TECH ignite

simmons+simmons

Session 2

The EU Digital Rulebook in Practice – From Data Act to AI as a Service.

TECH ignite

simmons+simmons

Session 2

New EU Digital Laws – Building a Practical Compliance Roadmap.

Jaap Tempelman
Partner (Amsterdam), Digital Business
Simmons & Simmons Netherlands

Snapshot of EU/DE Digital Laws

AA EU
Accessibility Act
All

AIA EU
Artificial Intelligence Act
All

AIL EU
AI Liability Directive
All

AVD EU
Vehicle Data Access
Industry

CER EU
Critical Entities Resilience Directive
All

CMR DE
Consent Management Regulation
All

CRes EU
Cyber Resilience Act
All

CSAM EU
Child Sexual Abuse Regulation
Technology

CSec EU
EU Cybersecurity Strategy
All

CSol EU
Cyber Solidarity Act
Public Sector

CSReg EU
Cybersecurity Regulation
Public Sector

DA EU
Data Act
All

DCD EU
Digital Content Directive
All

DFSC EU
Distant Financial Services Contracts Directive
Finance

DGA EU
Data Governance Act
All

DMA EU
Digital Markets Act
Technology

DORA EU
Digital Operational Resilience Act
Finance, Technology

DSA EU
Digital Services Act
Technology

EBW EU
European Business Wallets Regulation
All

ECO EU
Ecodesign Regulation
All

EDP DE
Employee Data Protection Act
All

eID2 EU
eIDAS 2.0 Regulation
All

EPR EU
ePrivacy Regulation
All

ESAP EU
European Single Access Point
Finance

FDPA DE
Federal Data Protection Act
All

FIDA EU
Financial Data Access
Finance

FMD DE
Financial Markets Digitalisation Act
Finance, Technology

GD4A EU
GreenData4All
All

GDPR+ EU
GDPR Procedural Regulation
All

GDU DE
Data Usage Act
All

GPSR EU
General Product Safety Regulation
All

HDS EU
European Health Data Space Regulation
Health & Life Sciences, Technology

HDU DE
Health Data Use Act
Health & Life Sciences, Technology

HPC EU
High-Performance Computing Regulation
Technology

HVD EU
High-Value Datasets
Public Sector

MDA DE
Mobility Data Act
Industry

NIS2 EU
NIS2 Directive
All

NISI DE
NIS2 Implementation Act
All

PAR EU
Political Advertising Regulation
Technology

PLD EU
Product Liability Directive
All

PWD EU
Platform Workers Directive
Technology

R2R EU
Right to Repair Directive
All

SRR EU
Short-Term Rentals Data
Technology

EU Cybersecurity Regulations

An overview

NIS2-Directive

- Cybersecurity requirements for essential and important entities.
- Implementation deadline: 18 Oct. 2024.

Critical Entities Resilience Directive

- Physical security requirements for designated essential entities.
- Implementation deadline: 17 Oct. 2024

Cyber Resilience Act

- Cybersecurity requirements for connected hardware and software products.
- 11 Sept 2026: report actively exploited vulnerabilities.
- 11 Dec. 2027: fully applicable.

Cyber Security Act

- Mandate ENISA and voluntary certification scheme.
- 27 Feb. 2025: fully applicable.
- To be revised in 2026.

Cyber Solidarity Act

- Strengthening EU's collective ability to respond to large-scale cybersecurity threats.
- 4 February 2025: in force.

Digital Operational Resilience Act

- Cybersecurity requirements for financial entities.
- 17 Jan. 2025: fully applicable.

NIS2 vs NIS1

Expansion of scope

- Moves beyond just "operators of essential services" to include many more sectors.
- Lowers thresholds to include most medium-sized and large entities.
- Designation by operation of law.

Enhanced security measures

- Mandates concrete measures like risk analysis, incident handling, supply chain security, and encryption.
- Explicit focus on securing the supply chain and supplier relationships.

Stricter incident reporting obligations

- Replaces vague reporting with strict, multi-stage requirements: a 24-hour "early warning" and a 72-hour incident notification.

Management liability and higher penalties

- Executives and board members are directly responsible for compliance, facing personal liability and potential bans for failing to implement required cybersecurity measures.
- Harmonized, stricter penalty regime, with fines up to €10 million or 2% of global annual turnover for essential entities, and up to €7 million or 1.4% for important entities.

Cybersecurity Package

Proposal to amend NIS2 – Jan 2026

Certification schemes

- Enabling Member States to require entities to demonstrate compliance through a certificate on cyber posture under a European cybersecurity certification scheme provided under the (revised) Cyber Security Act.

Maximum harmonisation through Implementing Acts

- Mandates concrete measures like risk analysis, incident handling, supply chain security, and encryption.
- Explicit focus on securing the supply chain and supplier relationships.

Introducing new "small mid-cap enterprises"

- Entities with <750 employees and <€150 million in annual turnover are only deemed "important entities".

Ransomware information gathering

- Empowering national CSIRTs to request additional information when a significant incident reported is caused by ransomware, including whether a ransom demand was made, by whom, whether it was paid, the amount, the payment method.

EU Cyber Resilience Act

CRA

Scope

- Harmonised cybersecurity obligations imposed on manufacturers/importers/distributors of connected products that are made available on the EU Market:
  - products with digital elements, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network.

Product with digital elements (PDE)

- A software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately.

Remote data processing obligations

- Data processing at a distance for which the software is designed and developed by or under the responsibility of the manufacturer of a PDE, and the absence of which would prevent the PDE from performing one or more of its functions.

Penalties

- fines up to €15 million or 2.5% of the total worldwide annual turnover.

EU Cybersecurity Act

Overview

- Adopted in 2019.
- Establishes ENISA, the European Union Agency for Cybersecurity.
- Sets up a voluntary European cybersecurity certification framework for ICT products, ICT services and ICT processes.

Cybersecurity Package – proposal 20 Jan. 2026

- Broadening role of ENISA, notably to include managing unified incident reporting platform and repository of incidents and threats.
- Strengthening and streamlining certification framework – still voluntary but potentially de facto mandatory through procurement rules, market expectations, or national requirements.
- Introduction of supply chain security mechanisms to identify, restrict, or exclude suppliers considered “high-risk” across 18 critical sectors.

EU Cyber Security Act

Supply chain security

- Security risk assessment by NIS Coordination Group of serious and structural non-technical risks to ICT supply chains posed by third countries, taking into account:
  - the existence of laws or practices requiring entities to report software or hardware vulnerabilities to authorities prior to those vulnerabilities being known to have been exploited;
  - the absence of effective judicial remedies, and independent and democratic control mechanisms, that can correct the identified security concerns;
  - substantiated information about one or more incidents of threat actors controlled from the third country and operating out of the territory of that country carrying out malicious cyber activities or campaigns, and the lack of ability or willingness of the third country to cooperate with the European Commission or EU Member States to address the risk

- Commission can identify high-risk countries, high-risk suppliers and key ICT assets, and (inter alia):
  - Prohibit NIS2 entities from using ICT components from high-risk suppliers;
  - Exclude high-risk suppliers from holding EU certifications, taking part in EU public procurement procedures, and funding programmes.

Digital Omnibus

General

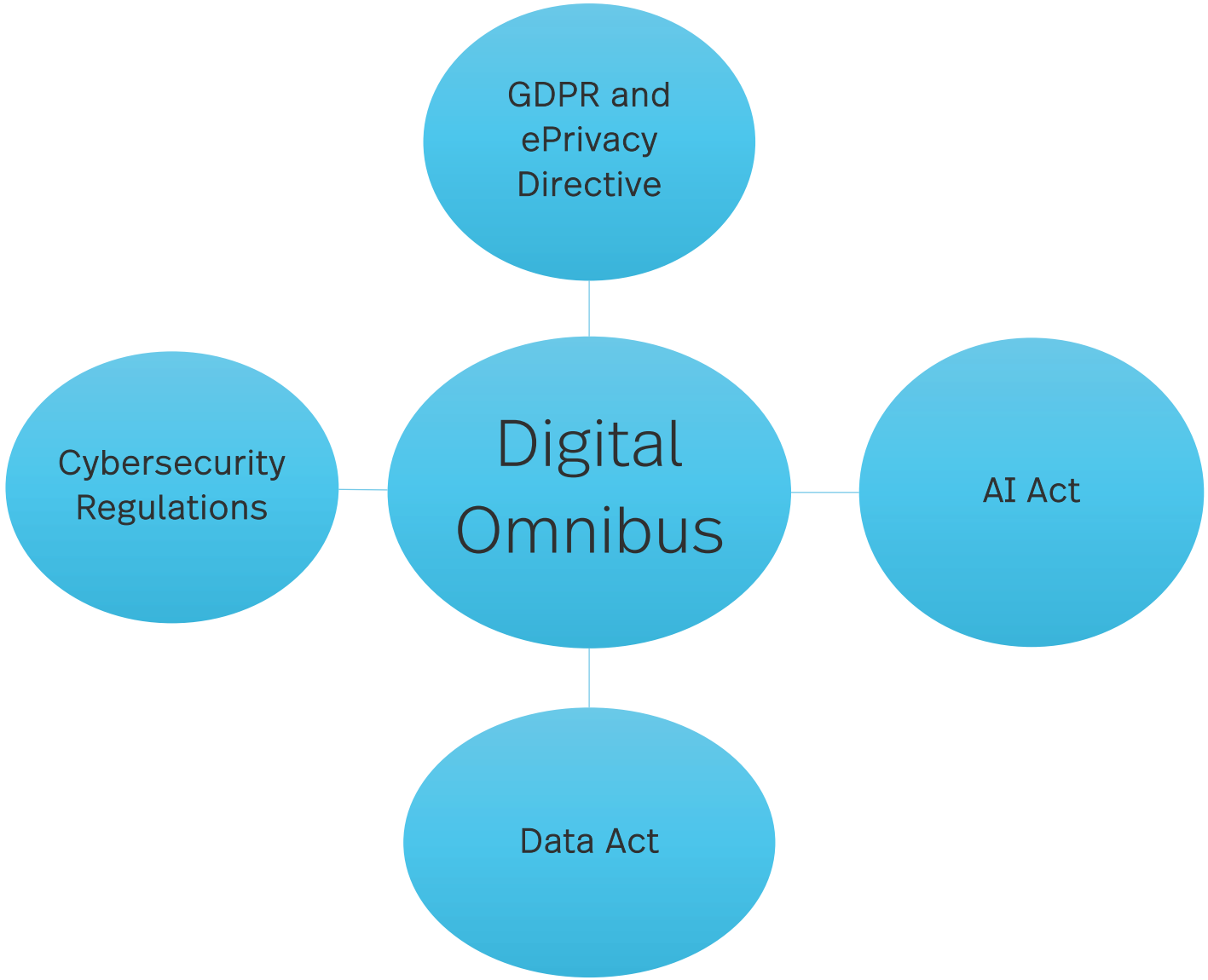
What is omnibus legislation?

- Single instrument amending multiple EU regulations
- Meant for “technical” or “specific” changes
- Fast-track legislative process
- Shorter turnaround times
- Steps can be skipped (such as impact assessments)

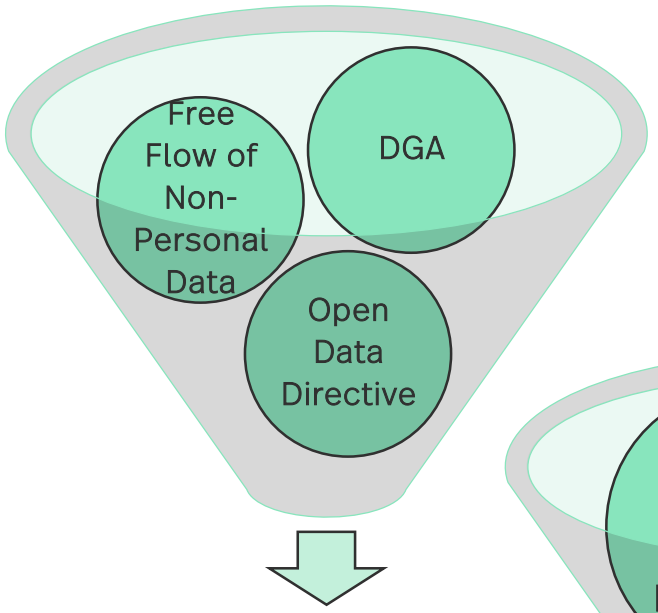
Two digital omnibus proposals to simplify EU digital rules:

- one amending personal and non-personal data and cybersecurity rules
- one amending the EU AI Act

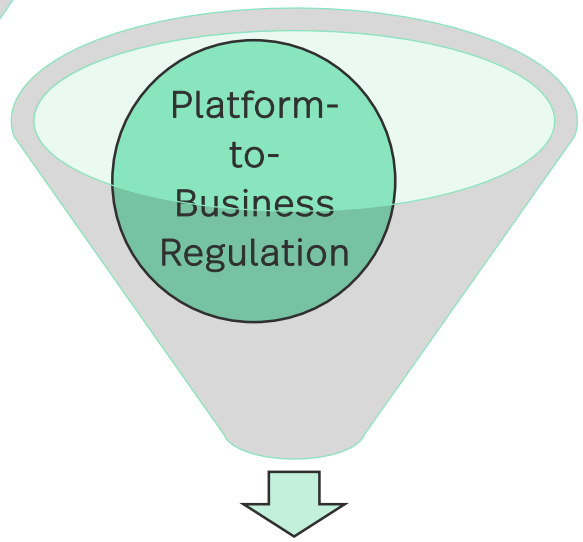
Core changes



Repealed regulations



Data Act



DSA and DMA

EU Digital Omnibus

Key impact on GDPR

1	**Personal data definition**: identification must reasonably be possible for the data holding entity, otherwise it is not personal data (e.g. dynamic IP address).
2	**Training of AI systems:** entities may rely on legitimate interests.
3	**Processing of special category data**: exemption for processing of special categories of personal data for development and operation of an AI system or model, subject to safeguards.
4	**Processing of biometric data:** permitted for identity verification in AI systems, if the data or means of verification remain under the sole control of the data subject.
5	**Data access requests:** controllers may charge fees or refuse a request if a data subject's access request is manifestly unfounded or excessive.
6	**Data breach notification:** breach notification to data subjects extended to 96 hours and only if high risk for individuals. Notification via new **single entry point** for security incidents and data breaches (also for incident notification under cybersecurity regulations).
7	**ePrivacy:** The cookie consent from the ePrivacy Directive moves into the GDPR. Consent required, with exceptions for technical storage, audience measurement, and security. Enablement of browser-level preferences.

EU Digital Omnibus

Key impact on AI Act

Cybersecurity Package

Delay to high-risk AI regime - Article 113

- Annex III in force latest in December 2027, instead of from August 2026.
- Annex I in force latest in December 2028, instead of from August 2027.

Registration of exempt HRAIS - Article 6(4)

- Removal of requirement to register in EU database for provider who considers that an AI system in Annex III is not high-risk.
- Provider must still document its assessment and provide this documentation on request.

Transparency regime - Article 50(2)

- Requirement to ensure that the outputs of an AI system generating synthetic audio, image, video or text content are marked in a machine-readable format and detectable as artificially generated or manipulated.
- Pushes back application date for existing systems from 2 August 2026 to 2 February 2027.

AI literacy – Article 4

- Current Article obliges providers and deployers to ensure a sufficient level of AI literacy of staff dealing with the operation and use of AI systems on their behalf.
- Replaces with obligation on EC and Member States to encourage providers and deployers to ensure sufficient AI literacy of staff.

Digital Omnibus: timeline

Key timings

19 Nov. 2025	• Adoption of legislative proposal by the European Commission
13 March 2026	• Publication of the Council's position (sets out how it will enter the negotiations)
18 March	• Publication compromise amendments European Parliament
26 March – 28 April	• Trilogue negotiations
June 2026	• Vote in plenary (trilogue agreement)
July 2026	• Publication in the Official Journal of the EU