

The background of the slide features a silhouette of several large satellite dishes on a horizon line against a dramatic sky at sunset or sunrise. The sky is filled with soft, wispy clouds in shades of blue, purple, and orange. The dishes are positioned at various angles, with the largest one on the left and several smaller ones further to the right.

TaylorWessing

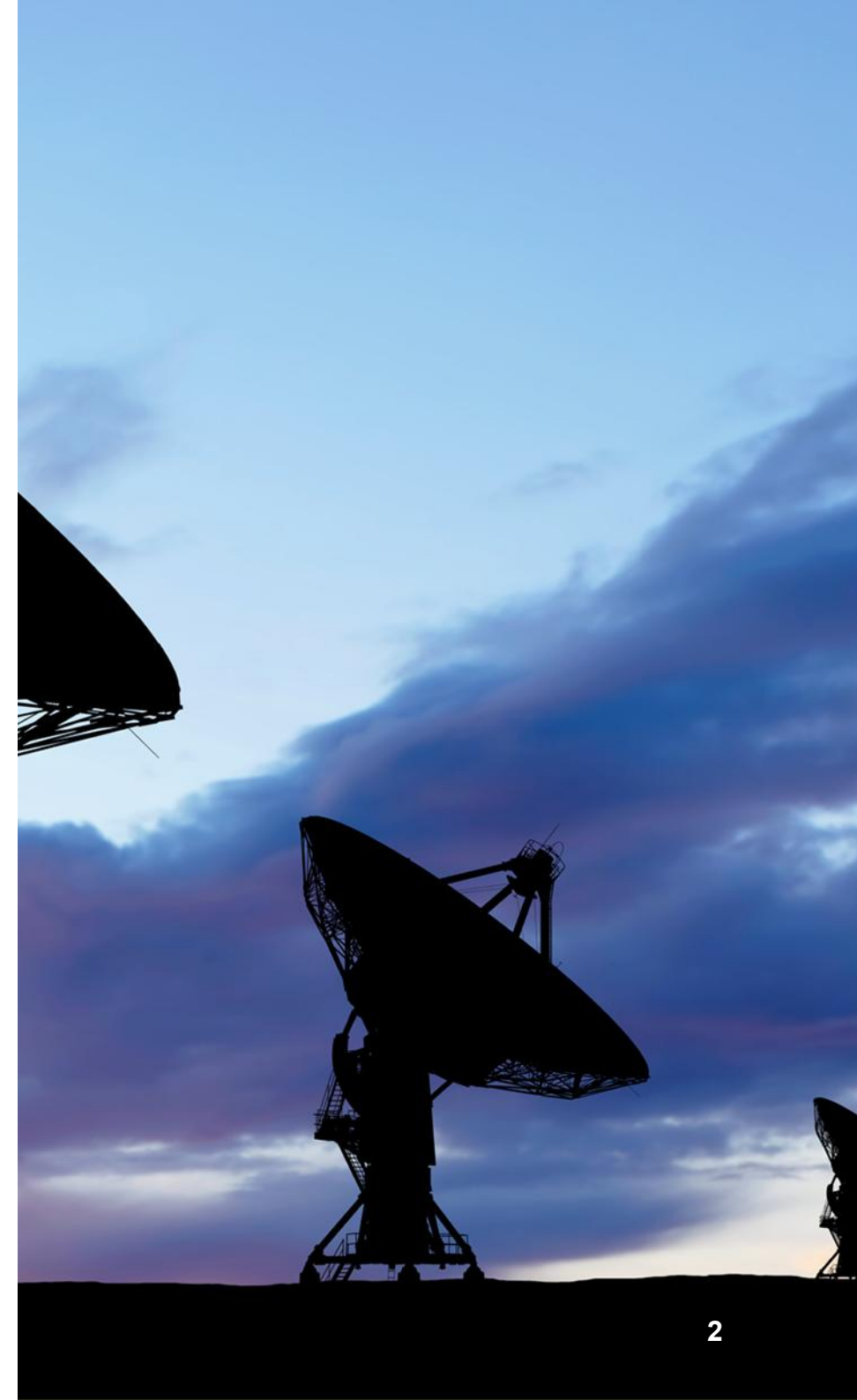
The new EU digital laws

Follow the sun webinar | Taylor Wessing

September 2, 2025 | Dr. Axel Frhr. von dem Bussche

Overview

1	European regulatory framework	3
2	Dealing with AI and EU AI Act	5
3	European data strategy (Data Act and Data Governance Act)	13
4	Digital Services Act Package (DSA and DMA)	21
5	EU cybersecurity (NIS-2, DORA, and CRA)	27
6	EU Accessibility Act	32





1 | European regulatory framework

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Finance	Overview of EU legislation in the digital sector Status: August 21, 2025								
Digital Europe Program Regulation	Recovery and Resilience Facility Regulation	Frequency Bands Directive	...	Database Directive	Regulation for a Cybersecurity Act	Law Enforcement Directive	Toys Regulation	...	EU Merger Regulation	Common VAT system									
Horizon Europe Regulation	InvestEU Program Regulation	Radio Spectrum Decision	GDPR	Community Design Directive	European Cybersecurity Centre	Directive: combating fraud	European Standardization Regulation	EU Accessibility Act (EEA)	Technology Transfer	Administrative cooperation (tax)									
Regulation on a pilot regime distributed ledger tech. Market	Connecting Europe Facility Regulation	Broadband Cost Reduction Directive	Regulation on the free flow of non-personal data	Enforcement Directive	NIS-2 Directive	Interoperability between EU information systems in the field of borders and visas	eIDAS Regulation	Geo-blocking Regulation	Company Law Directive	Payment Services Directive 2									
Private and Confidential	Regulation on Joint Undertakings under Horizon Europe	Open Internet Access Regulation	Open Data Directive	Directive on the protection of trade secrets	Information Security Regulation	Regulation on terrorist content online	Radio Equipment Directive	Regulation on cooperation for the enforcement of consumer protection laws	Market Surveillance Regulation	Digital Operational Resilience Act (DORA)	<table><tr><th>Applicable law</th><th>Published in the Official Journal of the EU</th></tr><tr><td>Under negotiation</td><td>Proposal by the Commission entered the legislative process</td></tr><tr><td>Planned initiative</td><td>Mentioned by the Commission as potential legislative initiative</td></tr><tr><td>Abandoned</td><td>Negotiations failed</td></tr></table>	Applicable law	Published in the Official Journal of the EU	Under negotiation	Proposal by the Commission entered the legislative process	Planned initiative	Mentioned by the Commission as potential legislative initiative	Abandoned	Negotiations failed
	Applicable law	Published in the Official Journal of the EU																	
	Under negotiation	Proposal by the Commission entered the legislative process																	
	Planned initiative	Mentioned by the Commission as potential legislative initiative																	
	Abandoned	Negotiations failed																	
	Decision on a path to the Digital Decade	EECC	Data Governance Act (DGA)	Design Directive	Cybersecurity Regulation	Temporary CSAM Regulation	Regulation for a Single Digital Gateway	Digital Content Directive	P2B Regulation	Crypto-assets Regulation (MiCAR)									
	European Chips Act	EU top-level domain regulation	Data Act (DA)	Compulsory licensing of patents	Cyber Resilience Act (CRA)	E-evidence Regulation	General Product Safety Regulation	Directive on certain aspects concerning the sale of goods	Single Market Program	Financial Data Access Regulation									
	European Critical Raw Materials Act	Roaming Regulation	European Health Data Space	Standard essential patents	Cyber Solidarity Act	Directive on combating violence against women	Machinery Regulation	Digital Services Act (DSA)	Vertical Block Exemption Regulation	Payment Services Regulation									
	Net Zero Industry Act	Secure Connectivity Program Regulation	Data collection for short-term rental Regulation				Digitalization of travel documents	AI Act	Political advertising regulation	Digital Markets Act (DMA)	Digital euro								
STEP	RSPP 2.0	Interoperable Europe Act	(New) Product Liability Directive				Rights to repair Directive	Regulation on distortive foreign subsidies	Regulation on combating late payment										
EU Space Law	Digital Networks Act	ePrivacy Regulation	AI Liability Directive				e-invoicing Directive	Platform Work Directive	EU Business Wallet										
European supercomputer capacity for AI start-ups		Digital Networks Act						Multimodal digital mobility services	Single Market Emergency Instrument	4									



2 | Dealing with AI and EU AI Act

AI Act – Overview

Subject

- World's first AI Act governing AI systems and AI models for general use (GPAI models)
- "Product compliance," market surveillance and control
→ **AI Act = product safety law**

Objective of the AI-Act

- Safety of EU citizens
- Protection of fundamental rights
- Trust and acceptance of AI as a technology
- Promotion of innovation

Who is affected?

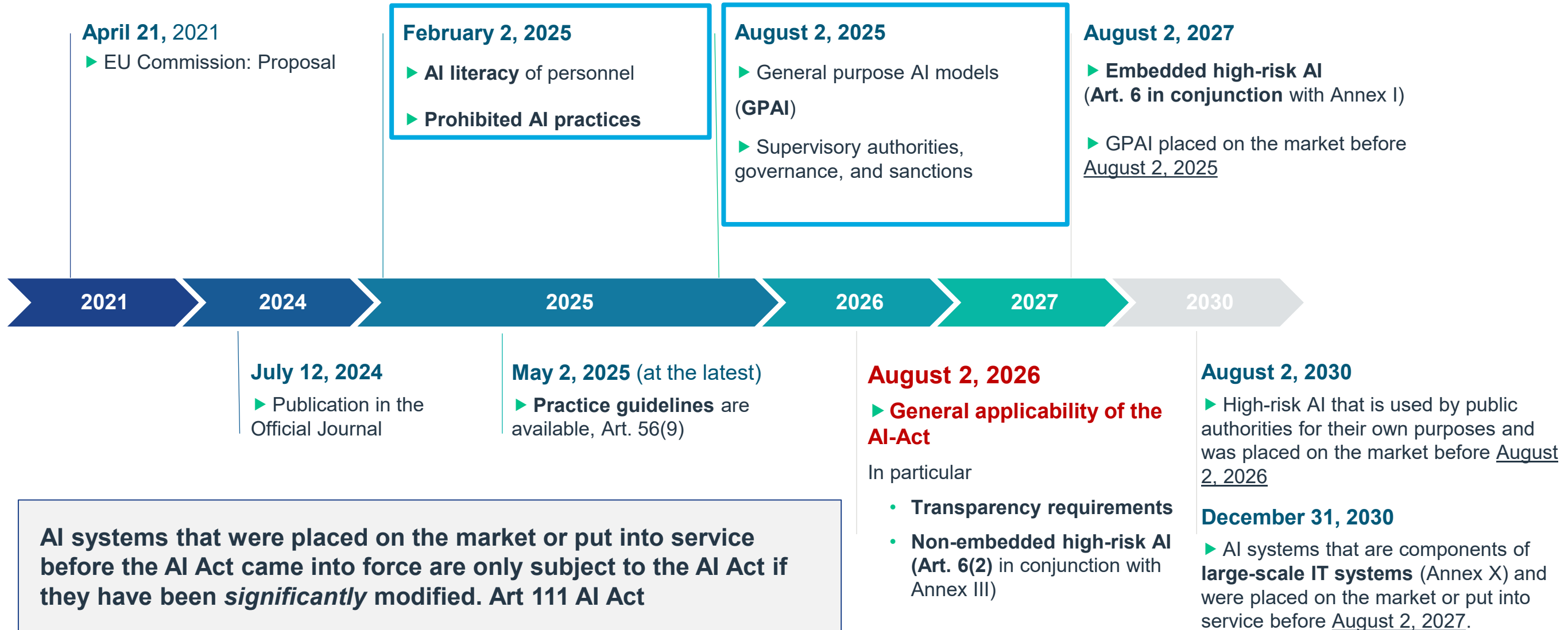
- Providers of AI systems or models
- Deployers of AI systems
- Product manufacturers who place AI systems on the market together with their product
- Extraterritorial approach

Sanctions?

- Up to EUR 35 million or up to 7% of global turnover
- Administrative measures (including a ban on offering AI systems)

AI Act: Timeline

☐ - Regulations already apply



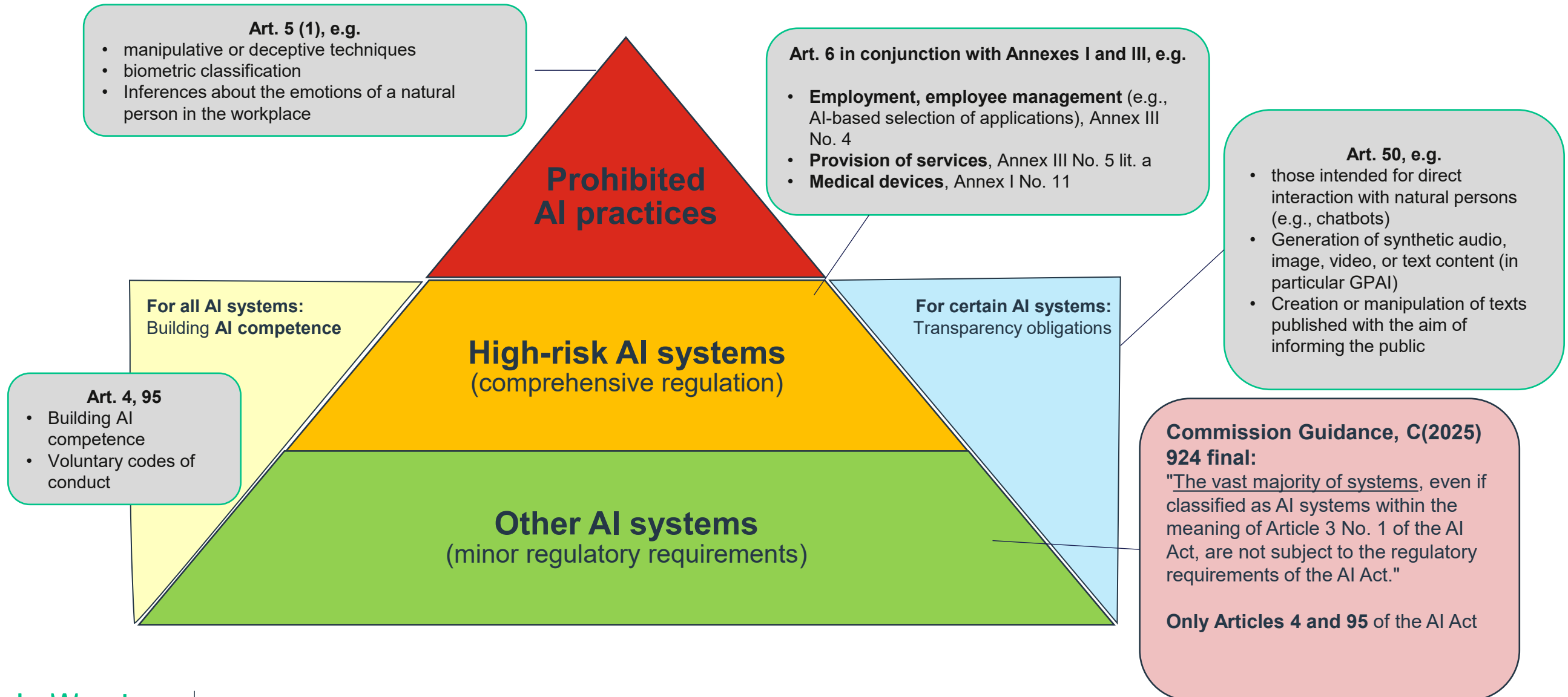
Personal and territorial scope of application of the AI Act

Personal and territorial: The persons subject to the regulation are listed in Art. 2 (1) of the AI Act

- a) **Providers** placing on the market or putting into service AI systems or placing on the market general-purpose AI models **in the Union, irrespective of whether those providers are established or located within the Union or in a third country**
- b) **Deployers** of AI systems that have their place of **establishment or are located within the Union**
- c) **Providers** and **deployers** of AI systems that have their **place of establishment** or are **located in a third country**, where the **output** produced by the AI system is **used in the Union**
- d) **Importers** and **distributors** of AI systems
- e) **Product manufacturers** who placing on the market or putting into service an AI system together with their product and under their own name or trademark **[in the Union]***
- f) **Authorised representatives of providers** which are **not established in the Union**
- g) **Affected persons** that are located **in the Union**

*cf. Art. 1(2)(a), Art. 25(3) AI Act

Risk-based approach of the AI Act!



Risk classification

High-risk AI:

Embedded AI

Art. 6 (1) + Annex I

Safety component of a product or the product itself

+

Subject to conformity assessment



Equipment that
burns gaseous
fuels



Civil aviation



Recreational boats



Toys



Medical devices



Agricultural
vehicles

Non-embedded AI

Art. 6 (2) + Annex III



General and
vocational education



Work:
promotion/dismissal
decisions



Service provision



Recruitment



Energy supply

High-risk AI
(comprehensive regulation)

Notwithstanding Article 6(2), the AI systems listed in Annex III **shall not be considered high risk if they are intended to:**

Art. 6 (3) subpara. 1

- to perform a narrow process control task;
- to improve the result of a human activity already completed;
- to identify decision patterns or deviations, and it is not intended to replace or influence the human assessment previously carried out without proper human review;
- to carry out a preparatory task for an assessment

Art. 6 (3) subpara. 2

and does not carry out profiling of natural persons

Requirements of the AI Act: Brief overview

"Normal" GPAI models:

- Technical documentation
- Compliance with copyright
- Detailed summary
- Code of conduct

GPAI models with systemic risk

- Model evaluation & stress tests
- Systemic risk assessment & cybersecurity measures
- Reporting serious incidents & energy efficiency reports

High-risk AI systems:

- Technical Documentation
- Quality management system
- Transparency + provision of information
- Risk management system
- Human oversight
- Cybersecurity measures
- Impact assessment for fundamental rights
- Conformity assessment procedures



3 | **European Data Strategy (Data Act and Data Governance Act)**

Data Governance Act (DGA)

Subject

- Creation of an infrastructure for (voluntary) data exchange
- Removal of technical barriers

Objective of the DGA

Ensuring data availability, strengthening trust in data exchange, overcoming technical barriers

→ **Digital transformation** (through extensive data access and usage options)

→ **Better management of societal challenges** (e.g., climate change, mobility transition)

Who is affected?

- Public sector bodies
- Data intermediaries
- Data altruism organisations

When

Entered into force on June 23, 2022;
fully applicable since **September 24, 2023**

DGA: Measures

Data availability

- **Reuse** of certain categories held by **public bodies** (e.g., confidential statistical data from the Federal Statistical Office in which a research institution has an interest)
- **Data intermediation services** as a **key role in the data economy** (e.g., through data marketplaces for data exchange between companies)
- **Data altruism** – incentives for data donations

Strengthening trust in data exchange

- Avoiding **conflicts of interest**
- **Independence of pricing**
- **Structural separation**
- **Transparency, fairness & compliance**
- **Non-discriminatory access**

Removal of technical barriers

- Requirements for **neutrality** and **interoperability**
- **Appropriate level of protection**

Data Act (DA)

Subject

Promoting the availability and usability of data (personal and non-personal data) in the EU through:

- Data access and data use rights
- Interoperability of data and easier switching between data processing services (especially cloud services)
- Obligation to disclose data in exceptional circumstances (B2G)
- Promote Fairness in B2B and B2G Contexts

Who is affected?

- Data holders
- Manufacturers of connected products or related services
- Users
- Data recipients / third parties
- Data processing services

When

Entered into force on January 11, 2024; will be applicable to the greatest extent possible from September 12, 2025.

September 12, 2025

Scope of application

Data access: Connected products



ISO/IEC 30141:2024
(reference
architecture)

Essential characteristics of connected/IoT products, Art. 2 No. 5 DA:

- Physical item
- **Data collection:** Product collects data about its performance, use, or environment through its components or operating system ("product data," Art. 2 No. 15 DA).
- **Data transmission:** Product transmits product data via an electronic communication service, a physical connection, or device-internal access (e.g., terrestrial telephone networks, television cable networks, satellite networks, and near-field communication networks).

- **Decisive:** Placing on the EU market
- **Excluded:** Prototypes

Material scope

Data access: Related service

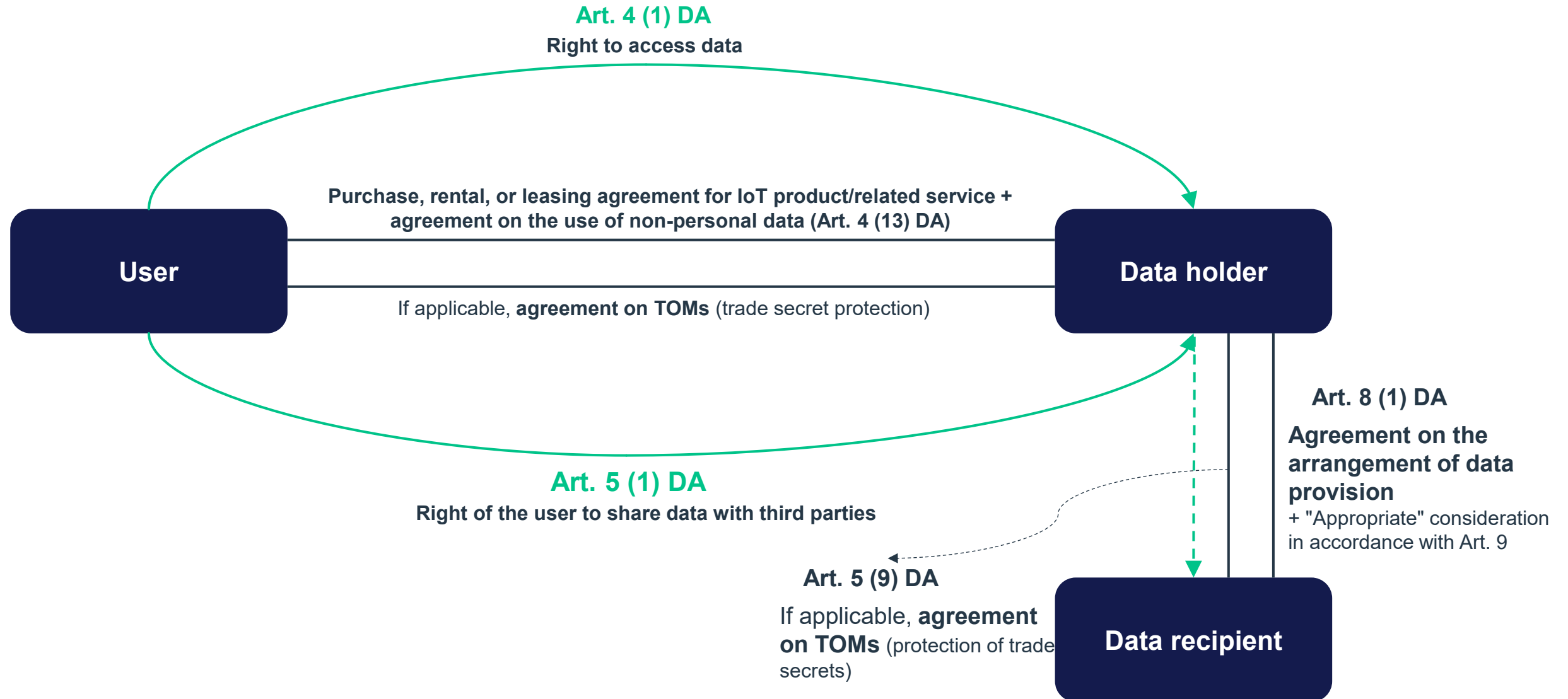


Essential characteristics of connected services, Art. 2 No. 6 DA:

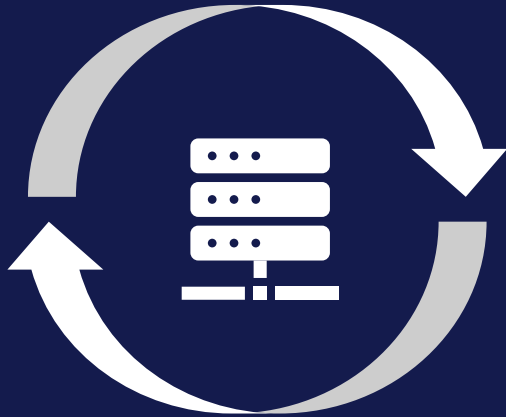
- Not a physical object, but "digital" products/services (including software)
- **Prerequisite:** Connected product
- **Mutual data exchange** between the connected product and the related service.
- Related service **influences the functions, behavior, or operation** of the connected product.
- By providing the related service to the user of the connected product, the **provider becomes the data owner**.

- **Decisive factor:** Placing on the EU market
- **Excluded:** Services related to connectivity and power supply, as well as aftermarket services (e.g., additional consulting, analysis, and financial services, as well as regular repair and maintenance work).

DA: Contractual relationships



DA: Switching between data processing services



Fair switching between data processing services

- Breaking out of
 - lock-in effect
 - Vendor lock-in
- Promotion of fair competition

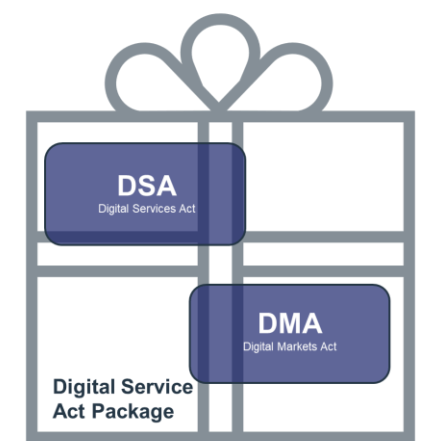
Requirements (providers of data processing services)

- Contract amendment (customer's right to switch)
- Removal of technical barriers to effective switching
- Duty to provide information
- Transparency
- Gradual abolition of switching fees
 - January 11, 2024 → January 12, 2027: reduced fees
 - From January 12, 2027: no fees
- Implementation of interoperability standards



4 | Digital Services Act Package (DSA and DMA)

Digital Service Act (DSA)



Subject

Uniform horizontal rules on due diligence obligations and liability privileges for intermediary services

Object

Creation of a safe, predictable, and trustworthy online environment

→ comprehensive protection of users' fundamental rights

Who is affected?

Providers of digital services that provide consumers with goods, services, or content

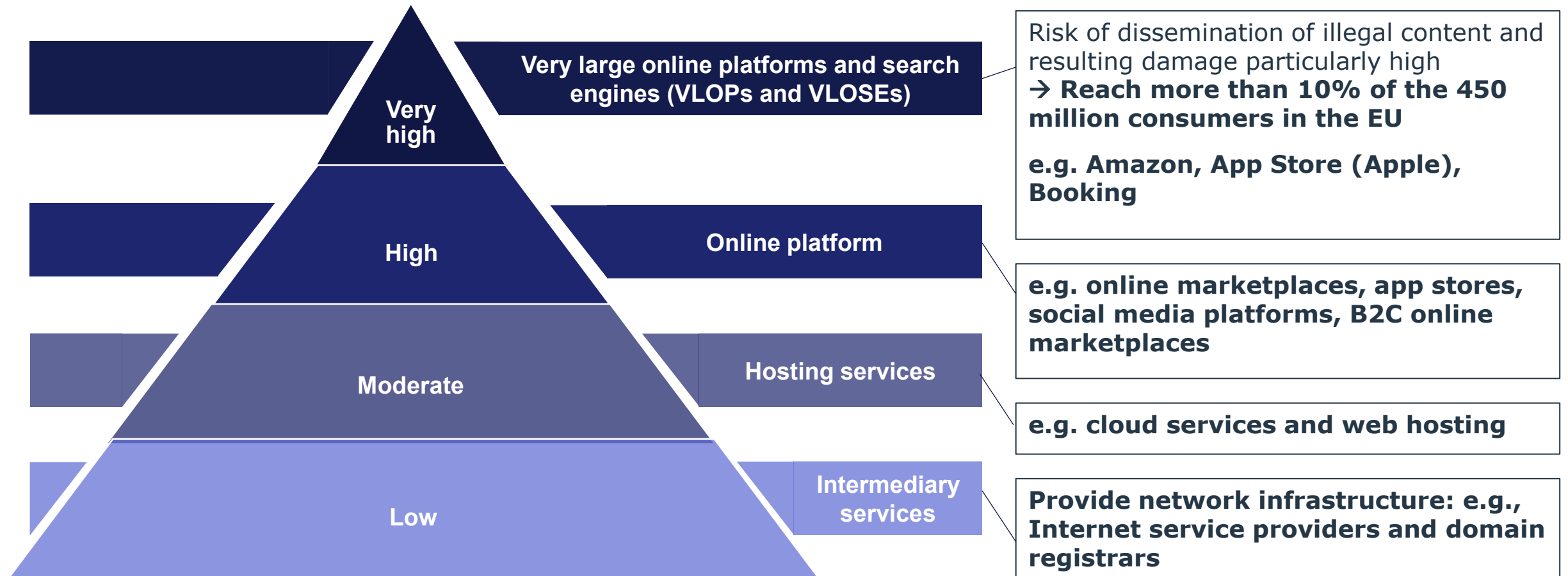
- Intermediary services
- Hosting services
- (Very large) online platforms or search engines

When

Entered into force on November 16, 2022;
fully applicable since **February 17, 2024**

The „Digitale-Dienste-Gesetz (DDG) implements the components of the DSA that require further elaboration in Germany.

DSA: Level of due diligence



DSA: VLOPs and VLOSEs and measures

To be designated by the Commission (see Art. 33(4) DSA)

Very large online platforms (VLOPs):

- AliExpress
- Amazon Store
- App Store (Apple)
- Aylo Freesites (18+ service)
- Booking.com
- Facebook (Meta)
- Google
- Google
- Google Shopping
- Instagram (Meta)
- LinkedIn
- NKL Associates s.r.o (18+ service)
- Pinterest
- Shein
- Snapchat
- Technius (18+ service)
- Temu
- TikTok
- WebGroup (18+ service)
- Wikipedia
- X
- YouTube (Google)
- Zalando

Very large online search engines (VLOSEs):

- Bing
- Google Search

Measures taken by the DSA

Easier removal of illegal content (e.g., hate speech, disinformation, counterfeit products)

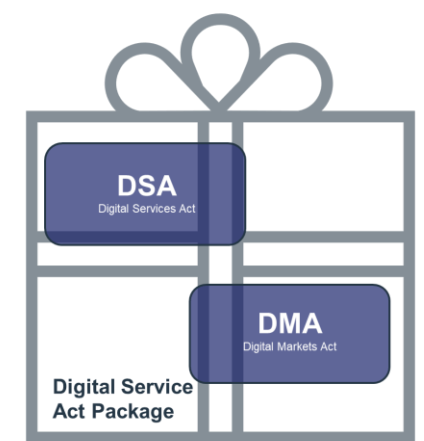
Prohibition of "dark patterns" and "nudging" → protection of user autonomy

Greater transparency in advertising

Higher requirements for access to B2C online marketplaces

Available at: <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>

Digital Markets Act (DMA)



Subject

Regulation and strengthening of digital markets by prohibiting certain practices that restrict competition

Objective of the DMA

Fair competition between digital platforms regardless of their size

→ More choice between better services at fairer prices for consumers

→ Market access for start-ups and SMEs

Who is affected?

So-called "gatekeepers" with certain core platform services ("CPS")

When

Entered into force on November 1, 2022;
Fully applicable since **May 2, 2023**

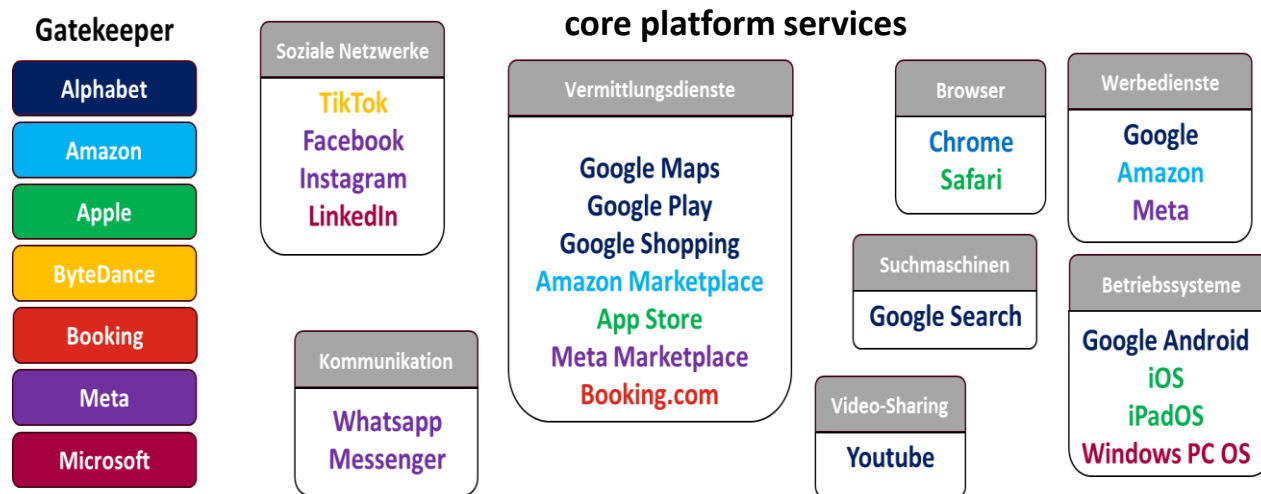
Sanctions

Up to 10% of the gatekeeper's global turnover (up to 20% for repeated infringements)

DMA: Gatekeepers and measures

The Commission designates companies as "gatekeepers" if:

1. **Annual** turnover **exceeds EUR 7.5 billion** (last three financial years) **or** **EUR 75 billion market capitalization**
2. **CPS** has more than **45 million active users per month** (including at least 10,000 commercial EU users)
3. **CPS** provided in at least three member states



Measures taken by the DMA

Code of Conduct for Gatekeepers

Prohibition of unfair practices

Examples of unfair practices:

Rankings: Favoritism toward own offers

Technical blocking of the installation of external applications

Preventing developers from using third-party payment platforms for the sale of apps

Pre-installing software applications without the option to uninstall them



5 | EU cybersecurity (NIS-2, DORA, and CRA)

NIS-2 and DORA at a glance



NIS-2 Directive



- **Objective:** EU-wide minimum standards for cybersecurity to make critical and important companies more resilient (Art. 1 (1) NIS-2 Directive)
- **Who is affected?** Public or private entities listed in Annex I ("high criticality") or II ("other critical sectors")
 - Not only "critical infrastructure," but also, for example, digital services, food production, etc.
- **Obligations**
 - **Introduction of risk management measures** (security by design, emergency plans)
 - **Reporting obligations for security incidents** (often within 24 hours)
- **Geographical:** in EU member states
- **Time**
 - > Entry into force: January 16, 2023
 - > Implementation deadline: by October 18, 2024
 - > In Germany: **NIS 2 Implementation and Cybersecurity Strengthening Act** (has since been rejected by „the traffic light coalition“; to be reintroduced by the new federal cabinet in **July 2025**)

"Cybersecurity twins"

NIS-2: general for society and the economy

DORA: specific to the financial sector (with some higher requirements)

Digital Operational Resilience Act (DORA)



- **Objective:** To strengthen confidence in the financial markets by ensuring that they continue to function even in the event of serious cyberattacks or system failures (Art. 1 (1) DORA)
- **Who is affected?** Banks, insurance companies, payment service providers, stock exchanges, etc.
- **Obligations**
 - **Comprehensive IT risk management**
 - **Monitoring of IT service providers** (cloud providers, etc.)
 - **Reporting obligations in the event of IT disruptions**
 - **Regular resilience testing**
- **Geographical:** in EU member states
- **Time:**
 - > Effective date: January 16, 2023
 - > Mandatory application: since **January 17, 2025**

Note: NIS-2 aims to ensure that the failure of one company does not immediately jeopardize the supply of entire sectors of society.

Note: DORA aims to ensure that financial markets remain stable even when central IT systems come under pressure from cyberattacks or disruptions.

Cyber Resilience Act (CRA)

September 15, 2022: EU Commission proposal for a regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)

- Introduction of security requirements for a wide range of **tangible and intangible products with digital elements**, including non-integrated software
- 11.12.2024 enactment
- 11.09.2026 reporting obligations
- 11.12.2027 enforcement

Scope

- Manufacturers, importers, and distributors who place a product with digital elements on the market **whose intended or foreseeable use involves a logical or physical connection to a device or network**
- Exceptions, e.g., for certain medical products or products for military purposes
- No SaaS
- Free and open-source software only covered for commercial use
- The terms "manufacturer" and "product with digital elements" are broadly defined

CRA: Manufacturer obligations

- **Design, development, and production in accordance with Annex I CRA, e.g.**
 - Products with digital elements must be designed, developed, and produced in such a way as to guarantee an appropriate level of cybersecurity
 - Products with digital elements should be delivered without known exploitable vulnerabilities
 - Products should be delivered with a secure default configuration that allows the product to be restored to its original state
- Cybersecurity **Risk Assessment** to minimize security risks
- Due diligence when integrating third-party components
 - Documentation requirements before the product is placed on the market
- **Conformity assessment procedures** (followed by CE certification + EU declaration of conformity)
- Inclusion of product information and instructions for use
- **Reporting obligations**, e.g., to ENISA within 24 hours of discovering vulnerabilities

CRA: Market supervisory authority and sanctions

Market supervisory authority

- Monitors the effective implementation of the Cyber Resilience Act
- Verifies the compliance of products if they pose a significant security risk

Sanctions

- For violations of the essential security requirements set out in Annex I, up to **EUR 15,000,000** or **2.5%** of the global turnover of the previous financial year (Art. 64(1) CRA)
- For providing false information to the market surveillance authority, up to **EUR 5,000,000** or **1%** of the global turnover of the previous financial year (Art. 64(4) CRA)
- In the event of other violations, up to **EUR 10,000,000** or **2%** of the global turnover of the previous financial year (Art. 64 (3) CRA)



6 | EU Accessibility Act

European Accessibility Act

Core idea

- EU-wide standard for accessibility of products and services
- B2C only, but B2B offerings should be fully blocked for consumers

Who is affected

- Manufacturers, importers, and distributors of certain **products and services**, e.g.
 - **Products**: computers, smartphones, ATMs, e-books, and ticket machines
 - **Services**: online shops, e-banking, electronic communication services, passenger transport tickets

Object

- People with disabilities should be able to participate independently in digital life in the European single market.

Scope

- Entry into force: June 28, 2019
- Implementation deadline: by June 28, 2019
- Application of the provisions since **June 28, 2025** (in some cases with transition periods for products already on the market)



Implementation in Germany



Category	Legal basis	Scope	Exceptions
Private providers	BFSG (applicable since 2025)	Websites, apps, e-commerce, vending machines, etc.	Micro-enterprises
Public providers	BGG + BITV 2.0 , supplemented by BFSG	Digital services provided by public authorities	No specific exceptions mentioned

European Accessibility Act (2) – measures



General functional requirements

- Information must be **perceptible, operable, understandable and robust**
- Accessible interfaces: such as tactile, voice-based, or alternative operating options
- Compatibility with assistive technologies (screen readers, Braille displays, speech recognition software)
- **Accessibility statement** with information on compliance and contact details
- **Reporting and documentation obligations** towards supervisory authorities

Digital services

- Texts, images, forms, etc. must be **machine-readable**
- Videos with **subtitles and audio descriptions**
- Clear and consistent user guidance, no barriers in ordering or payment processes



Products

- **Operation possible via various senses** (visual, acoustic, tactile)
- Clearly recognizable controls, also usable with assistive devices
- Provision of **accessible instructions for use**



European digital laws – a reminder

Digital and data regulation guide



[Home – Digital, data, and consumer regulation](#)



Digital legislation in a page

With so much complex digital legislation coming in in the EU and UK, it can be hard to navigate even the essentials. We've produced a set of one-page overviews of key legislation at the top of the agenda for 2025, covering:

- [EU AI Act](#)
- [EU Digital Services Act](#)
- [EU Data Act](#)
- [EU Data Governance Act](#)
- [EU Cyber Resilience Act](#)
- [EU NIS2 Directive](#)
- [EU Machinery Regulation](#)
- [EU Gigabit Infrastructure Act](#)
- [EU European Health Data Space proposal](#)
- [UK Online Safety Act](#)



You can see table summaries of other aspects of the EU AI Act [here](#), and of the UK Online Safety Act [here](#). You may also be interested in our [Digital Legislation Tracker](#) and our [Digital and data regulation guide](#).

[Digital legislation in a page](#)

Q&A



Your contact

Axel Freiherr von dem Bussche is a specialist lawyer for information technology law in the Technology, Media & Telecoms practice group. He advises clients on national and international digital and data protection projects and is a proven expert in IT law and the GDPR.

With his many years of experience and outstanding expertise, Axel von dem Bussche expertly guides clients on both the provider and user side through complex international transactions, contract drafting, and regulatory issues. He advises corporations on their transformation to digital and global business models, supports companies in implementing AI and data protection regulations, acts as a strategic advisor to management on compliance in digitalization, and negotiates with the relevant supervisory authorities.

Languages

- German, English, French

// "Data protection specialist Axel von dem Bussche advises renowned clients on data protection issues (...). He also represents clients in proceedings at regional and national level against data protection supervisory authorities."; "He is up to date on all new developments, is very client-oriented and quickly analyzes new laws," client, [Chambers Europe 2021-2024](#), [Chambers Germany 2025](#)

Recognized as a "Thought Leader" for data protection in Germany, [Who's Who Legal 2025](#)

Featured lawyer for data protection, [Chambers Europe 2019 - 2024](#)

Recommended for information technology and data protection "One of the best, an absolute strategist," Client, "very strong client focus, negotiating skills and assertiveness," "the expert in data protection, excellent specialist knowledge and negotiating skills," "excellent advice and specialist knowledge coupled with a strong client focus," "best lawyer in Germany for data protection litigation," client; "Very active, extremely strong," "absolute expert in the industry," "demands outstanding performance from junior staff," "pleasant and very experienced," competitor; [JUVE 2015/2016- 2024/2025](#)

Leading name for IT and digitalization, [The Legal 500 2021–2025](#)

Leading lawyer for data protection [Kanzleimonitor \(diruj\) 2020/2021 - 2023/24](#)

Top 100 lawyers in Germany, [Kanzleimonitor \(diruj\) 2023/24](#)

TOP Lawyer for Data Protection Law, [WirtschaftsWoche 2019-2023](#)

Outstanding Lawyer, [Thomson Reuters 2022](#)

Listed in the best list as a leading international lawyer for data protection and IT, [Who's Who Legal 2019-2024](#)

Highlighted as "Lawyer of the Year" [2024](#) and Best Lawyer for IT Law, [Best Lawyers in Germany](#), [Handelsblatt 2018 - 2024](#)



Dr. Axel Frhr. von dem Bussche, LL.M. (L.S.E.)

Partner
Hamburg

+49 40 36803-229
a.bussche@taylorwessing.com

Consulting

- Information technology/ Telecommunications
- Data protection
- Copyright & Media Law
- Litigation & Dispute Resolution
- Technology, Media & Communications



