Commission guidelines** e.g. on AI incidents, on transparency AI systems, and for providers of GPAI

Pressure to simplify regulation and reduce burden

- **Digital Omnibus:** to adapt/ simplify data and AI regulation
- **Guidance and studies on interplay between regulations e.g.:** DSA/GDPR, DMA/GDPR, AI Act and other EU digital legislation



Focus on growth, innovation and competition:

- **AI Continent Action Plan:** intended to develop and enable AI to support automation, optimisation and decision making - therefore competition and growth, as well as security, sovereignty and democracy
- **Apply AI Strategy:** to boost AI adoption and innovation in strategic sectors
  - Supported by Apply AI Alliance and AI Observatory

AI Regulatory landscape in APAC

Moving from “soft-law” guidance toward **targeted, risk-based regulation**

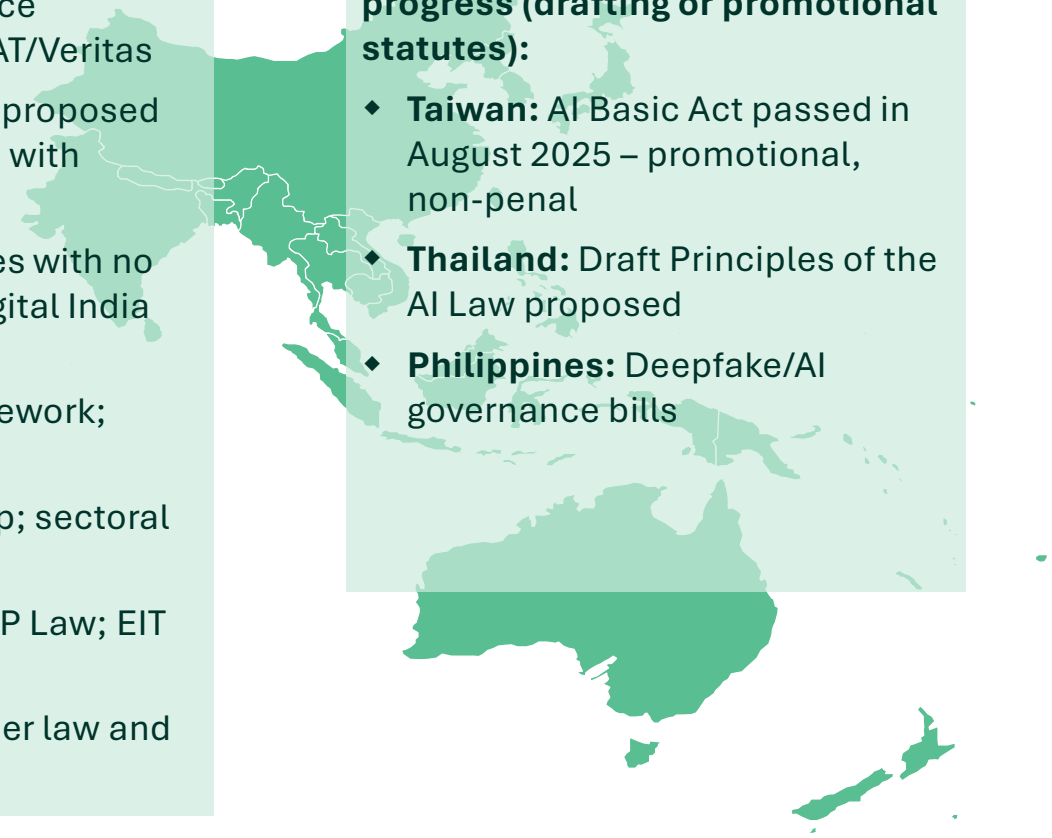
Soft-law, sectoral and privacy-anchored governance:

- **Singapore:** Model AI Governance Frameworks; AI Verify; MAS FEAT/Veritas
- **Australia:** AI Ethics Principles; proposed high-risk guardrails; integration with Privacy/Online Safety
- **India:** AI Governance Guidelines with no new AI law; DPDP Act 2023; Digital India Act drafting
- **Hong Kong:** PCPD Model Framework; HKMA guidance
- **Malaysia:** National AI Roadmap; sectoral guidance
- **Indonesia:** Ethical circular; PDP Law; EIT Law
- **New Zealand:** Privacy/consumer law and regulator guidance

Convergence toward EU-style risk classification is emerging but **approaches remain fragmented**

Comprehensive frameworks in progress (drafting or promotional statutes):

- **Taiwan:** AI Basic Act passed in August 2025 – promotional, non-penal
- **Thailand:** Draft Principles of the AI Law proposed
- **Philippines:** Deepfake/AI governance bills



Strong regional emphasis on **data privacy protection**, **transparency**, **testing** and **lifecycle monitoring**

Binding AI-specific statutes or regulations.

Regulatory philosophies diverge:

- **PRC:** Prescriptive, enforcement heavy model. Algorithmic recommendation, deep synthesis, generative AI measures. Draft AI Law proposed in March 2024
- **South Korea:** Balanced, risk-based statute. AI Basic/Framework Act – in force from 2026
- **Japan:** Innovation first, cooperative governance approach. AI Promotion Act – promotional, non-penal; proposals for responsible AI
- **Vietnam**: Risk-based AI Law passed December 2025, in force March 2026

The Digital Compliance Matrix
Making sense of the overlapping web of data laws

1

Understanding the Digital Law Matrix

- ***Regulatory Overview***
- ***Global Baseline & Common Themes***
- ***Digital Omnibus – Practical Considerations & Operational Impact***
- ***Initial Considerations & Opportunities for Multi-Domain Compliance***

2

Operationalizing a multi-domain compliance program

- ***Scaling Multi-Domain Compliance Programs : Best Practices & Standards***
- ***Embedding Digital Compliance into Product***
- ***Digital Governance & Evolving Role of DPO***
- ***Role of Privacy Enhancing Technologies & Automation in Scaling Compliance***
- ***Legal complexities impacting operationalization of digital laws***

3

Wrap Up, Future Trends & Key Takeaways

- ***Regulatory Enforcement Trends***
- ***Geo-political Considerations Impacting Digital Compliance Strategies***
- ***Key Lessons Learned & Practical Takeaways***

4

Concluding Remarks and Q&A

- ***Q&A***

EU GDPR regulatory enforcement

Subject to appeal /not yet finalised

Finalised

Status not specified

Date	Authority	Actors	Fine	Area of infringement
2021	Luxembourg DPA	Large online marketplace	€746m	Unlawful processing and transparency failures for advertising personalisation
2021	Ireland DPC	Messaging platform	€225m	Non-compliance with transparency obligations
2022	Ireland DPC	Social media / photo-sharing platform	€405m	Children's data and transparency
2023	Ireland DPC	Major social-media group	€1.2bn	Insufficient legal basis (US data transfers, first decision after Schrems II)
2023	Ireland DPC	Short-form video platform	€345m	Non-compliance with processing principles: public-by-default settings, Family Pairing risks, insufficient transparency, and dark patterns
2024	Ireland DPC	Professional networking platform	€310m	Behavioural and targeted advertising-insufficient legal basis
2024	Dutch AP 2024	Mobility / ride-hailing platform	€290m	Unlawful international data transfers (drivers' data sent to US without valid safeguard mechanisms)

Persistent challenges in cross-border enforcement - leading to the new Procedural Regulation (2025/2518)

Scrutiny of behavioural advertising and legal basis failures

Children's data protection and dark patterns are priority enforcement areas

Persistent lack of transparency on fine collection and increasing procedural streamlining

U.K. examples

Date	Actors	Fine	Area of infringement
2026 (Feb)	Social media platform	£14.47m	Children's data and privacy
2026 (Feb)	Image sharing platform	£247,590	Children's data and privacy
2020	Large retailer	£500,000	Security failures
2022	Facial recognition database	£7.5m	Transparency, lawful basis, special category data etc
2024	Leisure facility	Cease processing and destroy existing biometric data	Biometric monitoring

Majority of action relates to security failures

Examples demonstrate action regarding children and new tech

ICO takes an outcomes-based approach to enforcement with more clarity on approach provided in guidance

However, ICO approach faced some criticism due to perceive lack of action (including with respect to public sector)

ICO facing pressures of growing numbers of complaints
Recent refined approach to enforcement flags risk-based approach

DSA regulatory enforcement

Date	Authority	Actors	Fine	Infringements
2025	European Commission	Large social-media platform (VLOP)	€120m	Transparency failures, misleading verification design and obstacles to researcher data access
2025	European Commission	Short-form video platform	No monetary fine (binding commitments)	Deceptive design, opaque advertising practices and inadequate consumer transparency
2025	European Commission	Large social-media group – preliminary findings	Preliminary infringement findings	Failure to provide researcher data access and systemic-risk transparency obligations
2025	European Commission	Short-form video platform & large social-media group	Preliminary infringement findings	Burdensome and unreliable researcher data-access mechanisms under Article 40 DSA

Transparency & design practices

Researcher data-access obligations

Enforcement expanding

The Digital Compliance Matrix
Making sense of the overlapping web of data laws

1

Understanding the Digital Law Matrix

- ***Regulatory Overview***
- ***Global Baseline & Common Themes***
- ***Digital Omnibus – Practical Considerations & Operational Impact***
- ***Initial Considerations & Opportunities for Multi-Domain Compliance***

2

Operationalizing a multi-domain compliance program

- ***Scaling Multi-Domain Compliance Programs : Best Practices & Standards***
- ***Embedding Digital Compliance into Product***
- ***Digital Governance & Evolving Role of DPO***
- ***Role of Privacy Enhancing Technologies & Automation in Scaling Compliance***
- ***Legal complexities impacting operationalization of digital laws***

3

Wrap Up, Future Trends & Key Takeaways

- ***Regulatory Enforcement Trends***
- ***Geo-political Considerations Impacting Digital Compliance Strategies***
- ***Key Lessons Learned & Practical Takeaways***

4

Concluding Remarks and Q&A

- ***Q&A***

RESOURCE LIST

Digital Omnibus Package: How will these changes affect your business?

European Commission announces new Cybersecurity Package, including proposed amendments to the Cybersecurity Act

Digital Networks Act and CSA 2.0: key implications for telecoms and digital infrastructure

Insurability of cyber fines: Navigating a complex and evolving risk landscape

AI governance: adapting to AI agents and tech democratisation

AI Agents Podcast Series

White House issues executive order establishing a national policy framework for AI and signaling a strategy to pre-empt conflicting state laws

IAPP EU Digital Laws Report 2025

IAPP Organizational Digital Governance Report 2025

A&O Shearman on data

A&O Shearman on technology

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Intensive 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!