iapp

EU digital law and policy: Mapping the emergent landscape

Friday, 16 January
07:00–08:00 PST
10:00–11:00 EST
16:00–17:00 CET

Welcomes and Introductions

Anca Caruntu
Senior Public Affairs Director,
Samman

Moderator:

Müge Fazlioglu, CIPP/E, CIPP/US,
Principal Researcher, Privacy Law and
Policy, IAPP

Natallia Karniyevich
Partner, McDermott Will &
Schulte

Looking back at 2025

- Digital Operational Resilience Act (DORA)
- Cyber Solidarity Act
- AI's Act's ban on AI systems
- The European Health Data Space
- The Data Act
- The Commission's Digital Package – Digital Omnibus
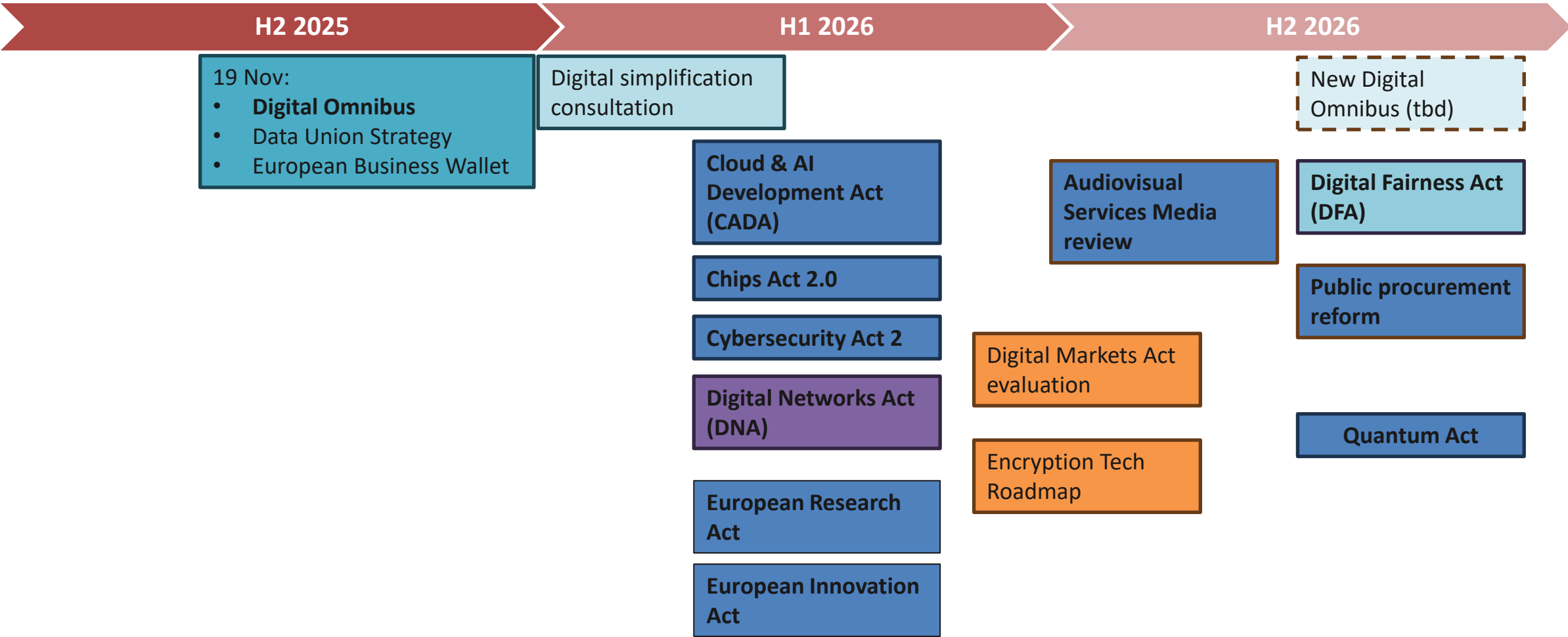
EU Digital Laws and Policies

EU Digital Laws Report 2025

iapp

Follow the link for the report!

- **Data Act**
- **Digital Services Act**
- **Digital Markets Act**
- **Data Governance Act**
- **NIS2 Directive**
- **AI Act**

Topics we would cover today:
- Current state of the digital Omnibus
- Key proposals for changes to these laws
- What is staying the same or unlikely to change
- Next steps

2026 EU Digital Agenda

H2 2025	H1 2026	H2 2026

19 Nov:
- **Digital Omnibus**
- Data Union Strategy
- European Business Wallet

Digital simplification consultation

New Digital Omnibus (tbd)

Cloud & AI Development Act (CADA)

Chips Act 2.0

Cybersecurity Act 2

Digital Networks Act (DNA)

European Research Act

European Innovation Act

Audiovisual Services Media review

Digital Markets Act evaluation

Encryption Tech Roadmap

Digital Fairness Act (DFA)

Public procurement reform

Quantum Act

Progressive entry into application and enforcement of the 2019–2024 digital acquis (DMA and DSA enforcement; transposition and application of the cyber acquis; Data Act entry into force; phased implementation of the AI Act; etc.)

A deeper look

- How are the Data Act and the DGA envisioned through the lens of the Digital Omnibus?

Cybersecurity

- What changes are envisaged under the Digital Omnibus in relation to cybersecurity?

Incident reporting

- **Introduction of the Single-Entry Point (SEP) for incident reporting.**
- **Common GDPR breach notification template for reporting to authorities.**
- **Common list of breach situations presumed to pose a high risk to** individuals' rights and freedoms.
- **End of ePD-based** <u>**personal**</u> **breach notifications.**
- **Aligning GDPR's threshold for notification to supervisory authorities with that for notifying individuals**:

A personal data breach would need to be notified **only if it is likely to result in a** <u>**high risk**</u> to individuals' rights and freedoms.

Notification deadline would be extended from **72 hours to** <u>**96 hours**</u>.

Notifications to authorities would be **routed via SEP** once operational.
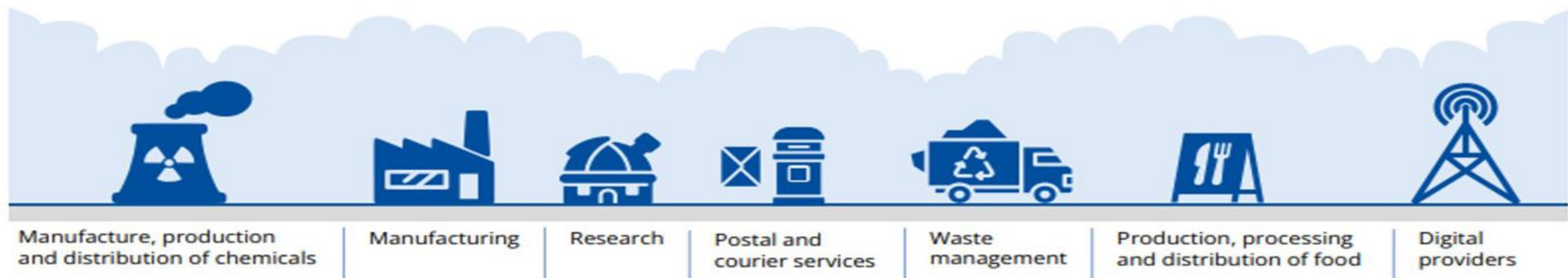
Cybersecurity

- How does the NIS2 Directive interact with other laws, such as the GDPR and other European legislation, including the CRA, CER, DMA, DSA, AI Act, and Data Act?
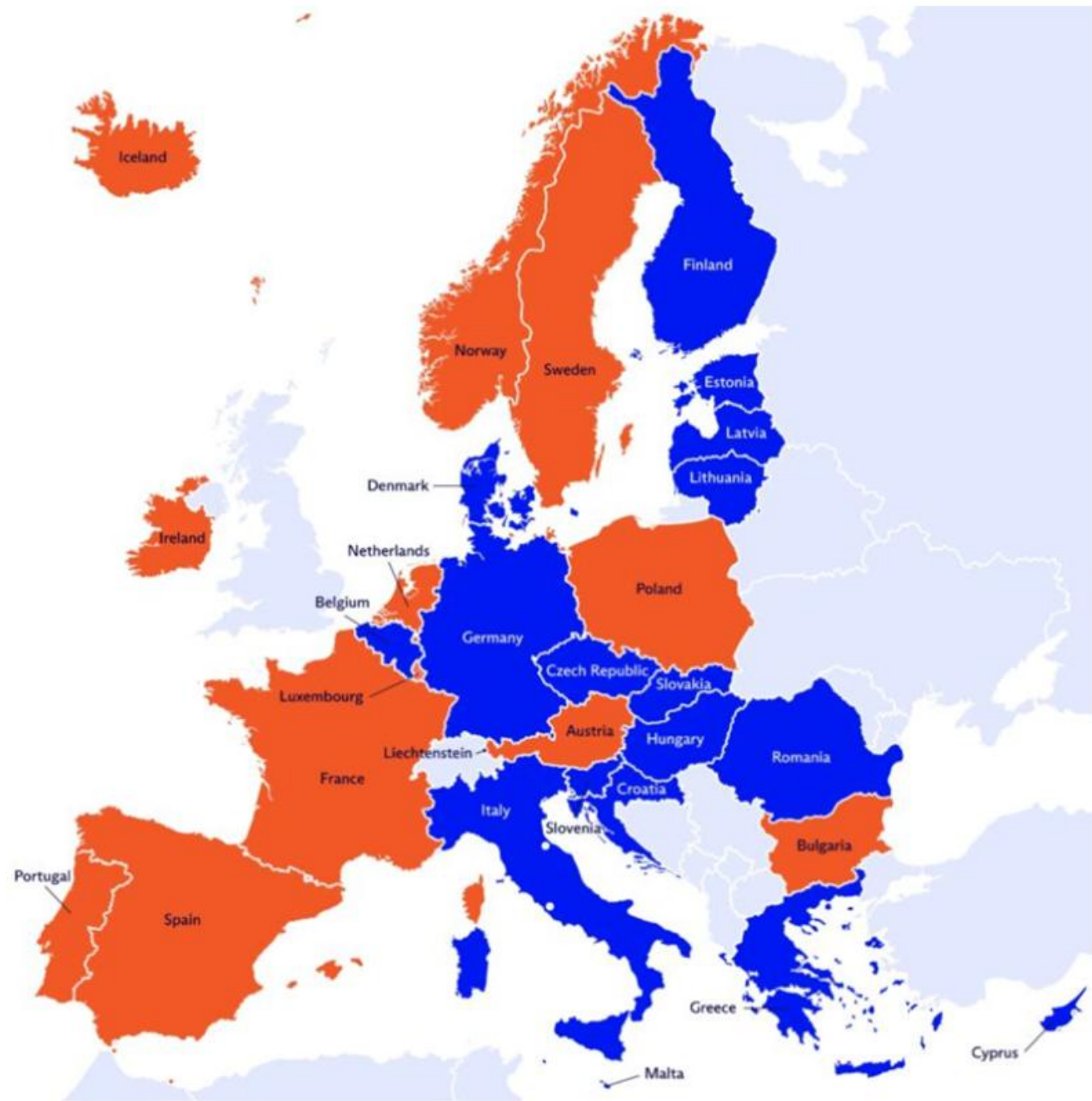
NIS2 Directive

Energy | Digital infrastructure | Transport | Space | Health | Public administration | Drinking water | Banking | Financial markets infrastructure | Waste water | ICT services management (B2B)

High criticality sectors

Manufacture, production and distribution of chemicals | Manufacturing | Research | Postal and courier services | Waste management | Production, processing and distribution of food | Digital providers

Other critical sectors

NIS2 Directive

- Transposition is underway (deadline was 17 Oct. 2024)

- 17 EU Member States have adopted implementing legislation

- Member States can adopt or maintain provisions ensuring a higher level of cybersecurity, provided that such provisions are consistent with Member States' EU law

NIS2 Directive and other European legislation

Regulation on Markets in Crypto-assets	Data Act	ePrivacy Regulation	PSD3
Database Directive	Digital Services Act	Artificial Intelligence Act	NISD2
Platform to Business Regulation	Data Governance Act	eIDAS2	Cybersecurity Act
European Cyber Resilience Act	Digital Markets Act	EHDS	Radio Equipment Directive

GDPR in the Digital Omnibus

- What are the ramifications of the EU's simplification agenda?
- What is the importance of these changes for the IAPP community?

GDPR in the Digital Omnibus

- New definition of personal data
- Legitimate interests for AI systems
- Use of sensitive data for AI development and operation
- Biometric data for identification verification
- Simplified privacy notice rules and new research exception
- 'Neutralized' abuse of access requests
- Consistent DPIAs

ePrivacy in the Digital Omnibus

- Cookie rules involving personal data **moved** to GDPR.
- Cross-border tracking falls under GDPR's **one-stop-shop + GDPR fines apply** (instead of lower national ones).
- Default **consent rule for access/storage** remains.
- **No consent** needed for requested services, security maintenance/restoration, or aggregated audience measurement for the controller's own use.
- **From banners to signals:** Websites and apps must allow users to give or refuse consent automatically; browsers must include tools to support this; standards to be created.
- After consent is declined, controllers **cannot** ask for a new consent for 6 months.
- Cookie rules for non-personal data now **effectively more onerous** for personal data.

AI in the Digital Omnibus

- **Delayed enforceability of rules on high-risk AI.**
- New legal basis for **processing sensitive data for bias detection**.
- **AI literacy obligations shifted** from companies to Member States / Commission.
- Several other smaller technical adjustments and simplifications are included.

What's next?

- What can we say about the future of digital responsibility and the role of the EU in shaping the digital landscape?

Web of implementation and monitoring

- Addition of new stakeholders
- What are the advantages and disadvantages?

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iappwf.questionpro.com/t/AbBPvZ7eSe

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your AIGP, CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration prior to the live webinar will automatically receive credit. After the broadcast date, individuals may submit for credit by completing the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other IAPP Web Conferences or recordings please contact: **livewebconteam@iapp.org**